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

EY Global Third-Party Risk Management Survey 2019–20

Overall survey results

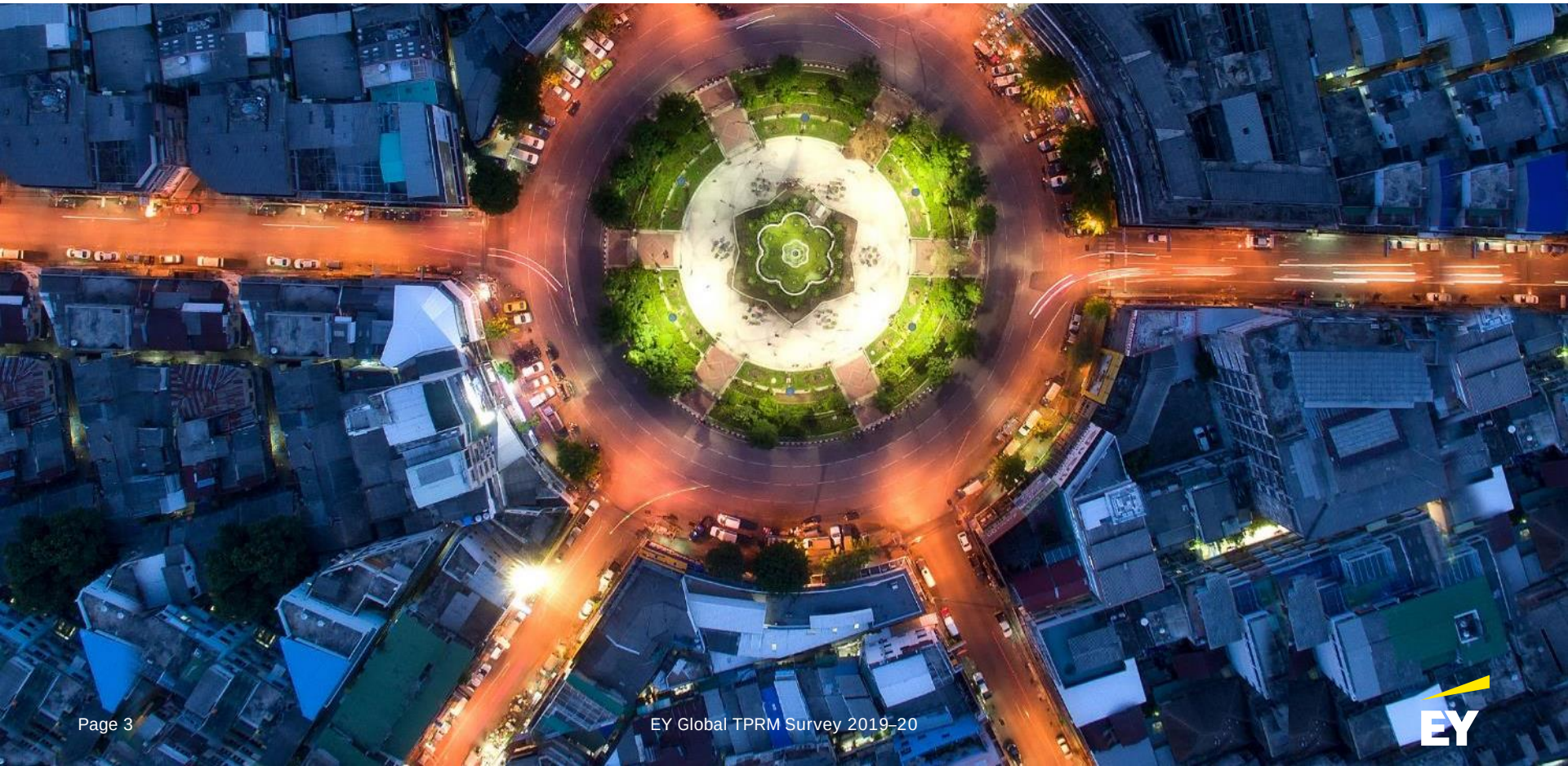
EY
Building a better working world

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

Global results



Background

From July through September of 2019, EY professionals conducted a survey of 246 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.

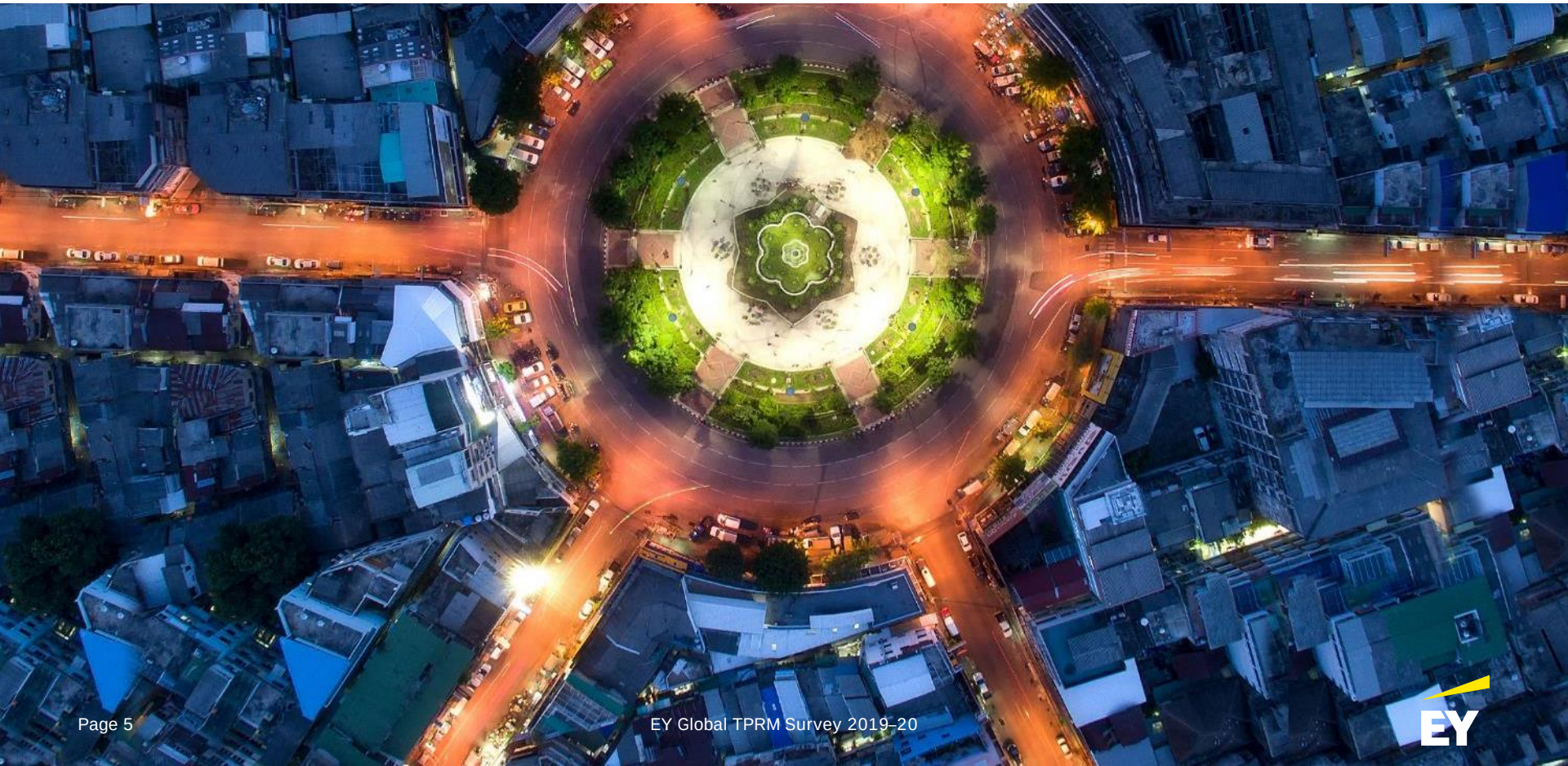
Industries in the survey included, but were not limited to, financial services, consumer products and retail, health care, life sciences, media and entertainment, technology, power and utilities, diversified industrial products, and government and public sector.

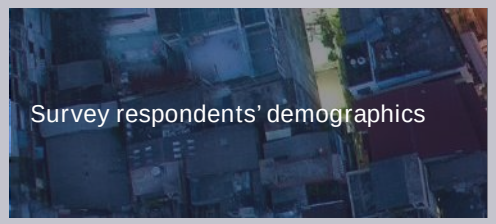
In this survey, we asked participants to respond to questions within several key areas of their respective third-party risk management (TPRM) programs. Topics included:

- Third-party risk management program/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
- Nontraditional third parties
- Concentration risks (financial services only)
- Affiliate management (financial services only)
- Innovation

This document includes the results aggregated for each question across all industries. For any questions, support for data interpretation or specific data requests, please reach out to tprm@ey.com.

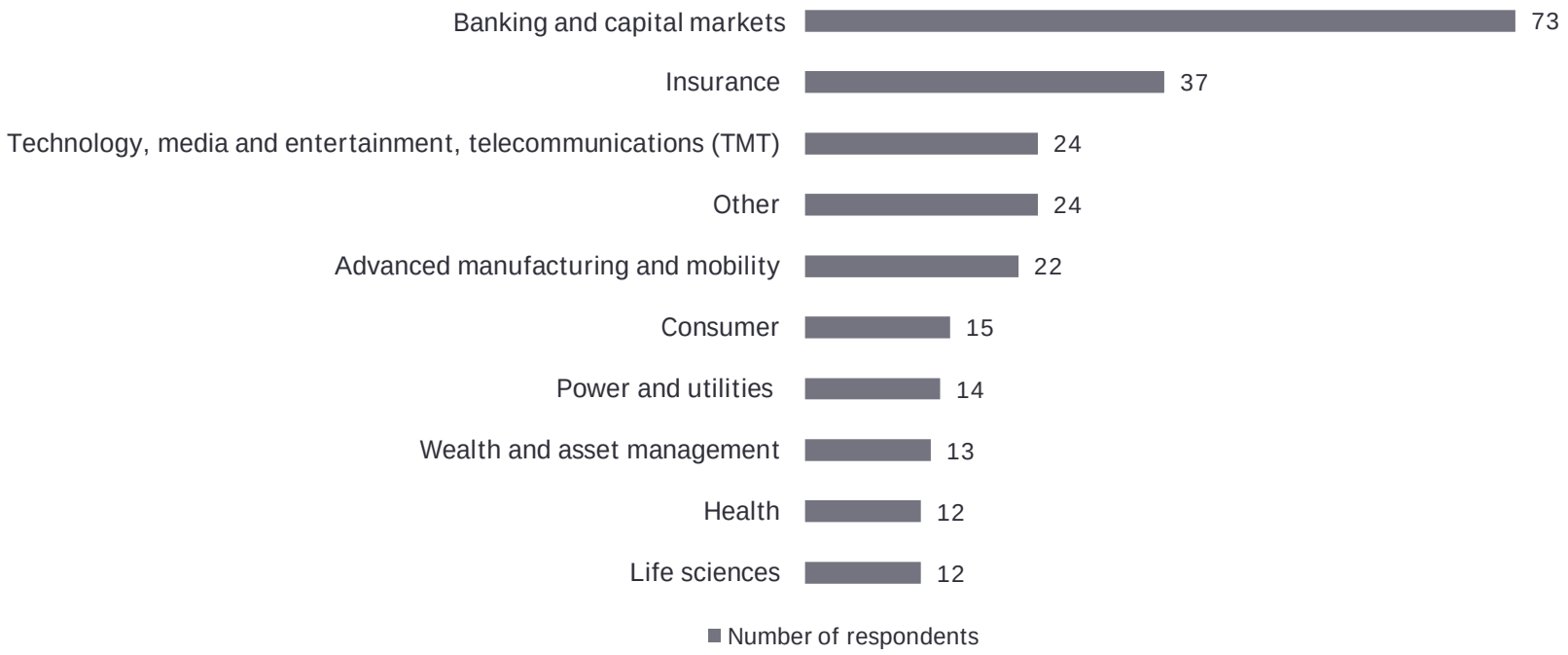
Survey respondent demographics

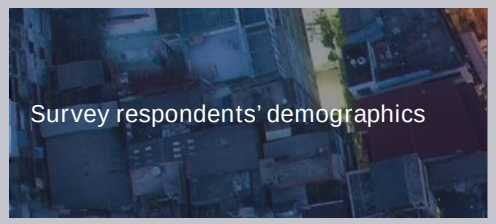




Of the 246 survey participants, the largest number of respondents came from the banking and capital markets sector, a result of the tenure of programs and regulatory pressures. This group was followed by insurance; technology, media and entertainment, telecommunications; advanced manufacturing and mobility; and consumer.

Respondent profile (Q1) number of respondents

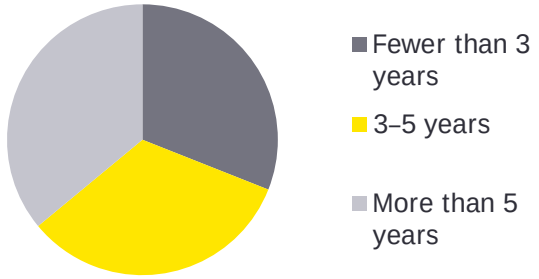




Almost two-thirds of the companies surveyed were in the US, more than one-quarter in Europe, and the remainder in Asia-Pacific. The companies were nearly evenly split among those that had third-party risk management programs in place for more than five years, three to five years and fewer than three years.

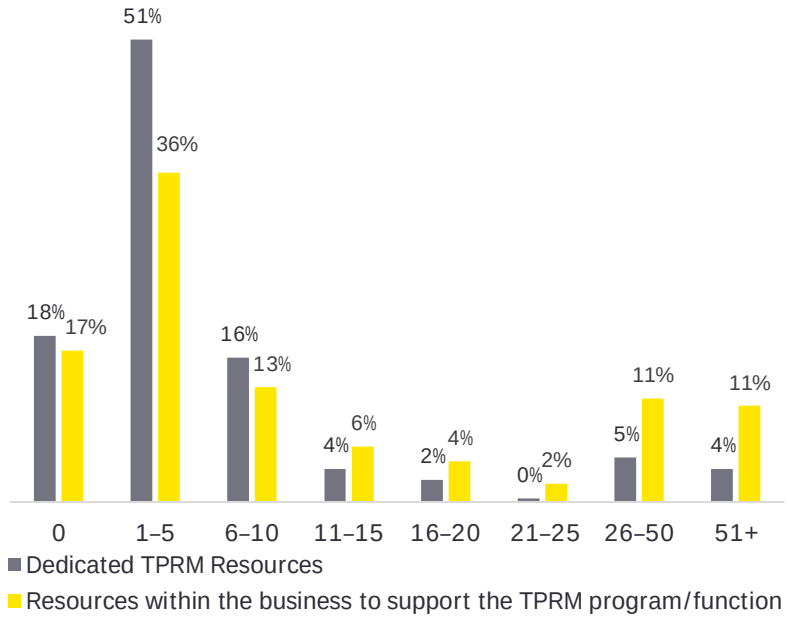
Respondent profile (Q2, Q3, Q4)	Participants	
By region	#	%
Americas	155	63%
Europe	75	30%
Asia-Pacific	16	7%
By company size (headcount)		
Fewer than 5,000	88	36%
5,001 to 15,000	52	21%
15,001 to 25,000	27	11%
25,001 to 50,000	25	10%
50,001 to 100,000	28	11%
More than 100,000	26	11%

TPRM program operation lifetime

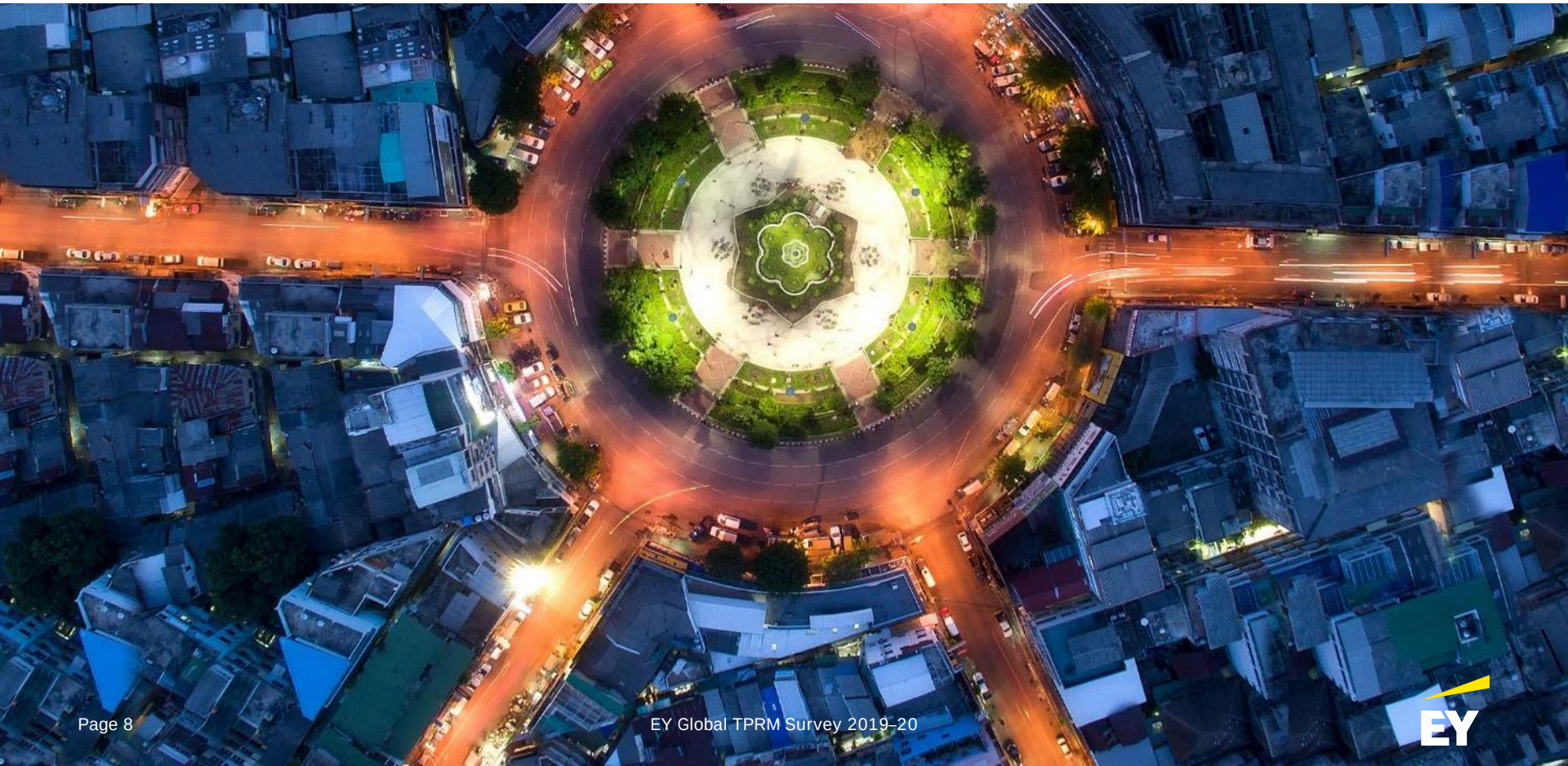


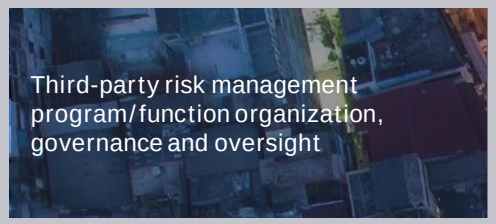
TPRM program resources

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



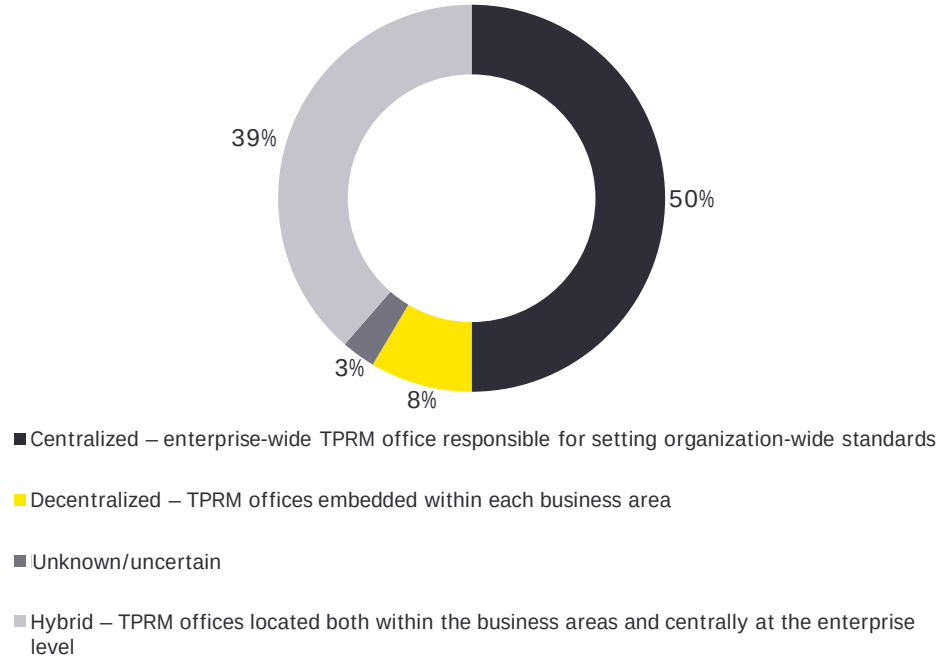


Third-party risk management program/function organization, governance and oversight

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

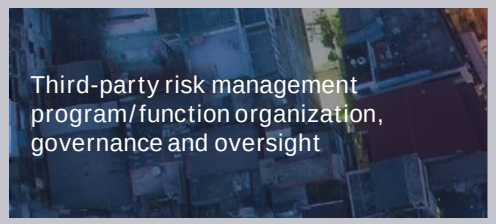
TPRM program structure

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?

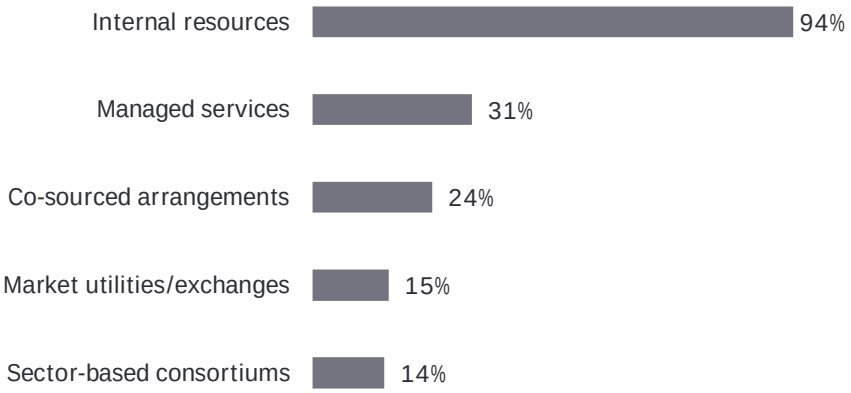


Third-party risk management program/function organization, governance and oversight

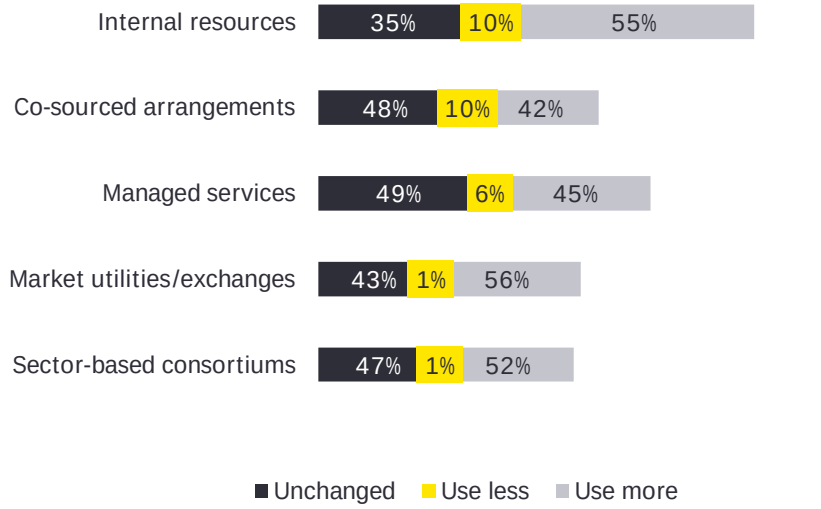
Looking out over the next two to three years, there is a clear desire among the organizations surveyed to leverage external solutions more actively. More than 40% of the organizations surveyed expect to more frequently use managed service providers or co-sourcing to execute their third-party risk management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

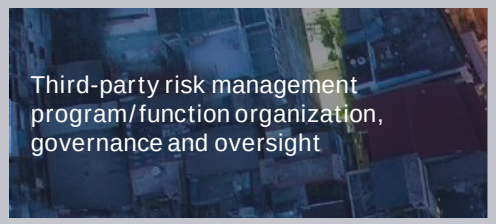
TPRM execution

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?



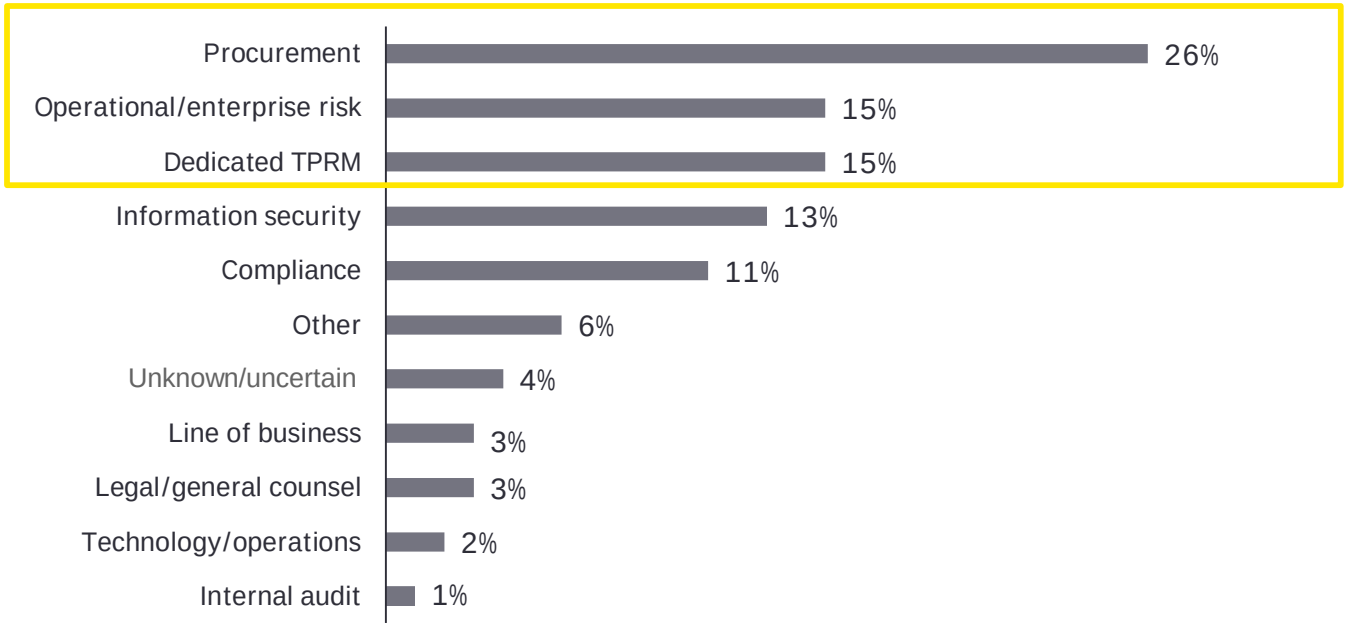


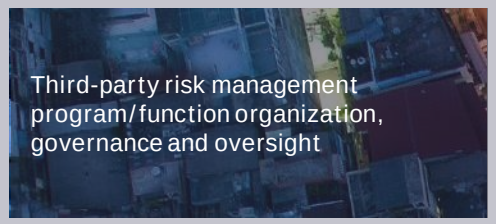
Third-party risk management program/function organization, governance and oversight

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

Integrated with TPRM program

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





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

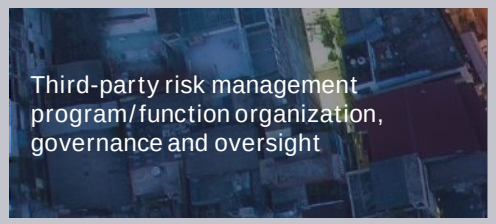
With the TPRM life cycle touching so many areas of an organization, it is not surprising that the surveyed organizations approach the activities differently. While there is some consensus on procurement's ownership of third-party inventory management and contract expiration and termination, there is 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	40%	20%	2%	6%	6%	6%	11%	2%	1%	1%	5%
Design and facilitation of the inherent risk assessment process/framework	12%	24%	5%	16%	17%	11%	4%	3%	2%	2%	3%
Review and updating of contract terms as part of ongoing monitoring	27%	5%	35%	7%	1%	5%	15%	1%	1%	1%	3%
Identification of expired contracts	48%	4%	17%	2%	1%	2%	21%	1%	1%	1%	3%
Termination of contracts	38%	4%	24%	2%	1%	1%	25%	1%	0%	1%	1%
Issue management/ risk treatment	8%	15%	6%	12%	14%	11%	24%	4%	3%	2%	2%

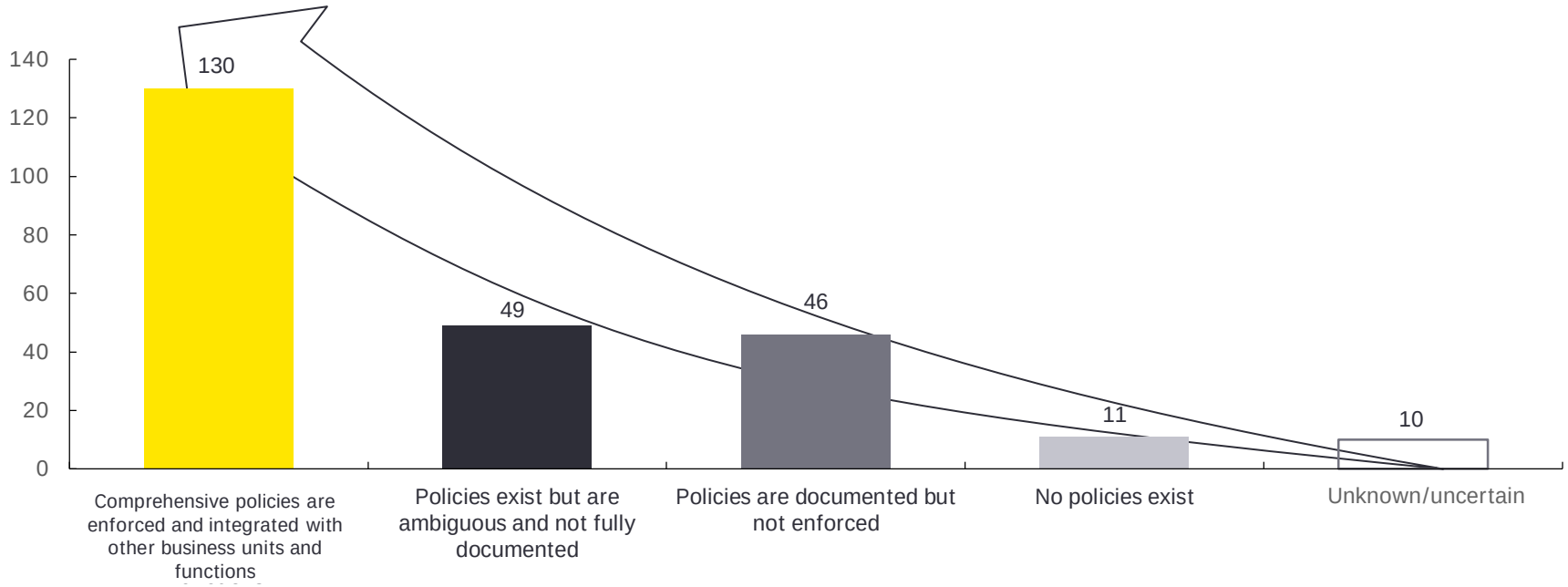
Note: Outlined percentages represent responses greater than 20%.



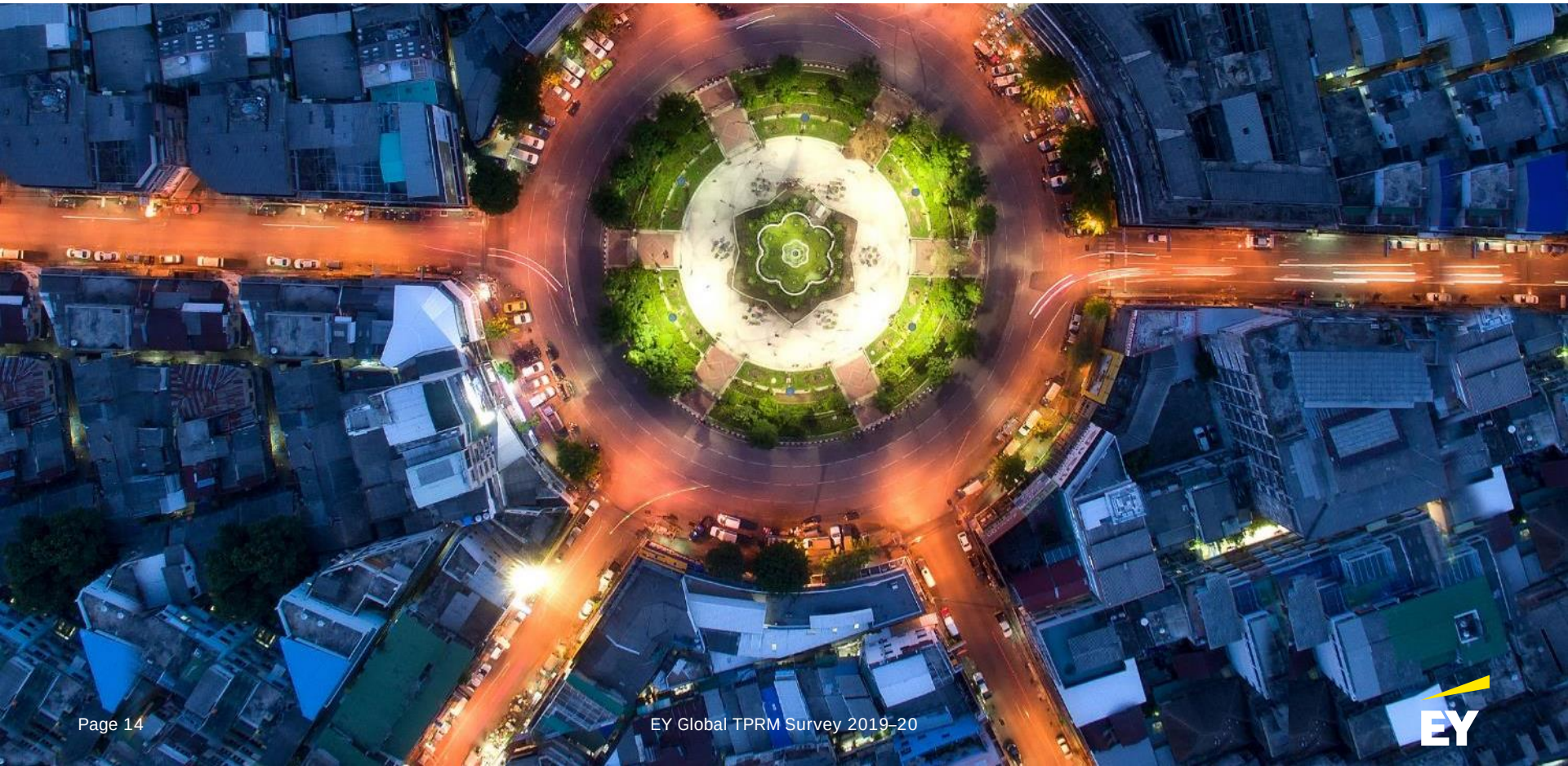
More than half of the organizations surveyed indicated they have comprehensive policies that are enforced and integrated; however, 39% indicated that policies are either documented but not enforced or exist but are not fully documented, indicating that there is a long way to go on the maturity curve for many organizations.

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



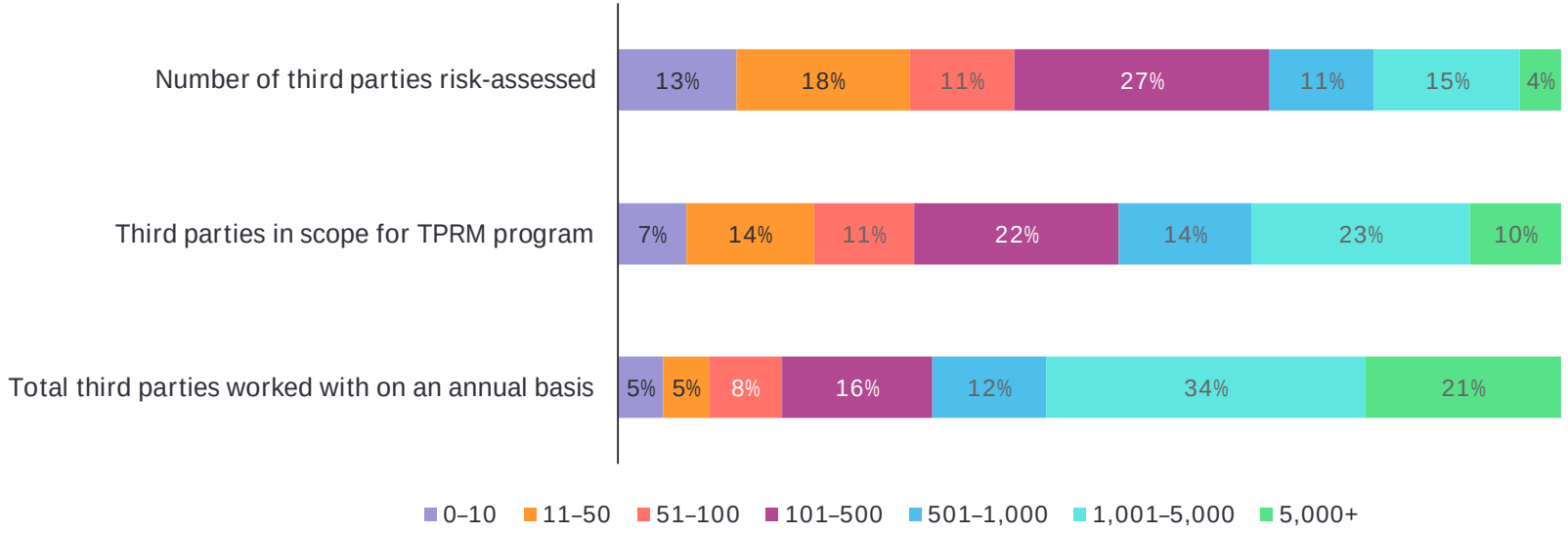
Contrary to previous years, when there was general consensus on the percentage of third parties subject to the TPRM program or a risk assessment, there is now more variability in the subsets of the overall inventory. This is likely due to continual challenges on totality of inventories and the changing environment of relevant risks.

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?

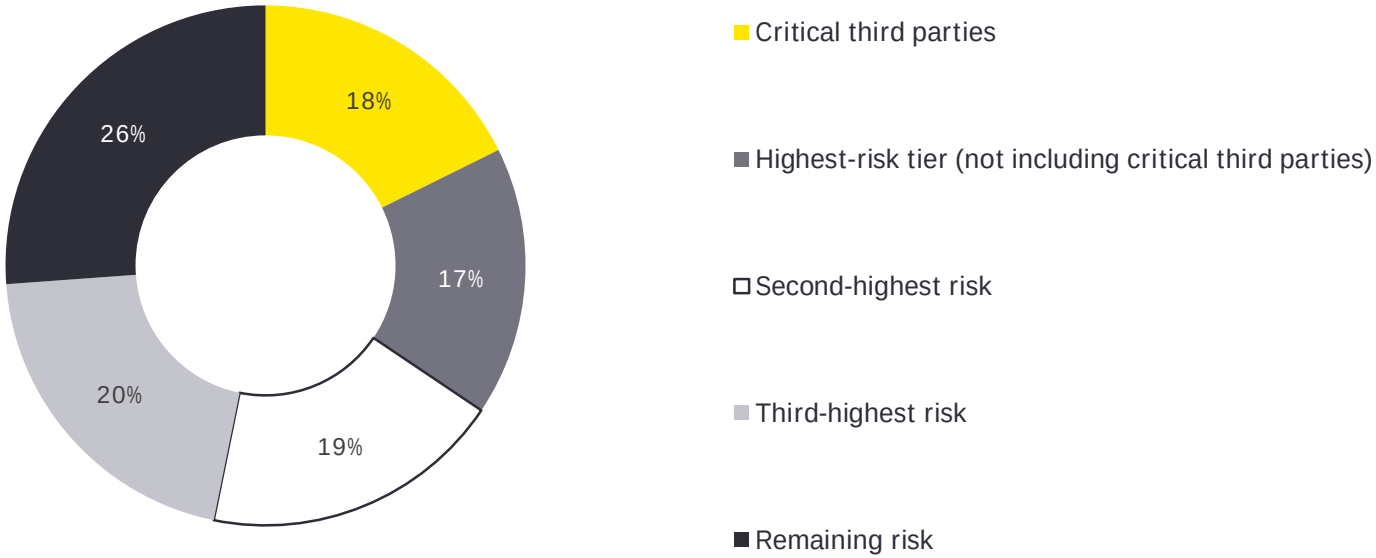


Third-party population breakdown/ risk tiering

In comparison with previous years, the nature of critical third parties is highly dependent on sector differences in maturity.

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%.

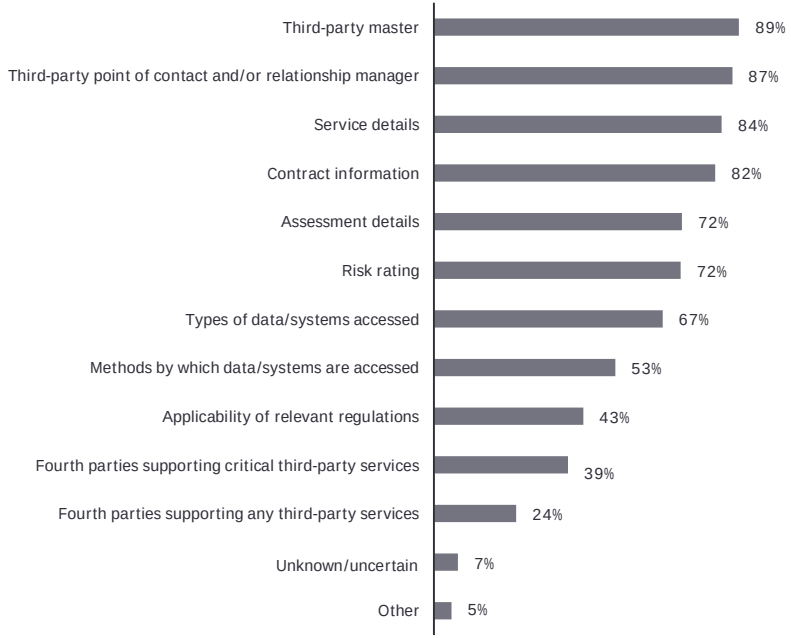


Third-party population breakdown/ risk tiering

In line with the previous slide, the criteria for criticality are highly dependent on sector, reducing the value of this data consolidated at a global level.

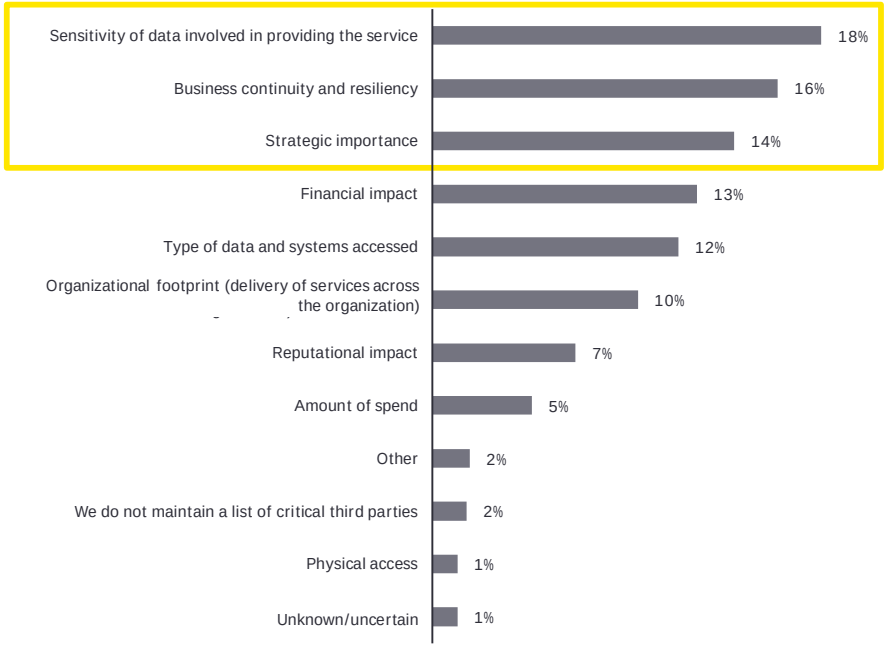
Information maintained

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

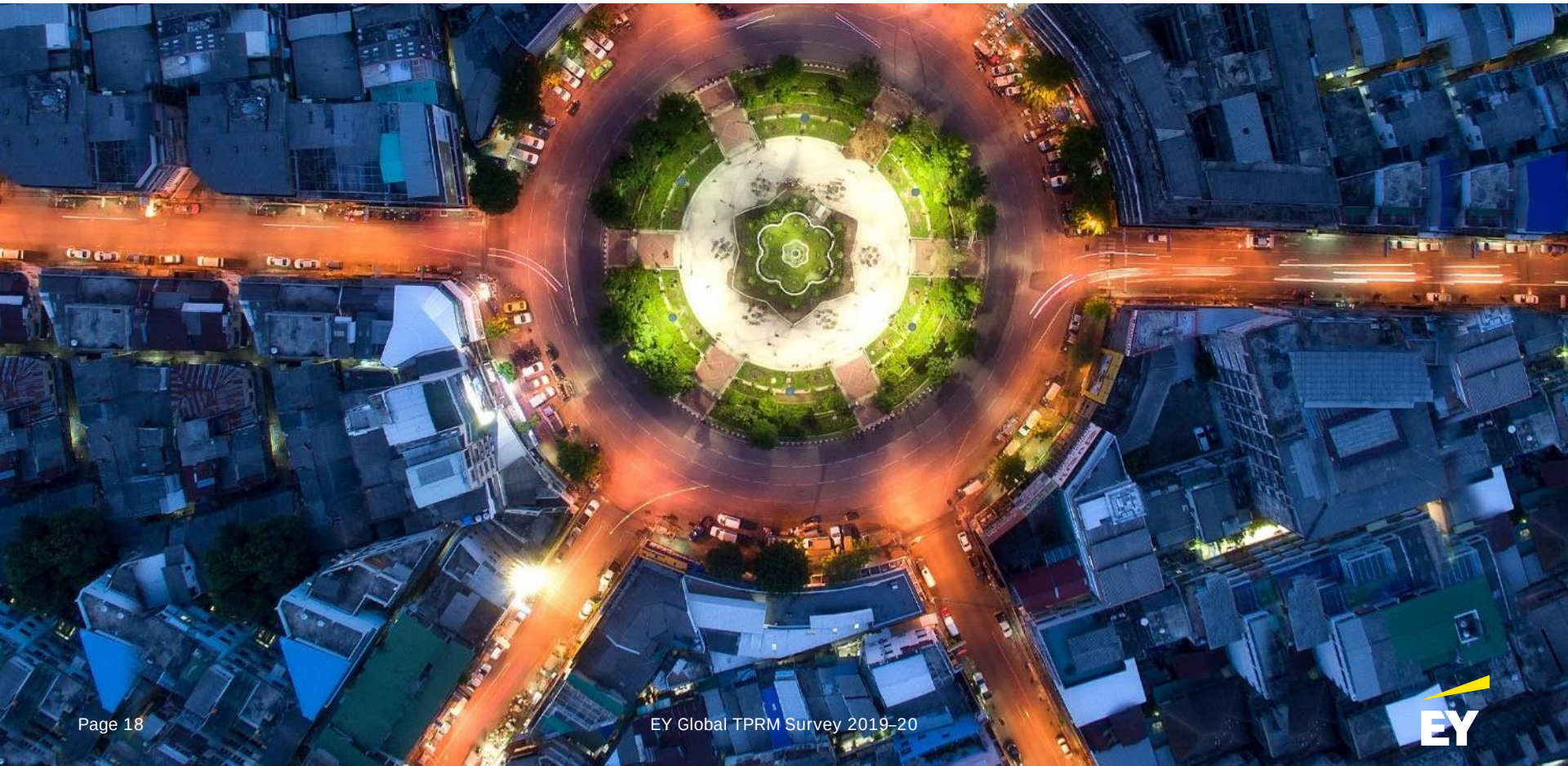


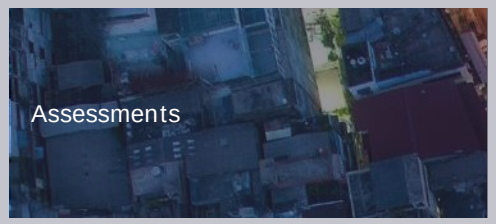
Critical third-party criteria

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



Assessments

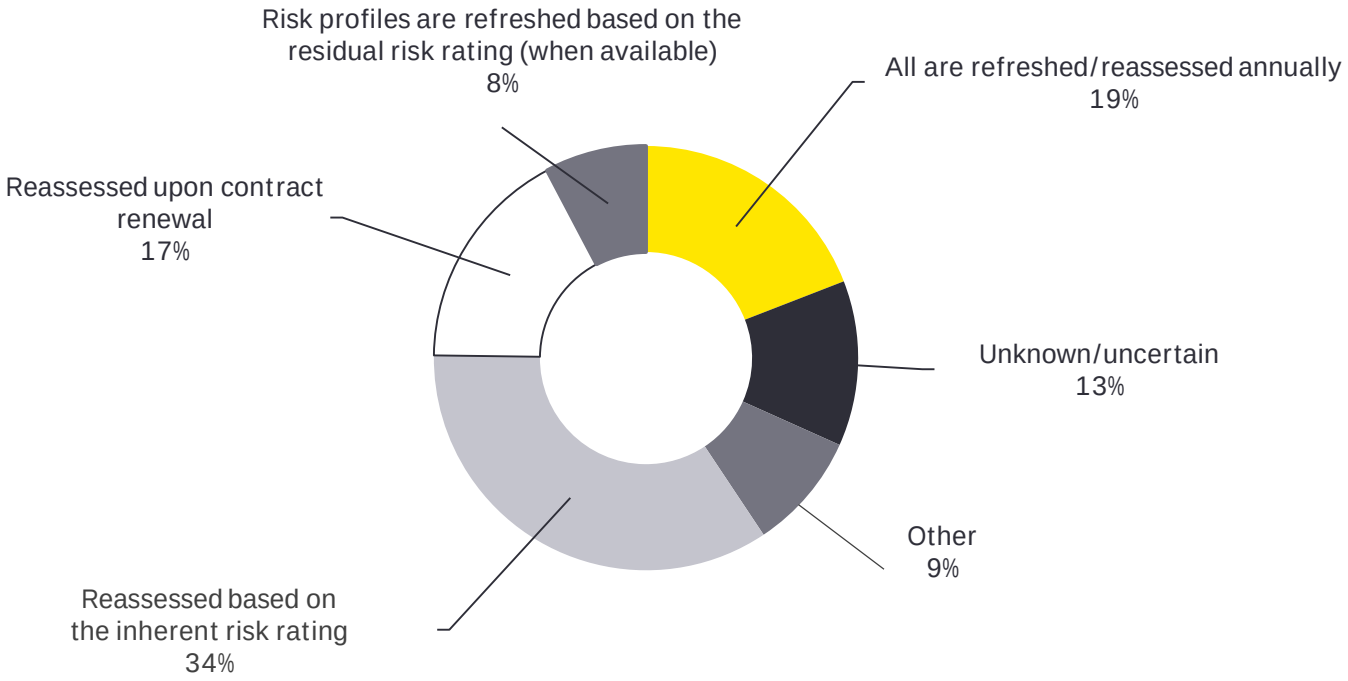


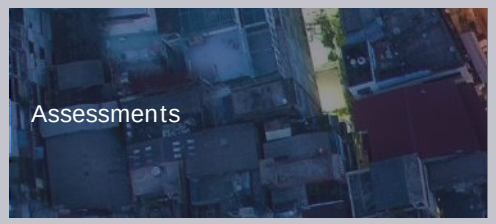


For nearly two in three organizations surveyed, the inherent risk profile of third parties is reassessed either based upon their inherent rating (e.g., only reassessing higher-risk third parties) or on a regular basis (e.g., annually) showing that continual refreshes do not always depend on a contract event.

Assessing inherent risk of third party

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

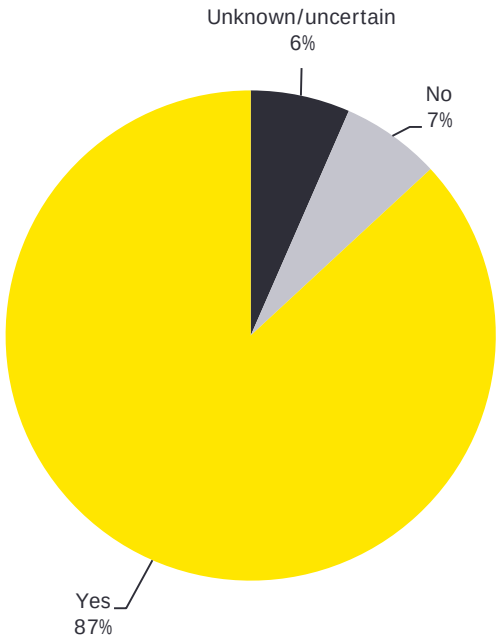




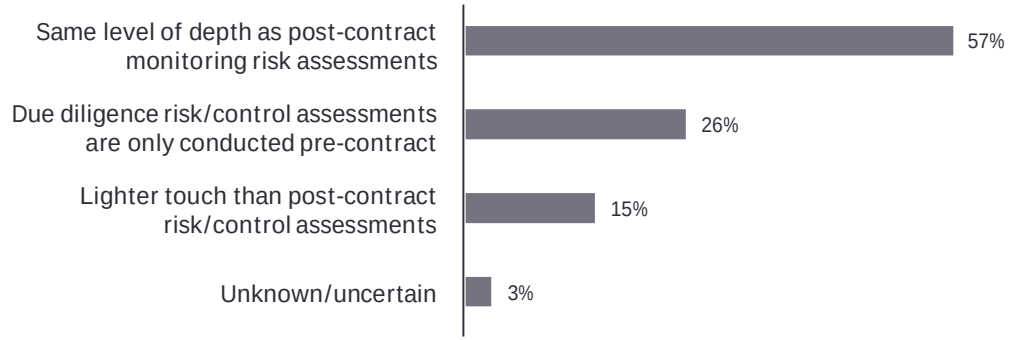
A majority of the organizations surveyed (81%) conduct some form of pre-contract due diligence risk assessment. For most of the organizations, the assessments are done at the same level of depth as post-contract monitoring assessments, raising the question of whether too much is being done before a contract is signed.

Pre-contract risk assessments

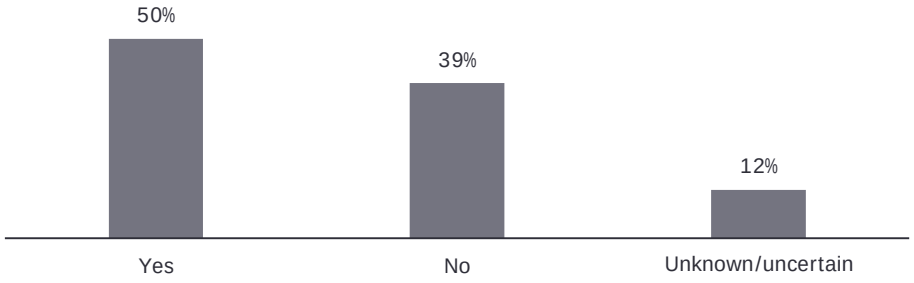
Q17. Does your organization currently conduct pre-contract due diligence risk assessments?

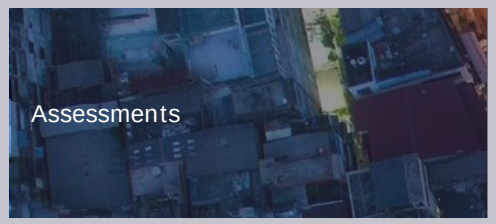


Q18. [If Yes to Q17] What level of depth is your organization's pre-contract due diligence risk/control assessment?



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





Based on survey responses, the typical pre- and post-contract risk assessment questionnaires typically have fewer than 200 questions. Cybersecurity and privacy risk account for almost half of all questions asked, aligning with respondents' answers to prior question on most important criteria of data sensitivity (Q15).

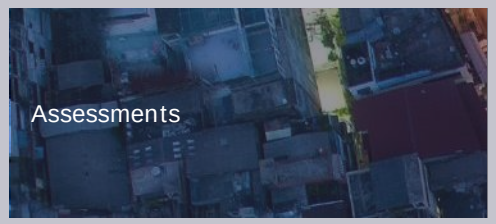
Risk assessment questionnaire

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	6.1	17.3	23.1
Strategic risk	1.7	1.9	5.1
Cybersecurity and privacy risk	26.8	57.9	72.5
Financial risk	2.6	4.0	15.9
Business continuity and resiliency	5.5	12.5	12.9
Geopolitical risk	1.0	1.1	1.8
Digital risk	1.6	4.2	16.4
Operational risk	3.2	6.5	27.1
Brand and reputational risk	1.9	2.0	3.0
Sustainability risk	0.7	1.3	13.2
Total	51.1	108.7	191.0

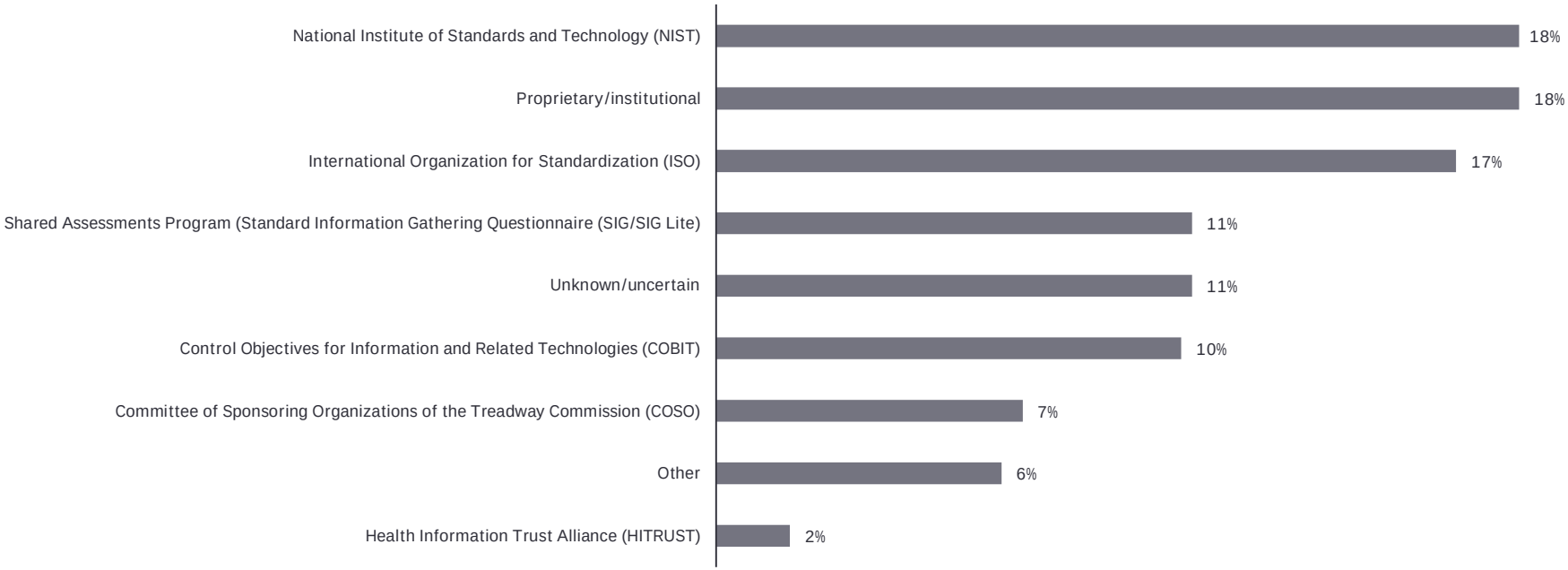
Note: Average number of questions outlined are greater than 25.

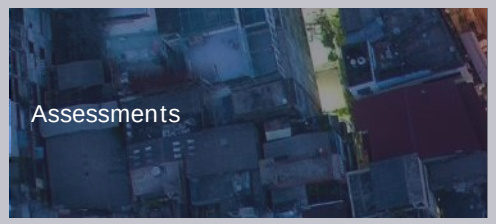


Over the past two to three years, there has been a significant uptick in the proportion of firms using NIST, although ISO and COBIT have also seen increased usage by organizations. By using industry-proven and trusted frameworks such as NIST, the organizations surveyed feel comfortable with using such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

Risk assessment questionnaire framework

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

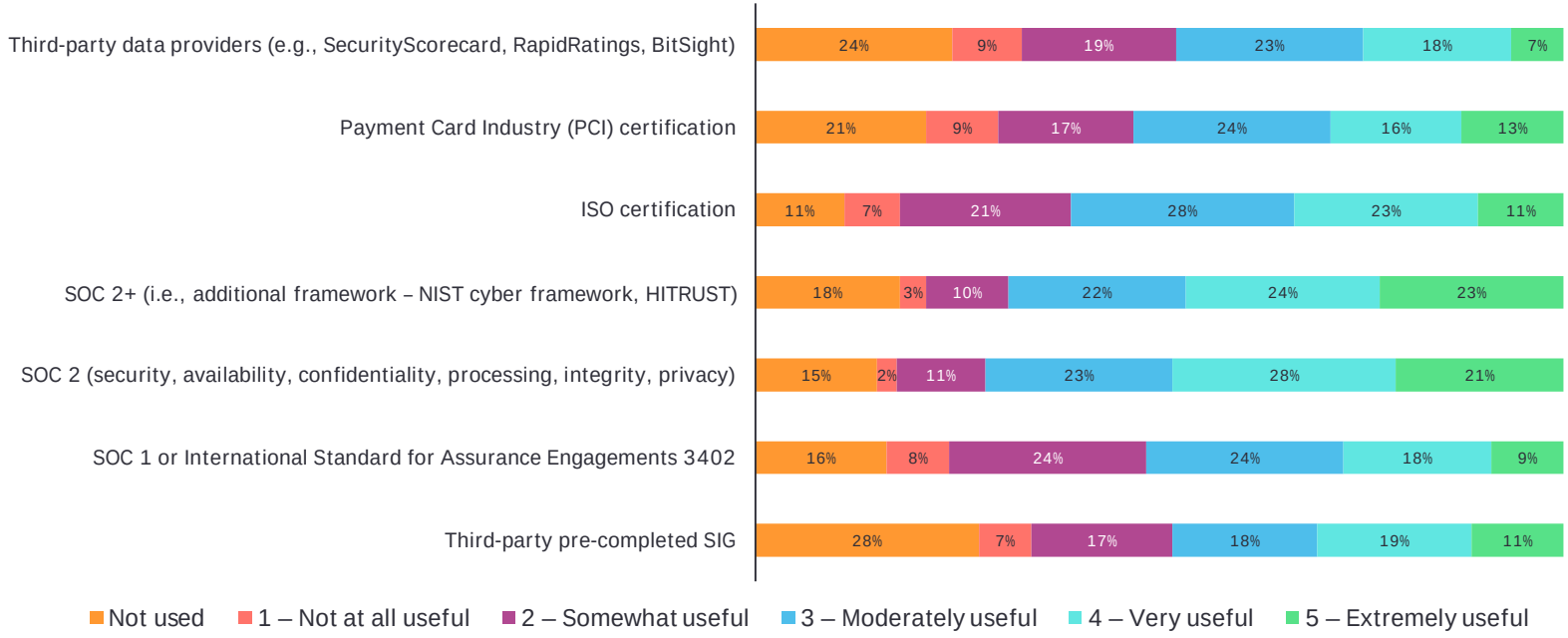


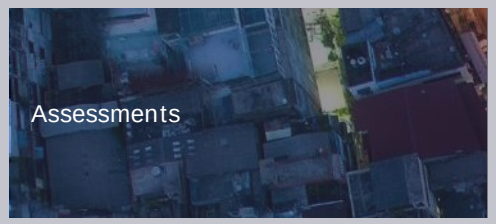


About half of the organizations surveyed found System and Organization Controls (SOC) 2 or SOC 2+ an additional framework to be useful, consistent with previous results. Other frameworks (ISO, PCI, etc.) are seen to be moderately less useful; however, organizations still have not found any frameworks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

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?





For third parties in the highest-risk tiers, reassessment is typically done every year, while for lower-risk third parties, reassessment is done less frequently, every three years or more.

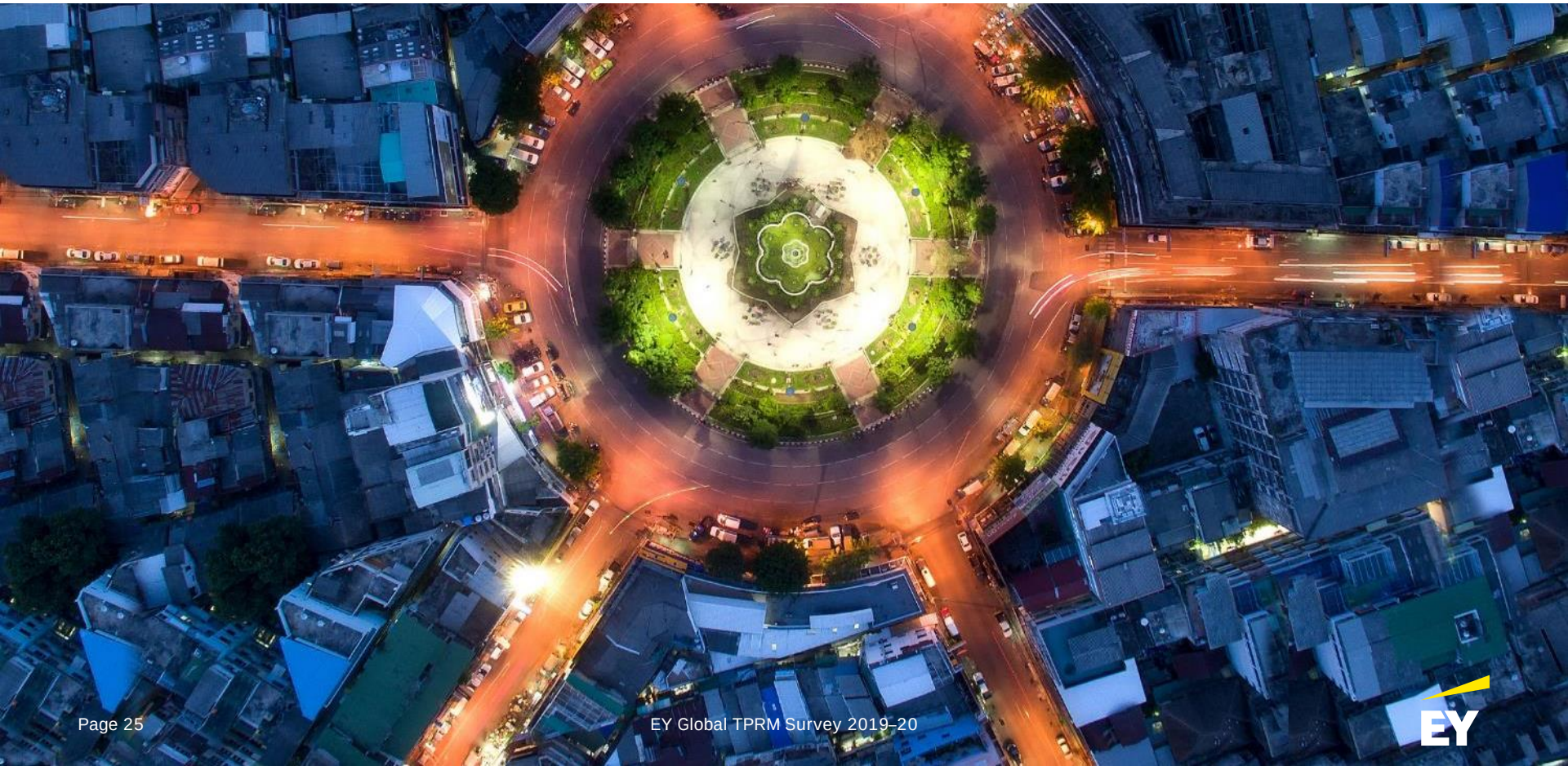
Frequency of performing third-party risk assessments

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%	76%	5%	6%	3%	0%
Highest risk	3%	52%	18%	7%	5%	14%
Second-highest risk	1%	22%	28%	19%	10%	20%
Third-highest risk	1%	15%	13%	30%	20%	22%
Remaining risk	1%	11%	6%	24%	35%	23%

Note: Outlined percentages are responses greater than 25%.

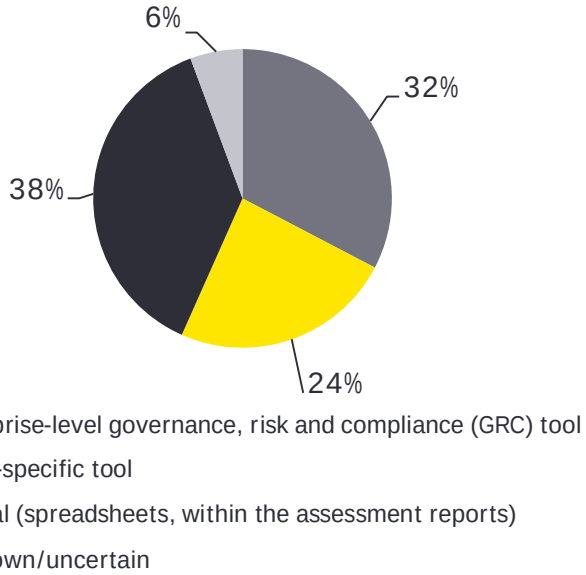
Issue management/risk treatment



For identified third-party issues in the critical-risk tier, termination and contractual changes are not uncommon outcomes, revealing that organizations use termination more often in the critical-risk tier than in the other tiers to resolve third-party issues despite the third party's significance to the organization. Action severity has a direct correlation to inherent risk.

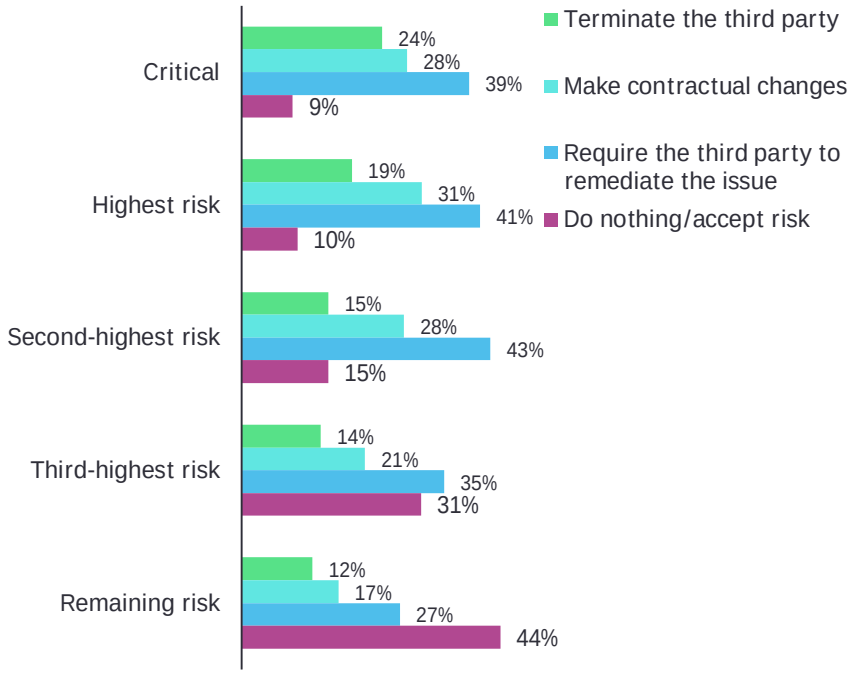
Issue tracking

Q24. How are issues and exceptions stored and tracked?



Actions for issues

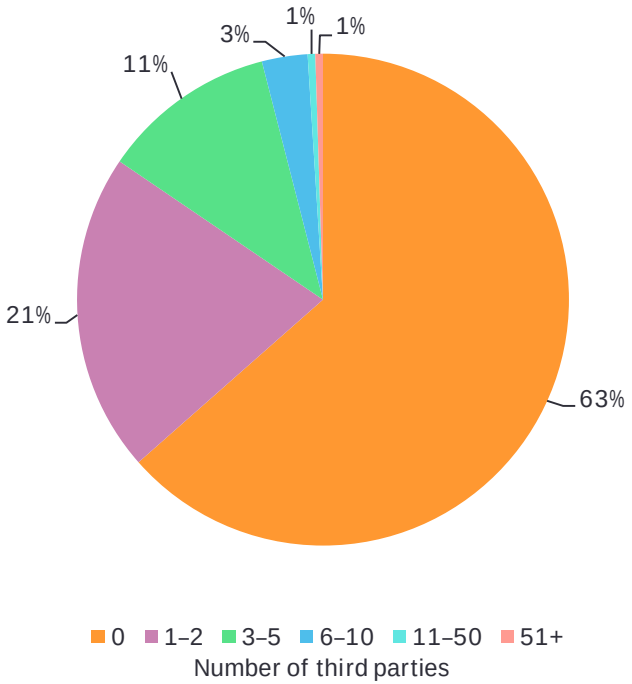
Q25. For third-party issues that you identify in each of the following risk tiers, what actions do you take?



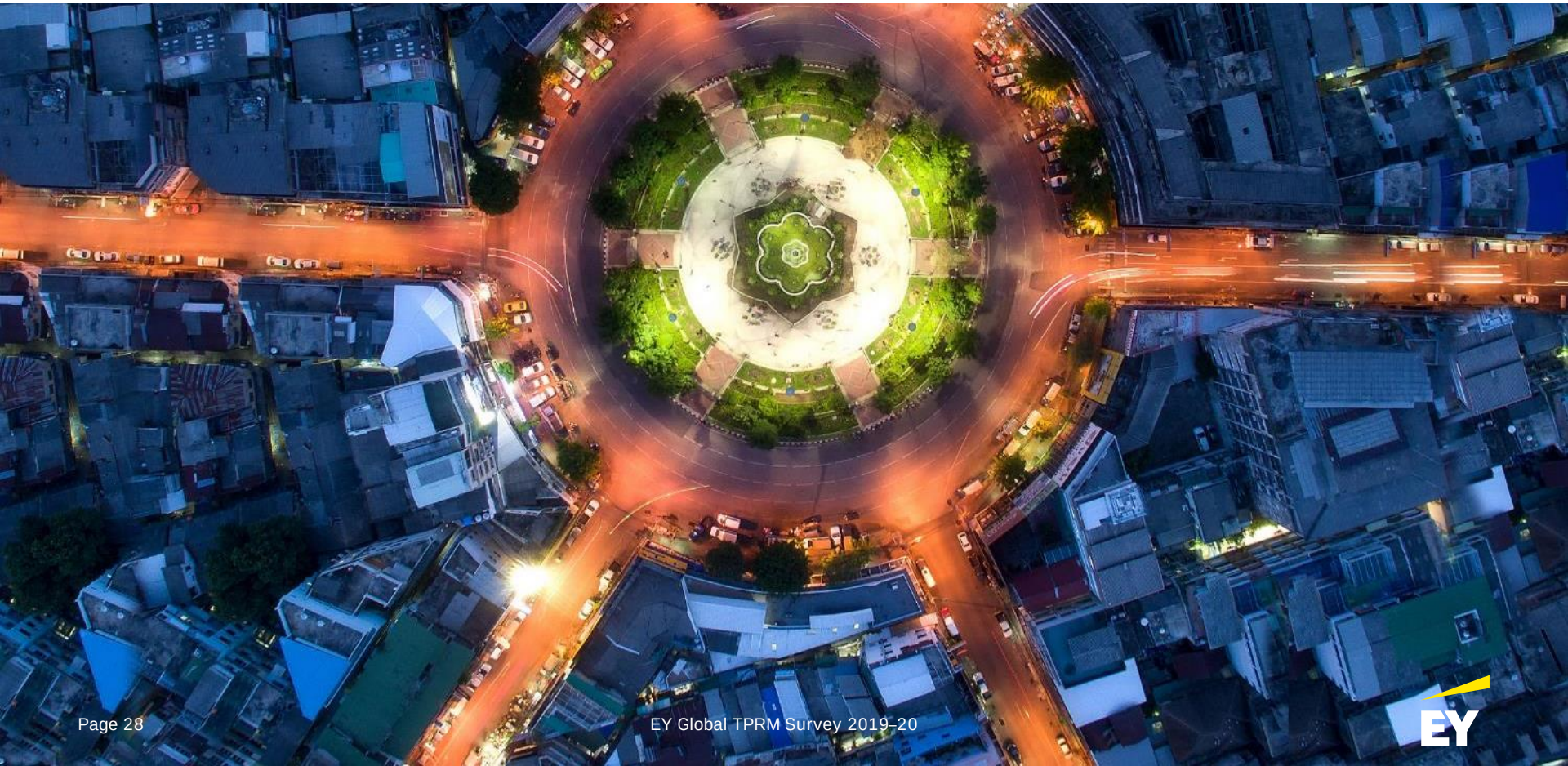
Correlating to the data on actions taken after issue identification (Q25), the most common action is remediation or contractual changes, and the majority of the organizations surveyed indicated that no third parties have been terminated due to issue identification. The remaining nearly one-third of the organizations terminated only one to five third parties, which is a small percentage since more than 50% of the organizations surveyed have more than 100 third parties in a TPRM program (Q12).

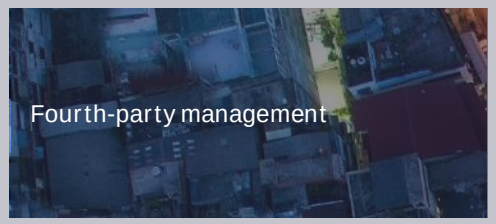
Termination of third parties due to issues

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



Fourth-party management

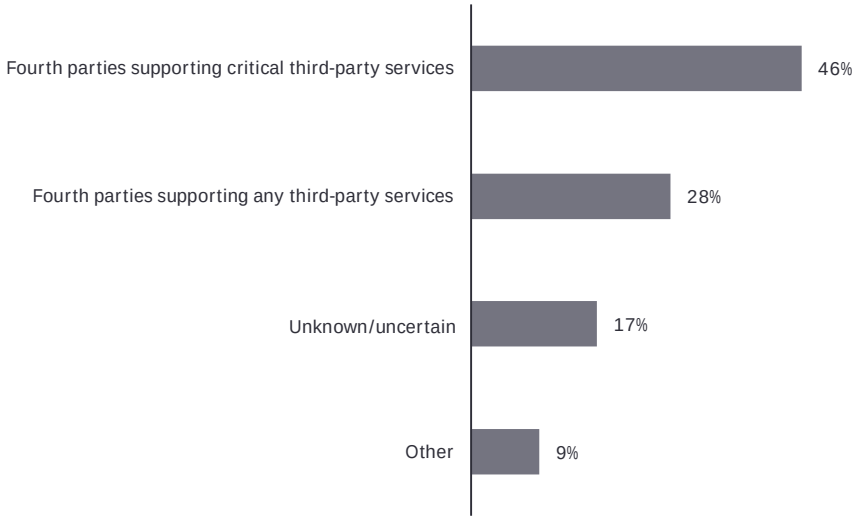




The majority of survey respondents (56%) collect information only on fourth parties that support critical third-party services. Only one in three of the organizations collect information on all fourth parties. Typically, fourth-party information is gathered during the risk/control assessment process. It is likely that privacy and global inventory expectations will increase the collection of fourth-party data in years to come.

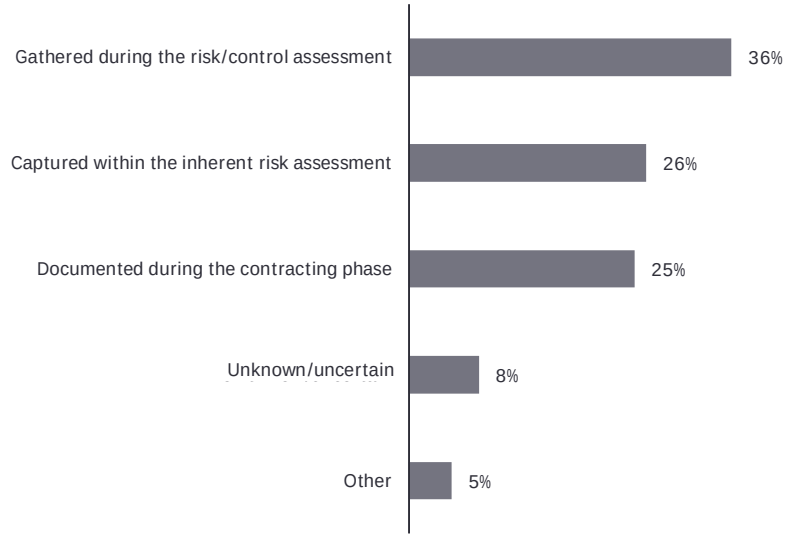
Fourth-party data collection

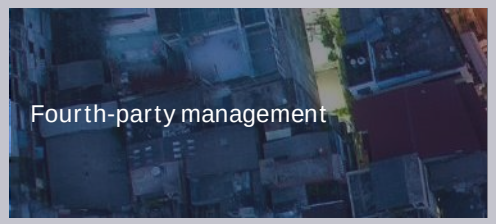
Q27. Which fourth parties/subcontractors does your organization collect information on?



Fourth-party data collection methods

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

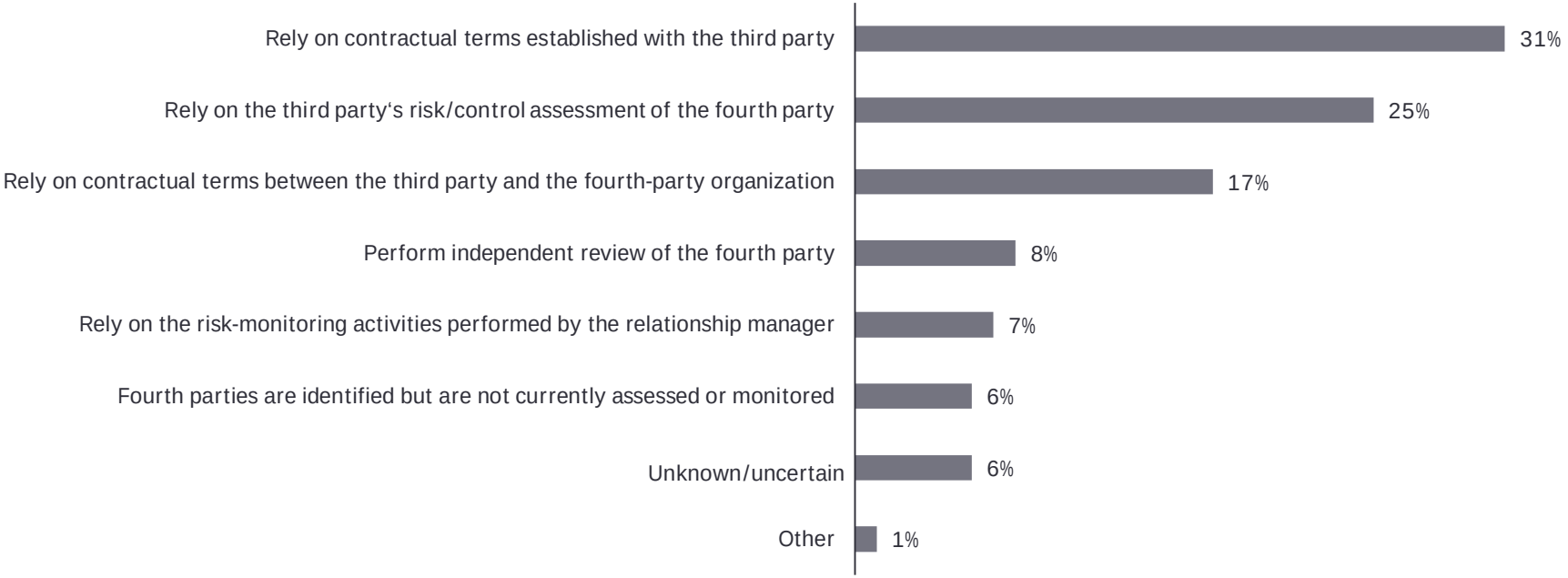




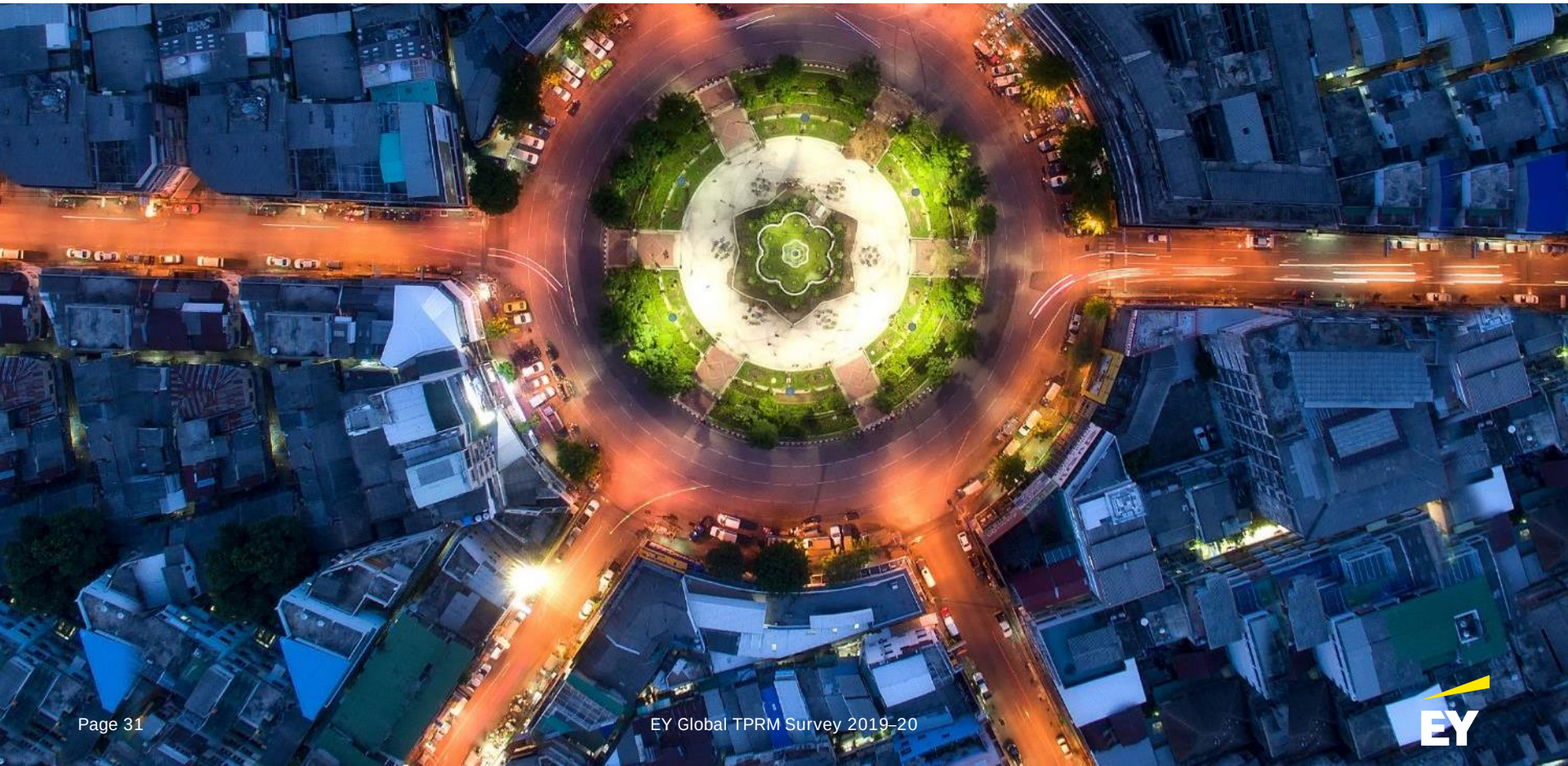
A meaningfully larger proportion of the organizations surveyed rely on contractual terms with their third parties for the purposes of overseeing/monitoring fourth parties. Increasingly, firms are also relying on contractual terms between the third and fourth party. Relatively few of the surveyed organizations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

Fourth-party monitoring

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



Technology



The organizations surveyed indicated that no tool or manual effort is used for approximately one-third of all functions to manage risk. Archer, SAP Ariba and other methods are used more frequently for the functions. Respondents indicated that other tools are used as well, 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?

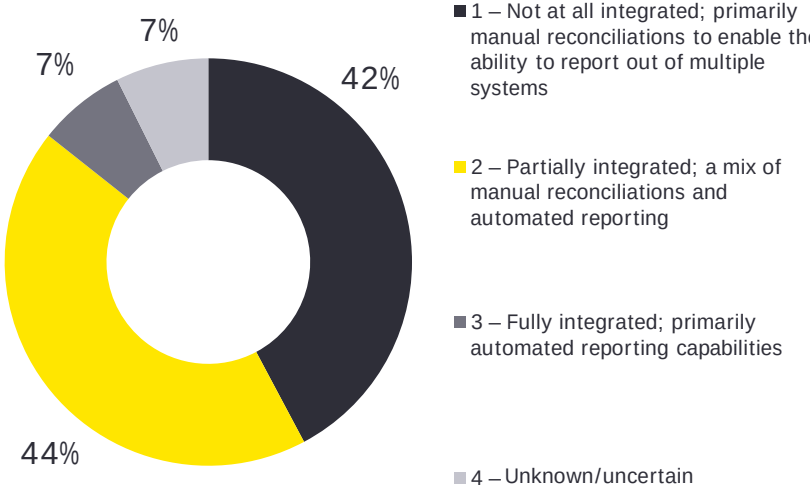
Function	No tool used (manual)	Archer®	Bwise®	Metric-Stream	SAP Ariba®	Hiperos®	Process Unity®	Prevalent®	Aravo	Service-Now	OneTrust	Lockpath	Proprietary	Other
Sourcing	34%	3%	0%	0%	29%	2%	1%	0%	0%	3%	0%	0%	8%	19%
Inherent risk assessment	31%	19%	0%	0%	2%	5%	6%	0%	2%	4%	1%	1%	14%	14%
Contract management	33%	5%	0%	1%	22%	2%	3%	0%	0%	2%	0%	1%	12%	22%
Primary third-party inventory	32%	15%	0%	0%	12%	3%	3%	0%	1%	4%	1%	0%	11%	17%
Risk/control assessment facilitation	29%	17%	1%	1%	3%	5%	7%	0%	2%	5%	2%	1%	11%	18%
Issue management	28%	20%	1%	1%	2%	2%	5%	0%	2%	8%	0%	1%	9%	18%

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

Among the surveyed organizations that use tools/technology as part of their TPRM programs, few note that a technology platform is fully integrated within the organization. Of the organizations that do have a technology platform, they are actively incorporating external data into their systems via application program interfaces (APIs). There is an opportunity for technology integration and platform adoption to enhance today's predominantly manual processes across TPRM as seen in the previous question (Q30).

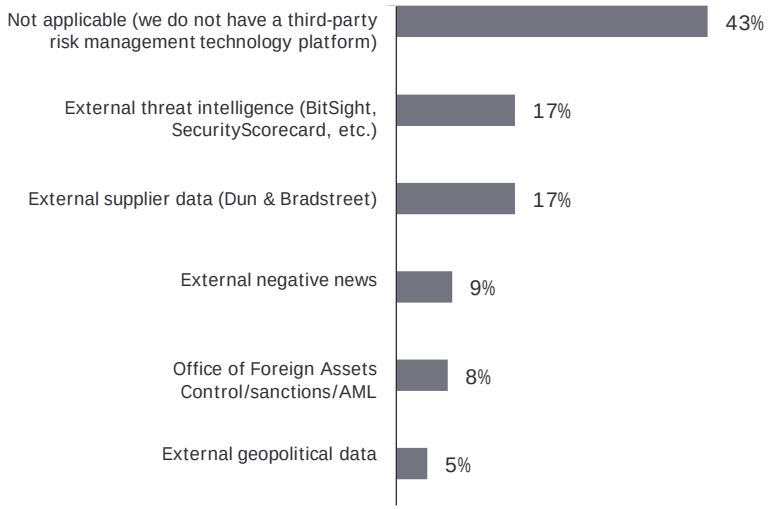
Technology integration

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

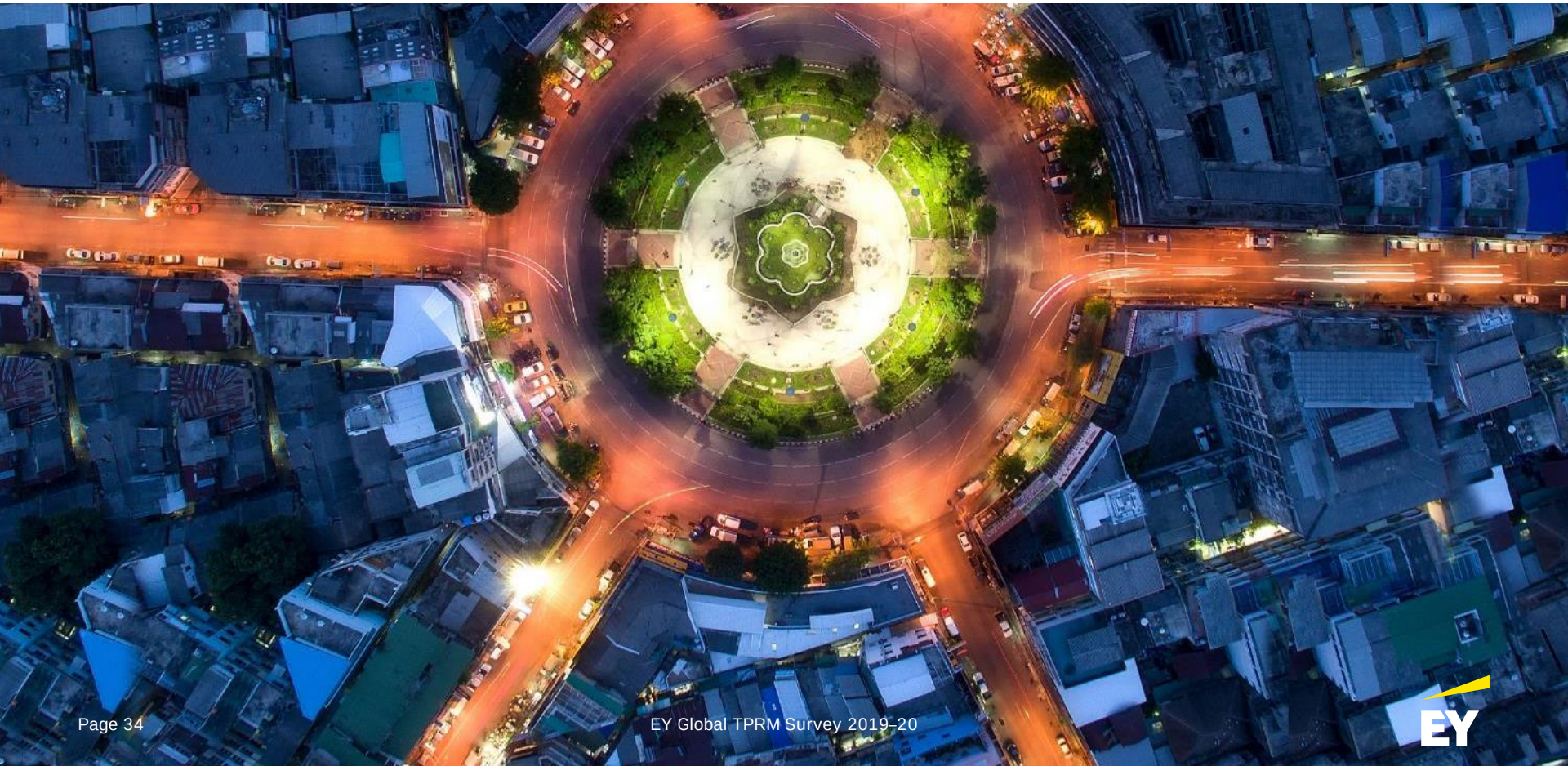


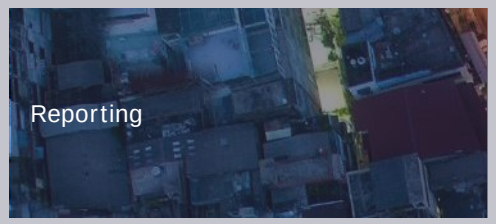
Technology integration

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 the surveyed organizations that report to the board about the TPRM program is still concerningly low. Typically, senior management is the highest level within the organization that receives regular reporting on most aspects of the TPRM program, and when it comes to critical third parties, only half of the organizations surveyed report on them to senior management or to business leadership. A sizable number of the organizations surveyed (upward of 20%) do not do any reporting on various aspects of their TPRM programs.

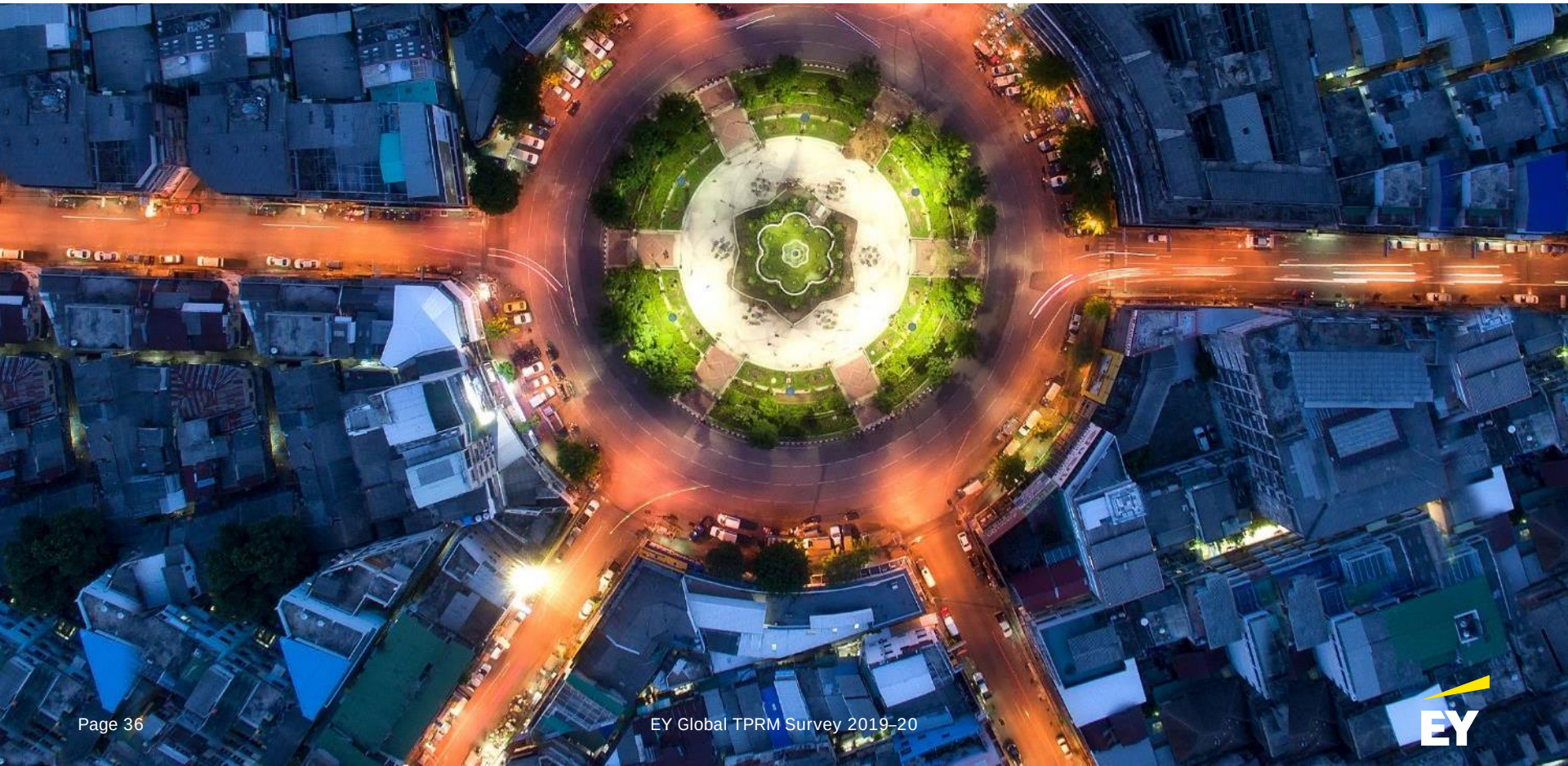
Reporting for TPRM

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	24%	48%	44%	36%	15%
KPIs/KRIs	22%	48%	43%	32%	15%
Third-party landscape	21%	43%	35%	28%	18%
Critical third parties	29%	54%	48%	33%	12%
Third parties with breaches or incidents	33%	60%	56%	40%	8%
Third parties with significant issues	24%	58%	58%	42%	9%
Third parties terminated prior to contract end date	11%	32%	40%	30%	20%

Note: Outlined percentages are greater than 50%.

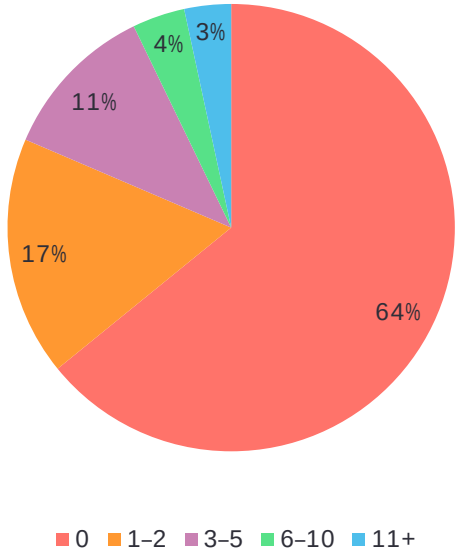
Cybersecurity and threat intelligence



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

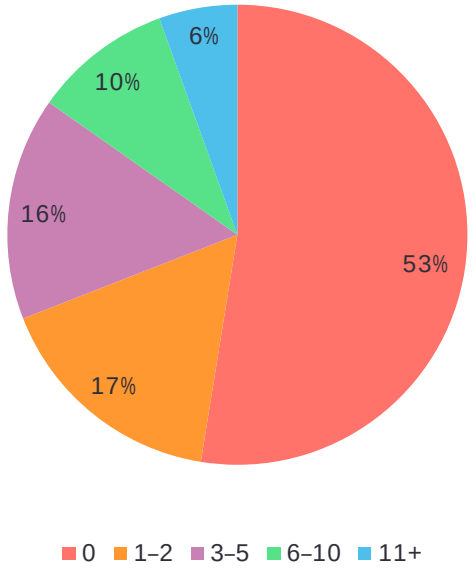
Data breaches caused by third parties

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



Outages caused by third parties

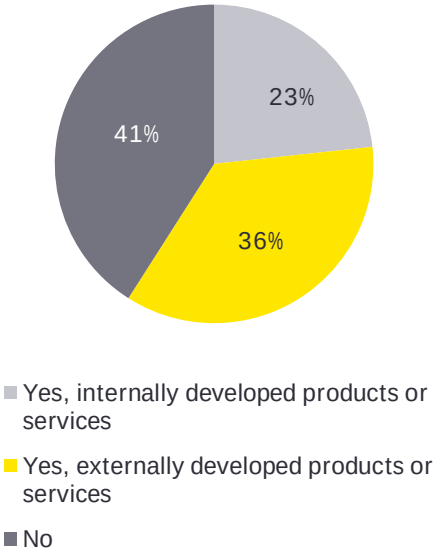
Q35. Over the past two years, how many outages have been caused by third parties?



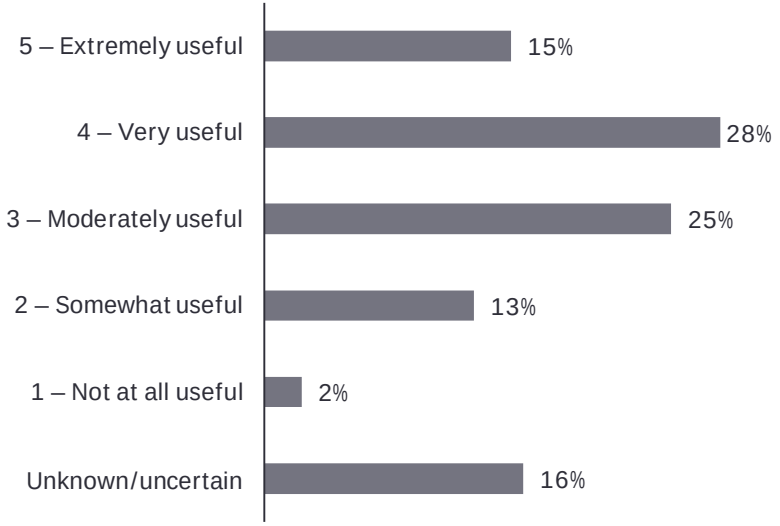
Despite the significant number of the organizations surveyed that have suffered a breach, nearly half of them do not utilize threat intelligence tools. This may be driven by the fact that only half found threat intelligence tools to be very useful at driving risk-based ongoing oversight activity, showing a low degree of valuable integration with threat intelligence tools.

Threat intelligence

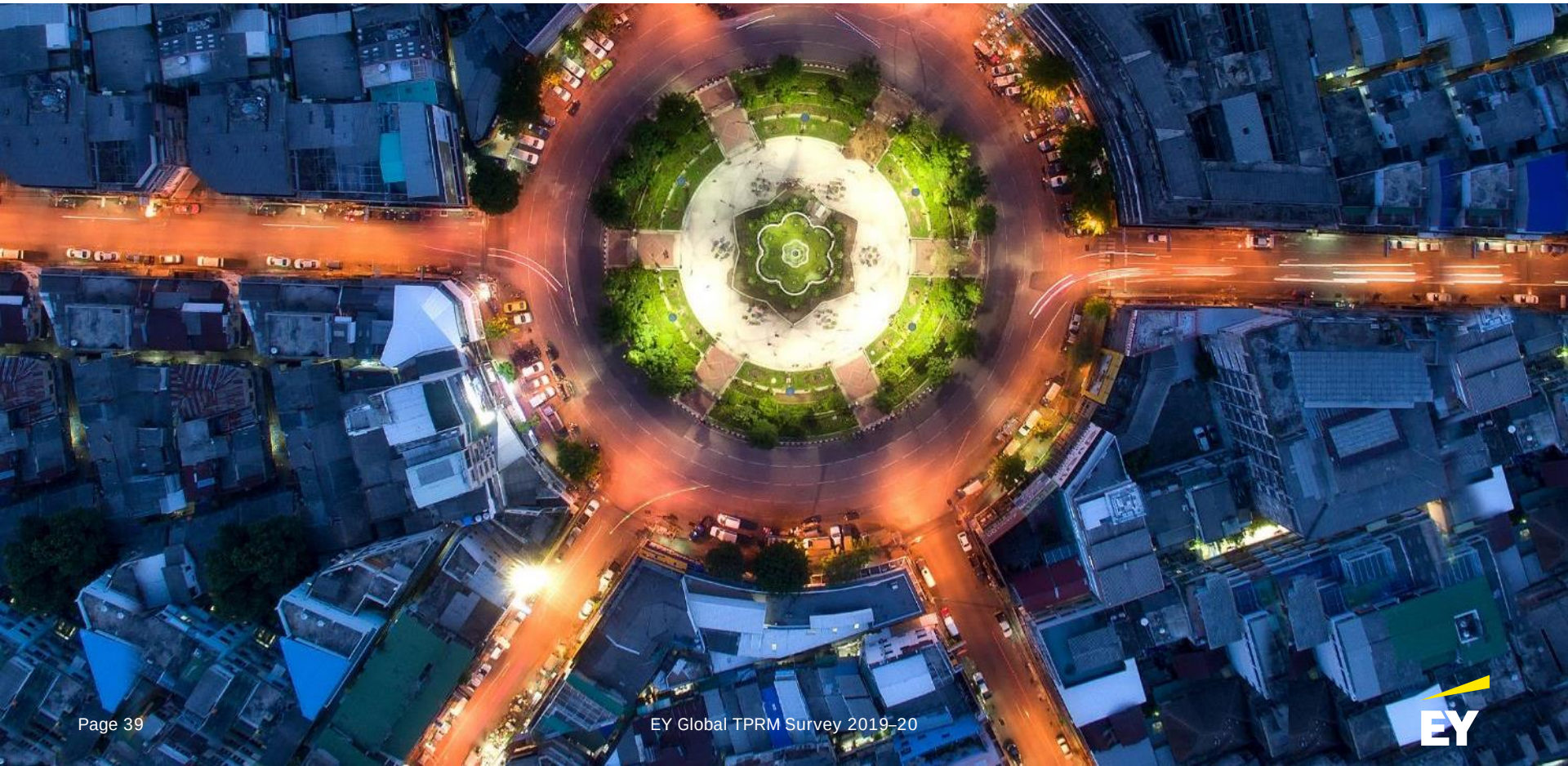
Q36. Does your organization utilize threat intelligence products or services to continuously monitor the cybersecurity environment of your third-party providers?

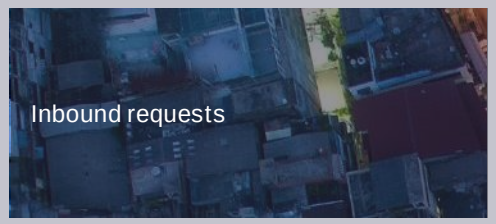


Q37. [For those who answered Yes] On a scale of 1 to 5, with 1 being not at all useful and 5 being extremely useful, how useful are threat intelligence tools at driving risk-based ongoing oversight activity?



Inbound requests

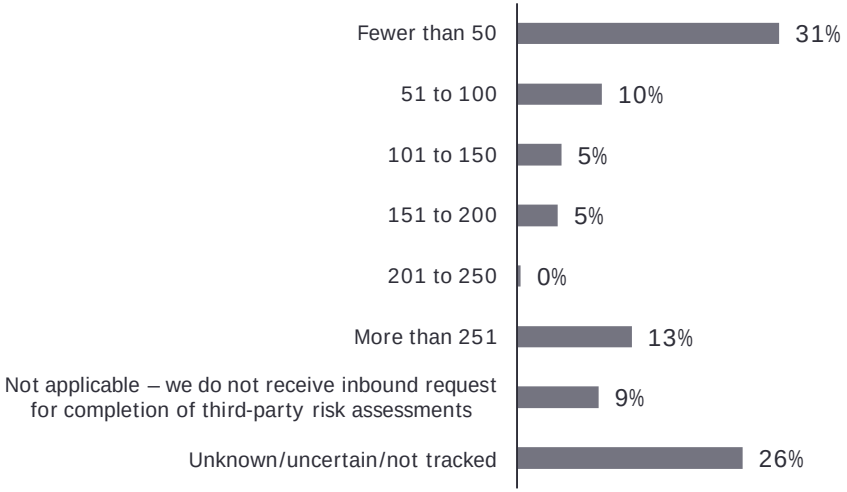




A third of the organizations surveyed facilitate more than 50 inbound assessments per year, and an additional quarter of participants don't even know if they are being assessed, showing a disconnect between inbound request management and internal risk management functions.

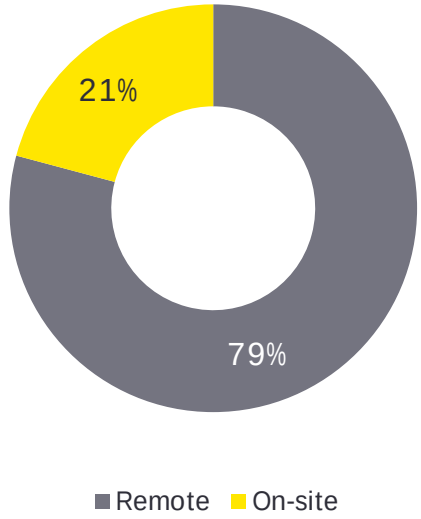
Inbound requests for TPRM

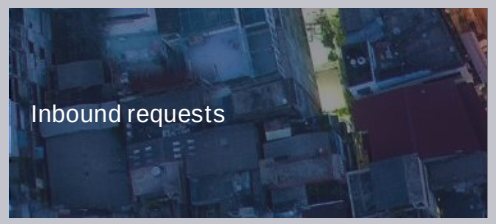
Q38. Approximately how many inbound requests for completion of third-party risk assessment questionnaires does your organization receive annually?



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%.

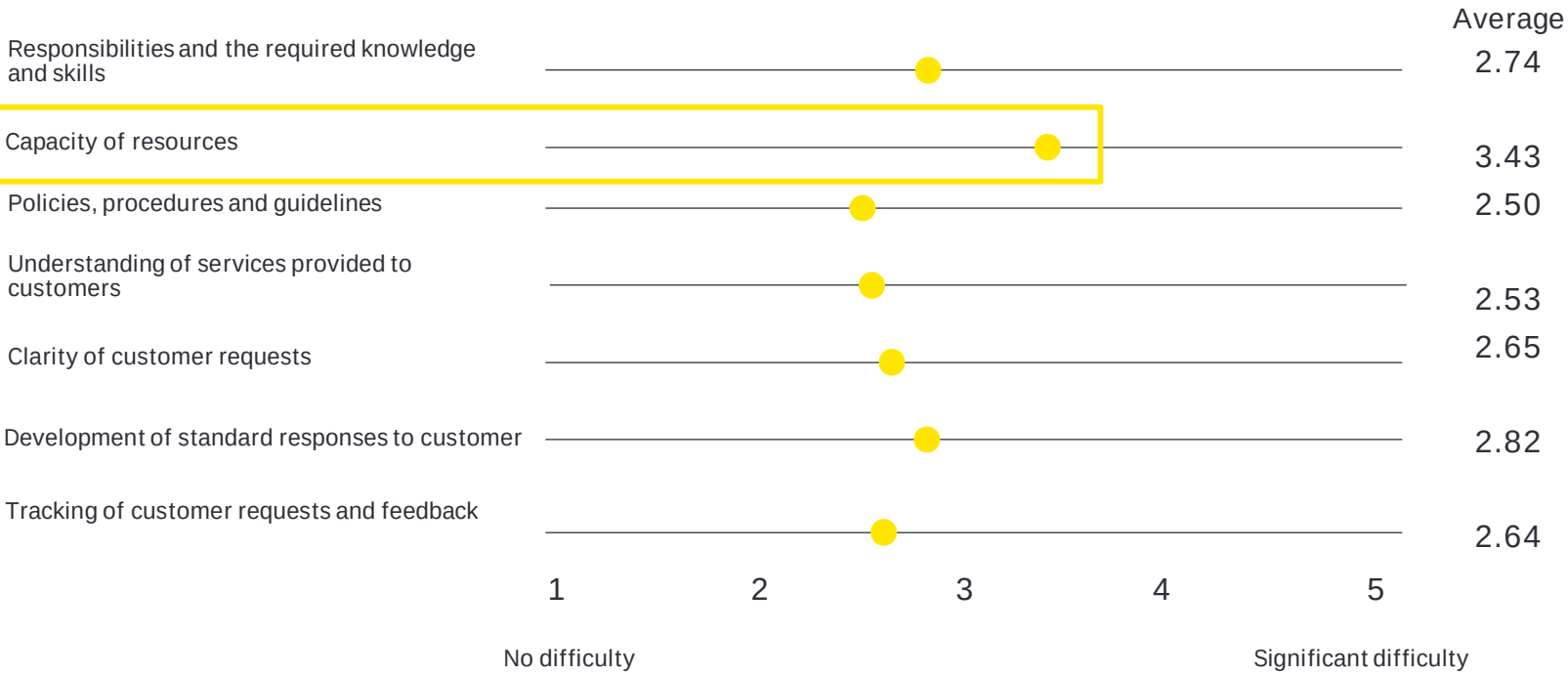




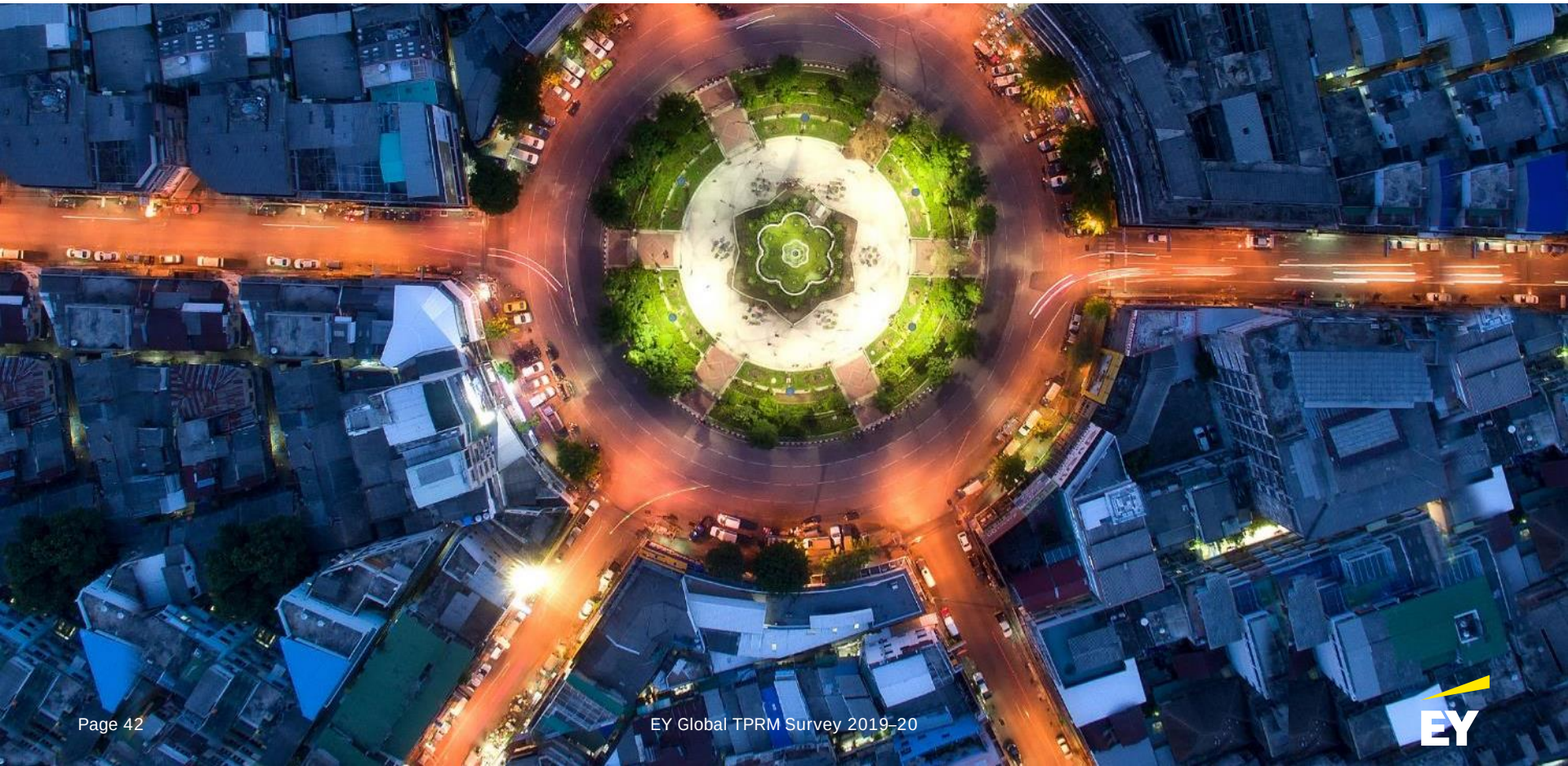
When it comes to inbound requests, more than half of the organizations surveyed noted that resource constraints presented a significant challenge. This is in alignment with organizations, indicating that they plan to use more internal resources for TPRM execution in next two to three years (Q7).

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?



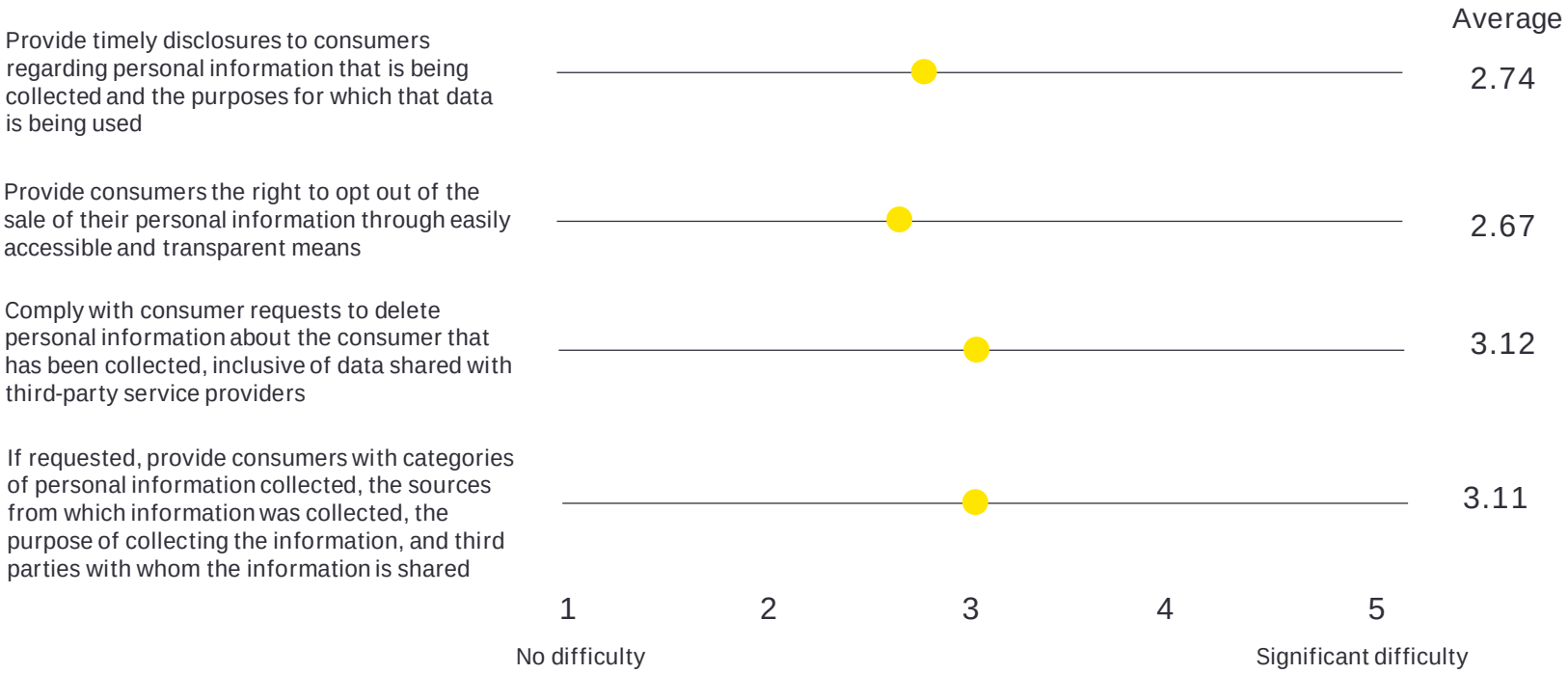
Privacy regulations



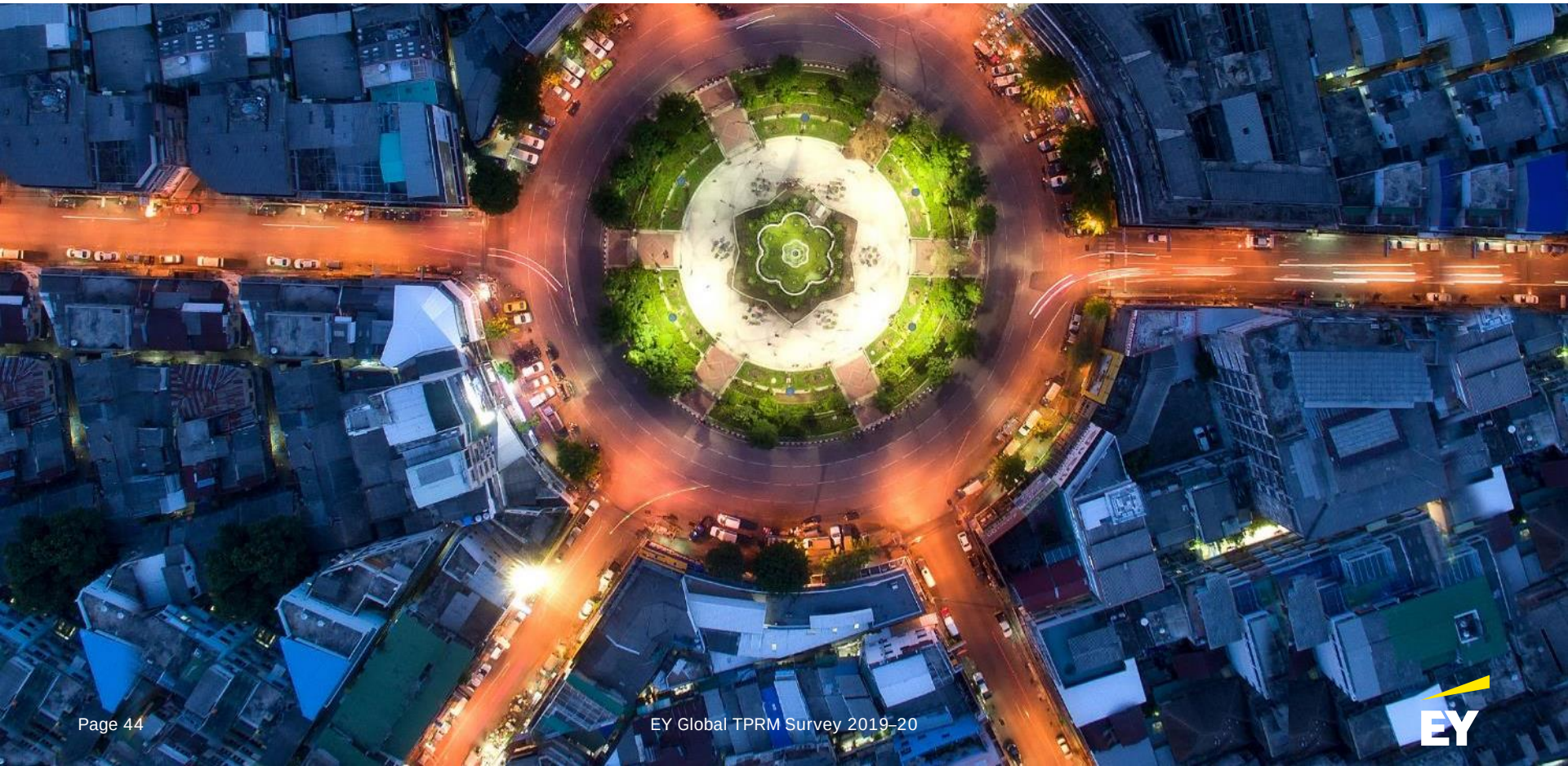
Organizations are not yet fully prepared to address all aspects of recent privacy regulations (CCPA, GDPR, etc.). In particular, the organizations surveyed feel it will prove challenging to provide customers the right to opt out of the sale of their personal information and provide timely disclosures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

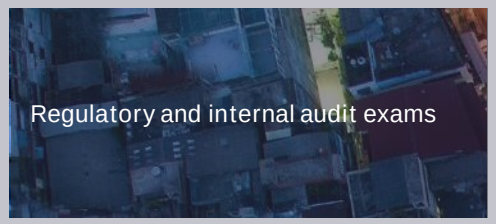
Privacy regulations in TPRM

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





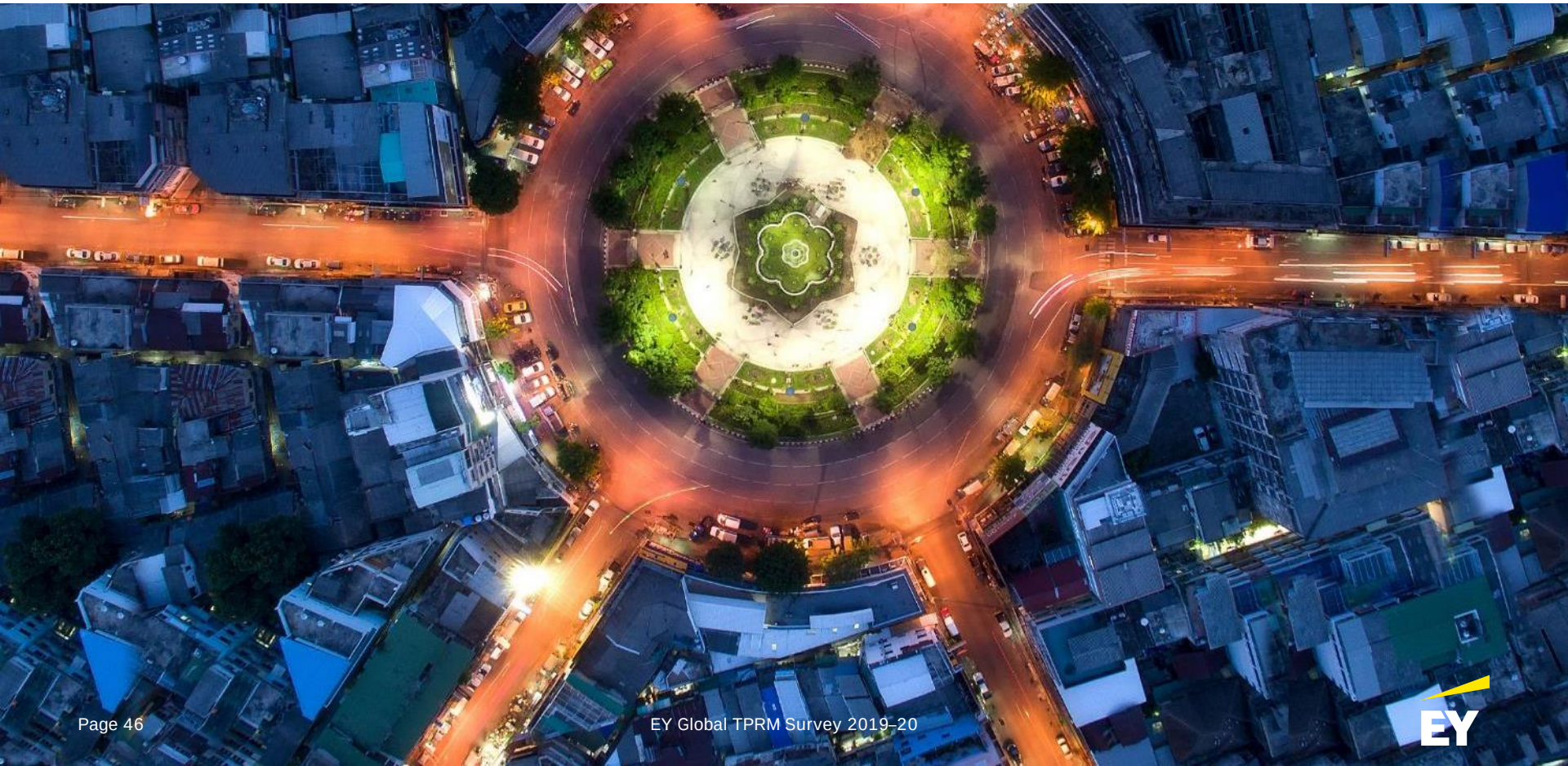
As with previous years, oversight and governance was the dominant area of focus among the organizations surveyed, with cybersecurity following in both areas and enterprise-critical third parties following for regulatory body and onboarding activities following for internal audit.

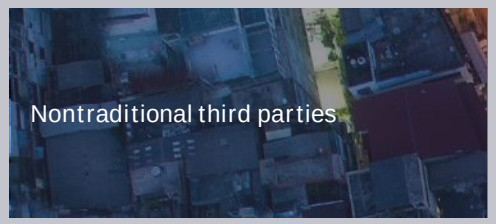
Areas of focus during regulatory body review and internal audit

Q42. During your organization's most recent regulatory body review and most recent internal audit of your third-party risk management program/function, what were the two to three most important areas of focus? Please select no more than three.

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

Nontraditional third parties





Of the organizations surveyed, the most likely nontraditional third parties to be covered by TPRM are strategic partnerships, insurance carriers and law firms providing outside legal counsel. The most likely not to be covered by TPRM are landlord premises, charitable organizations and pension plans.

Nontraditional third parties

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

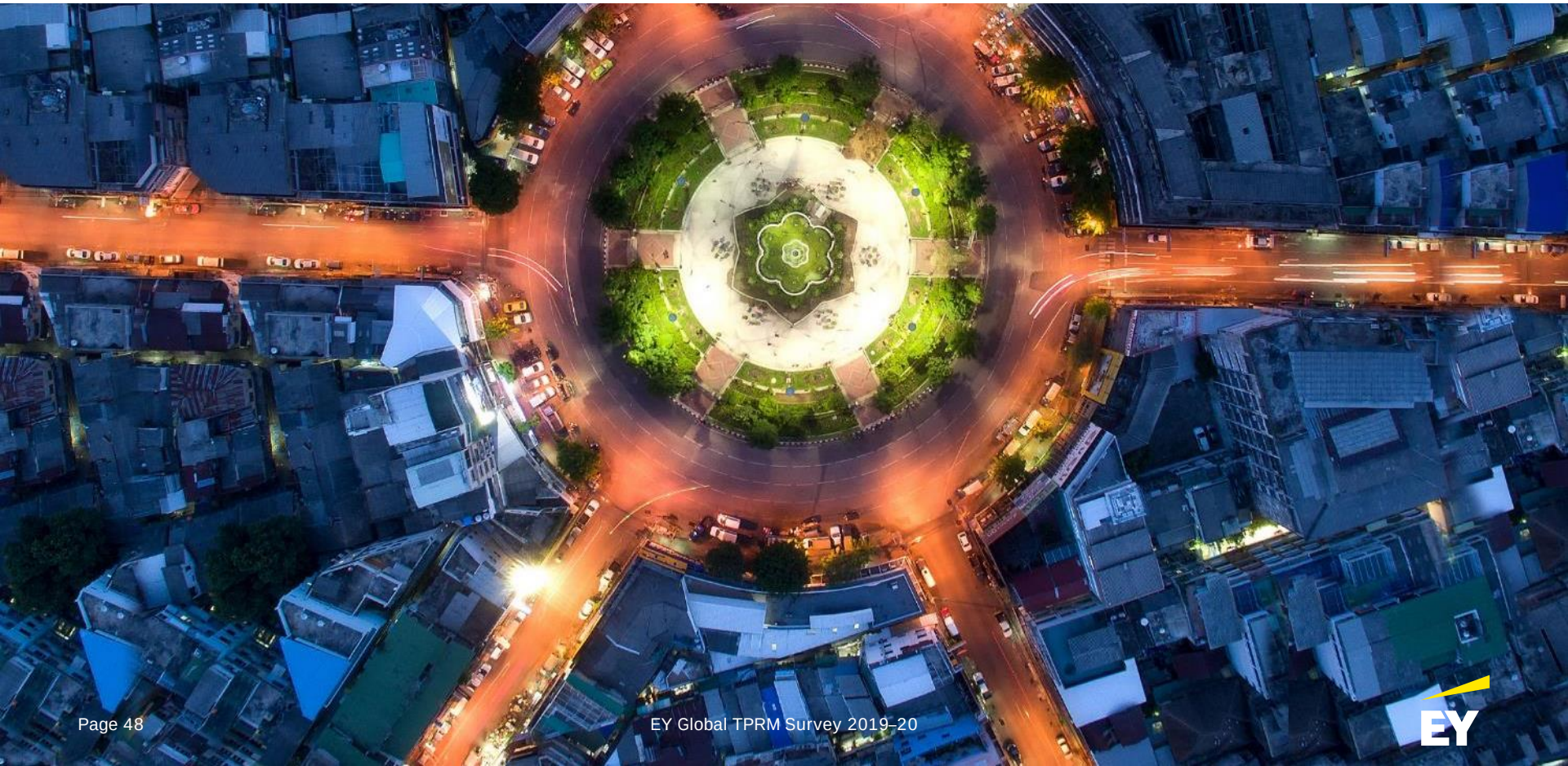
Nontraditional third parties*

Strategic partnerships	Law firms providing outside legal counsel (litigation)	Insurance carriers	Joint ventures
29% / 56% / 15%	29% / 49% / 22%	29% / 51% / 20%	38% / 42% / 19%
Pension plans	**Landlord premises**	**Broker dealers**	**Charitable organizations**
40% / 46% / 14%	29% / 51% / 20%	35% / 43% / 22%	31% / 46% / 23%

Covered by TPRM | Covered by specialized program | Not covered

* Results shown for the most common nontraditional third parties based on survey results.

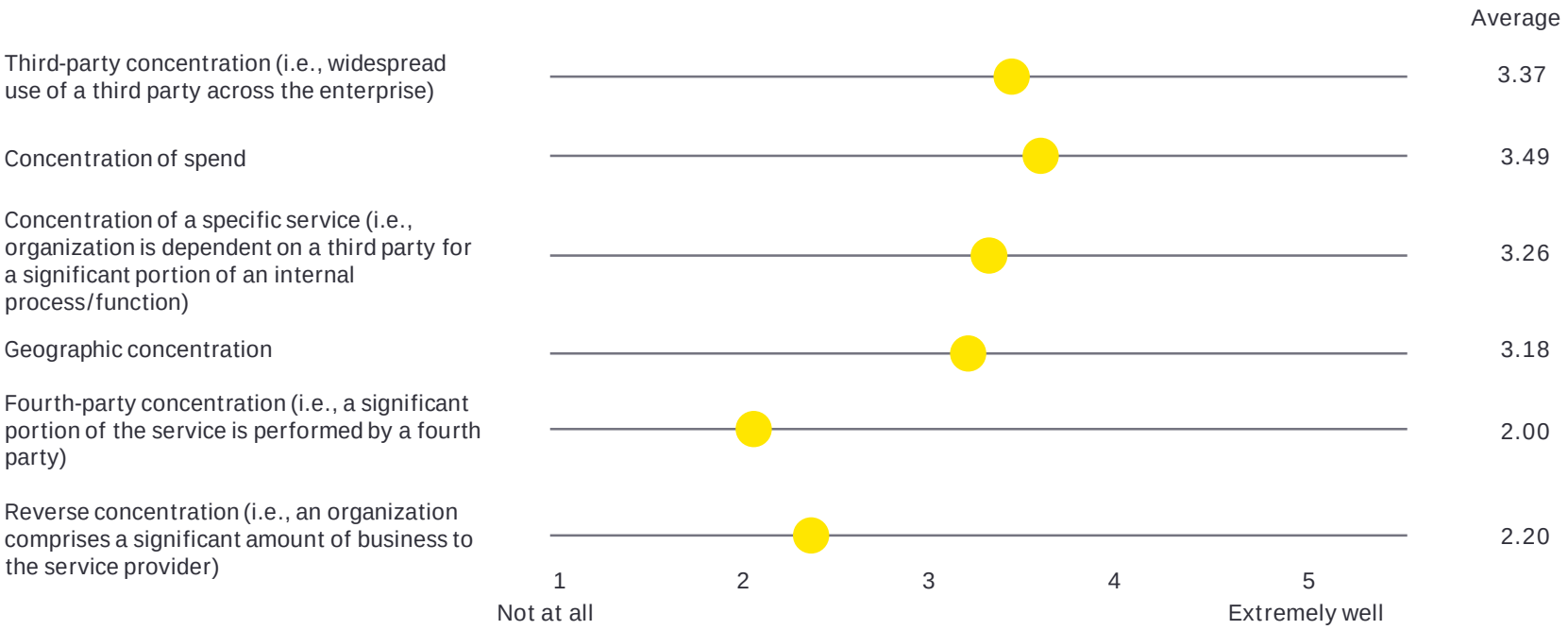
Concentration risks (financial services only)



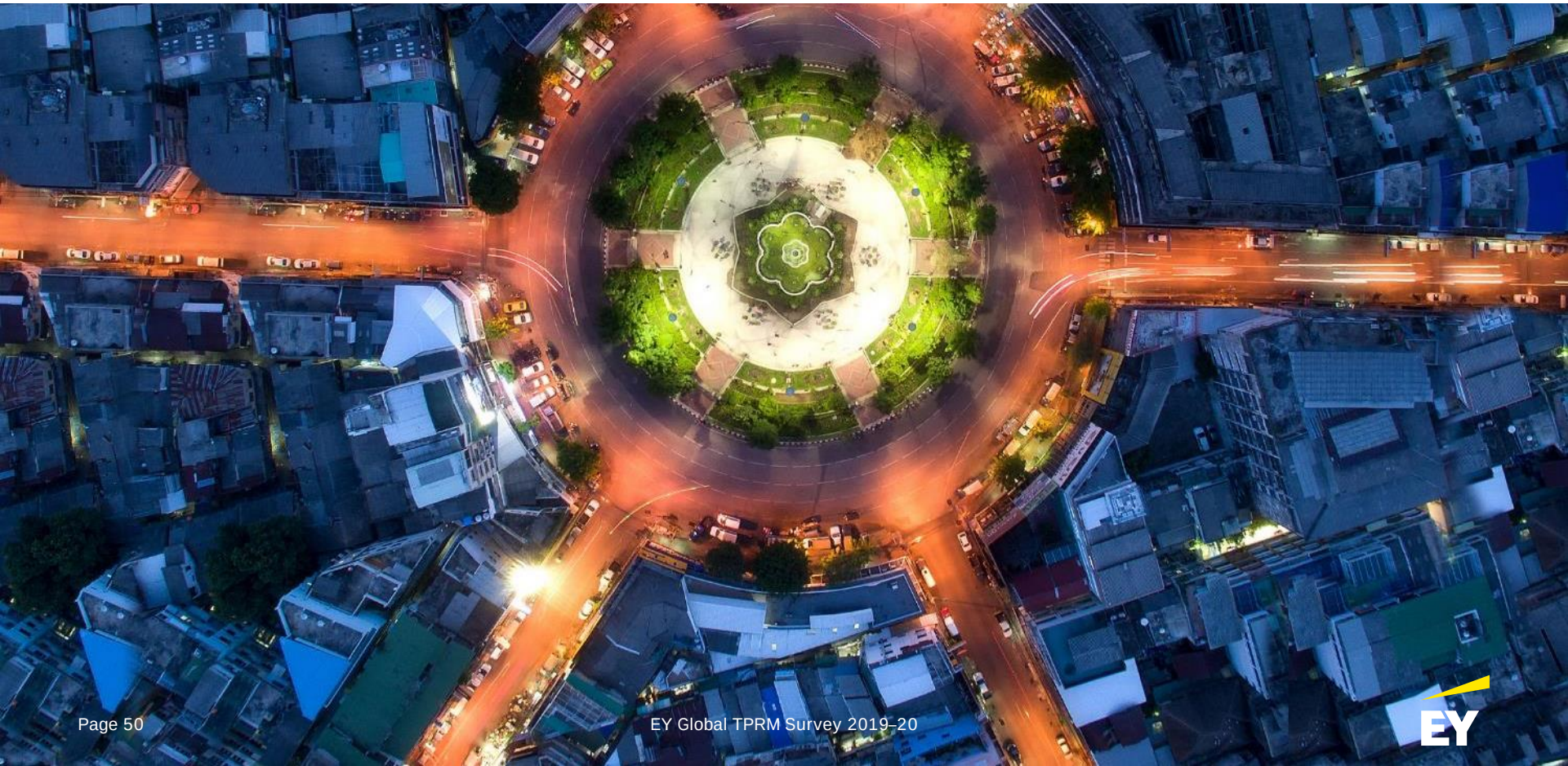
About half of the organizations surveyed find it relatively easy to report on concentration of spend and third-party concentration, but far fewer find it easy to report on fourth-party or reverse concentration.

Financial services concentration risk

Q45. [Financial services firms only] 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?



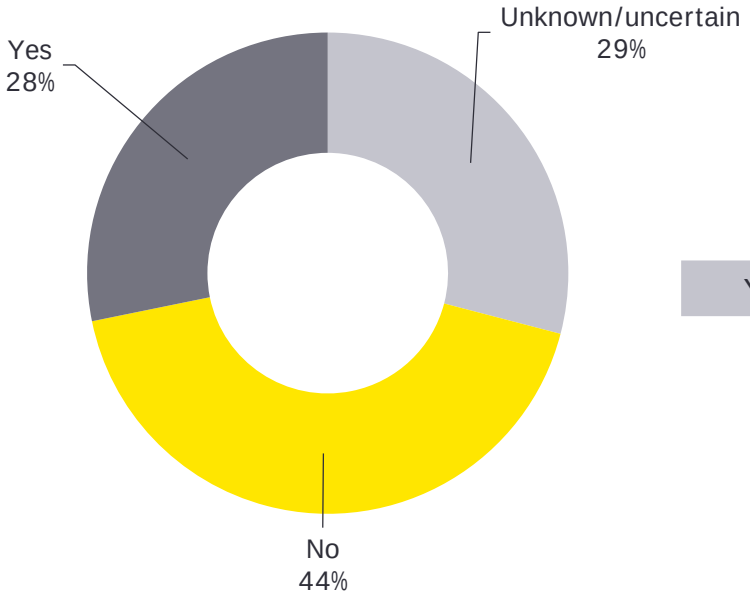
Affiliate management (financial services only)



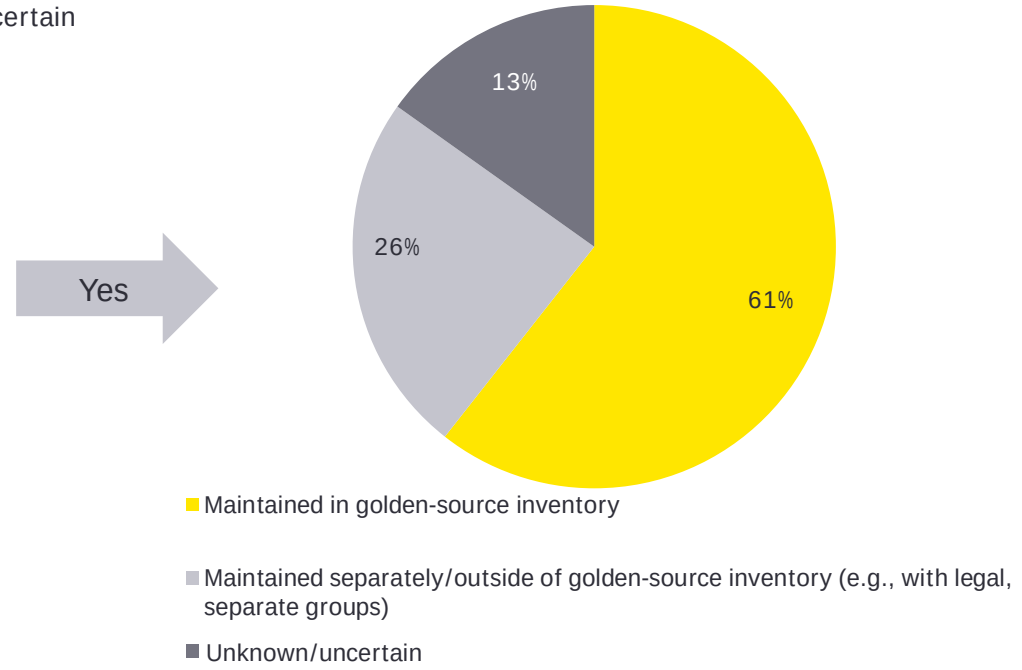
Twenty-eight percent of the organizations surveyed have intercompany affiliates that are in scope for their TPRM programs. Of those, 61% maintain those intercompany affiliates as part of their golden-source inventory.

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?

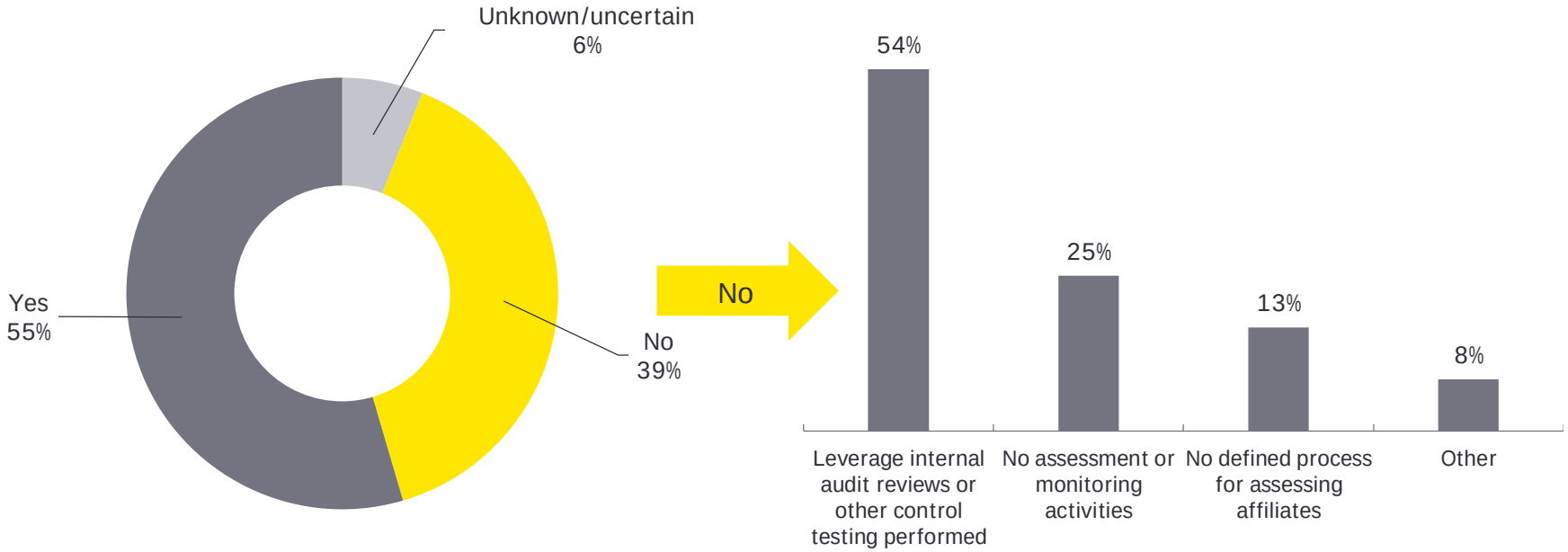


For those organizations surveyed that have intercompany affiliates that are in-scope for their TPRM programs, 55% say that the process is the same for assessing them. For those organizations that have a different process, most are leveraging internal audit reviews or other control testing, suggesting 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?

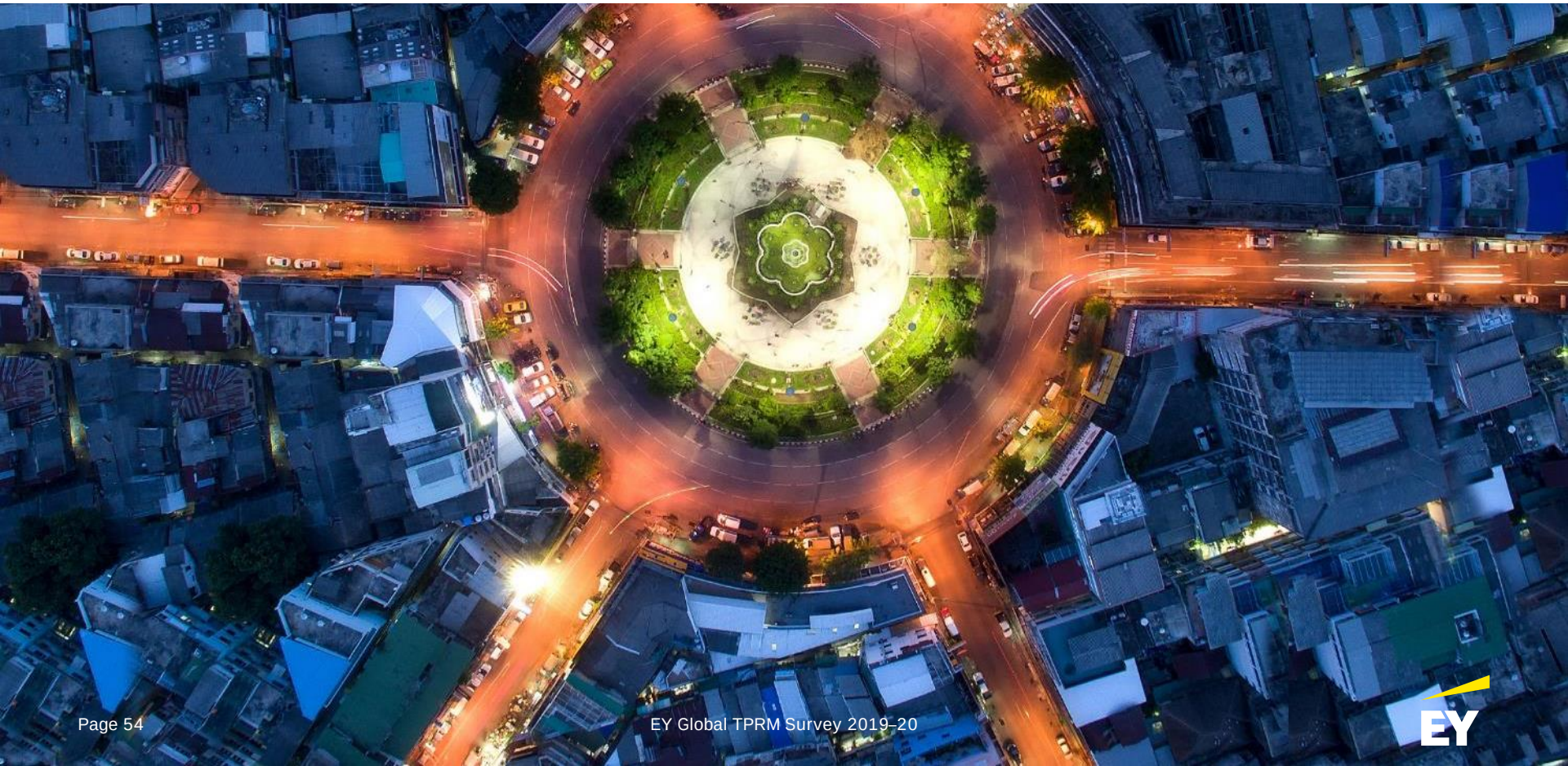


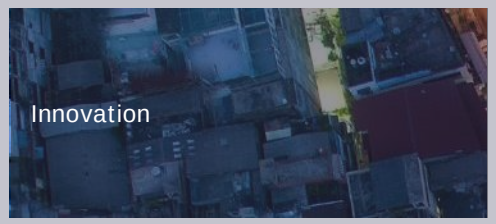
Affiliate monitoring requirements seem to vary greatly, without consensus on even the basic activities like service-level monitoring.

Intercompany monitoring requirements

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

Innovation



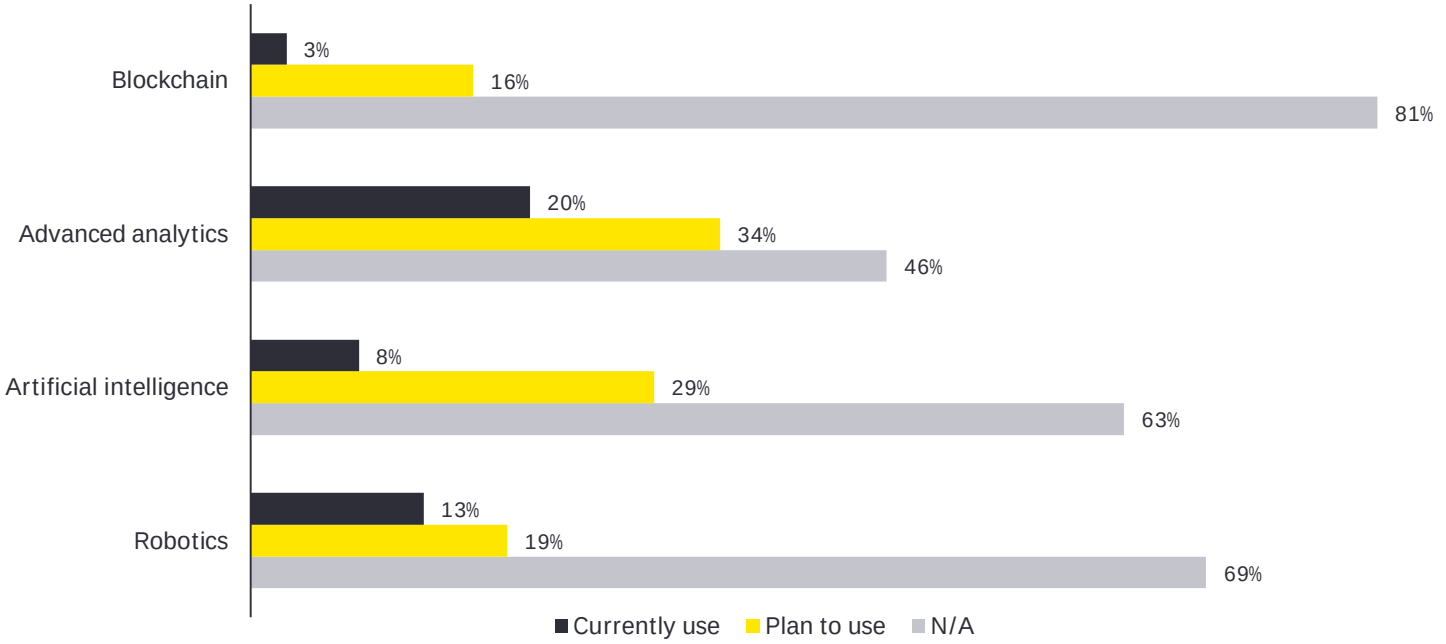


Just one in five organizations surveyed are using advanced analytics, and even fewer are using artificial intelligence (AI), robotics or blockchain. However, many more organizations recognize the benefits that such technology can provide. More than one in three expect to start using advanced analytics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

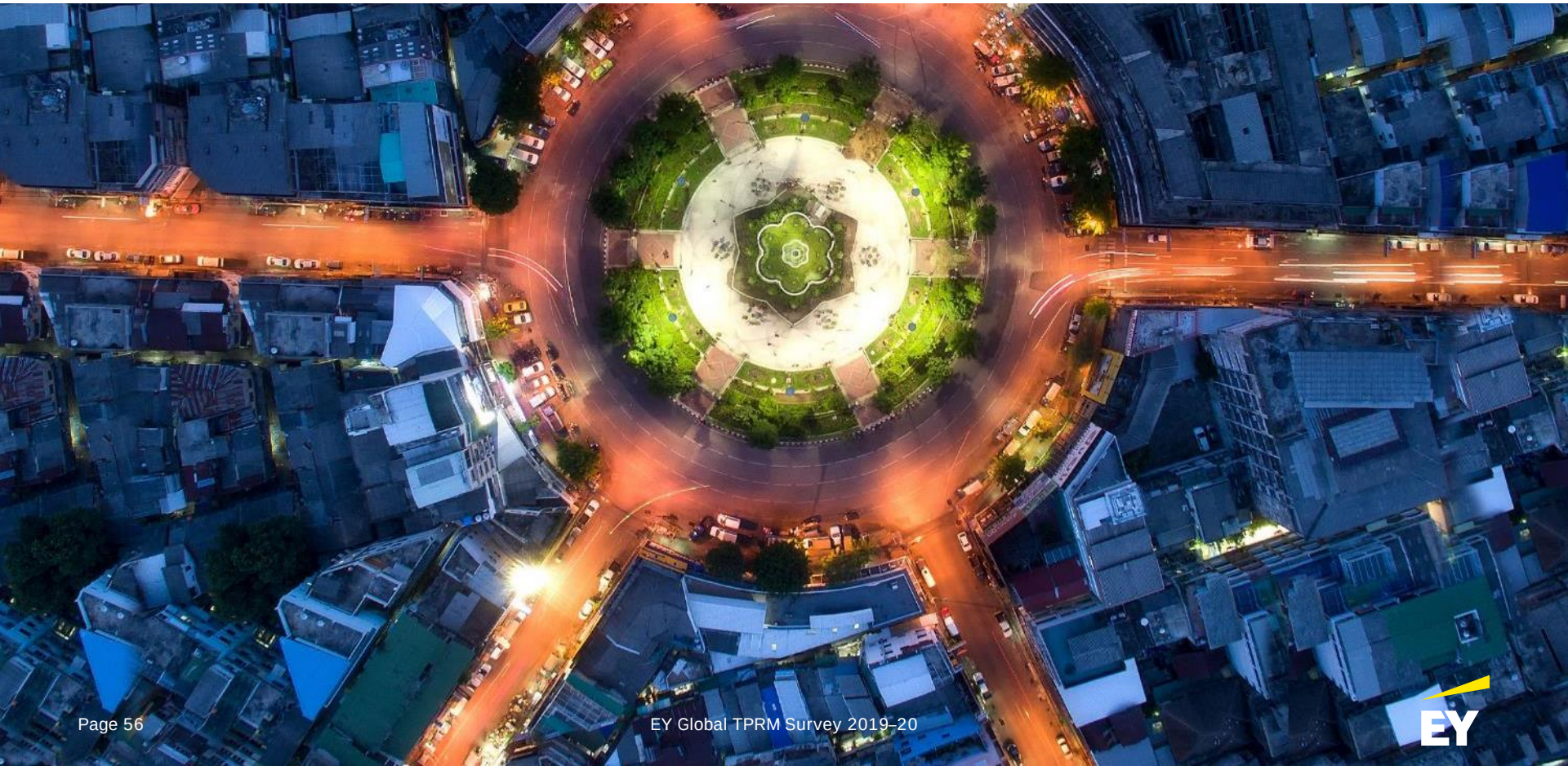
Emerging technologies for TPRM

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?



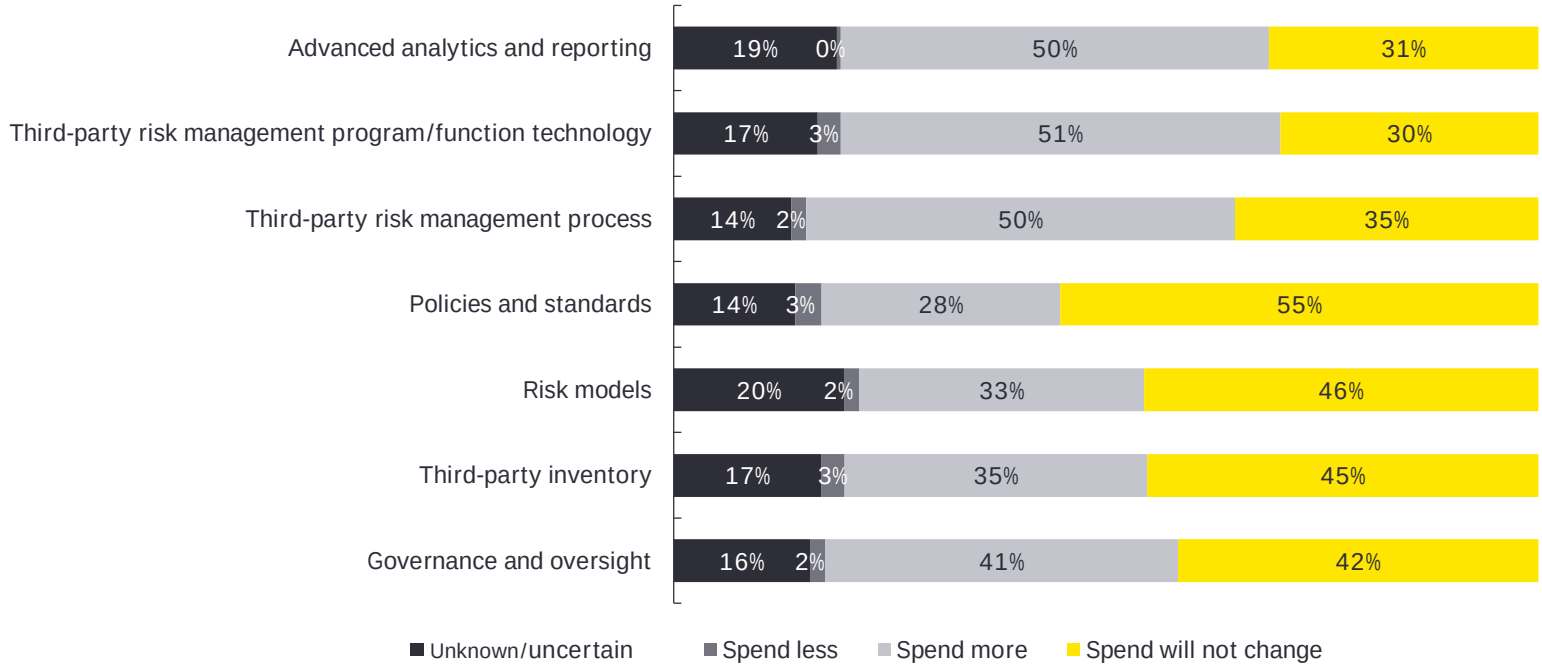
Areas of investment



To better leverage the technology they have, and stay ahead of the curve when it comes to emerging technologies, most 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 50% of organizations plan to spend more in the future. Eighty-five 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

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

Vignesh Veerasamy
EY Global and Americas TPRM Leader
vignesh.veerasamy@ey.com
+1 415 425 3993

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

Steven Xiong
APAC Risk Transformation Leader
steven.xiong@ch.ey.com
+862122282688

Oceania

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

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

Europe, Middle East, India and Africa (EMEIA)

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

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