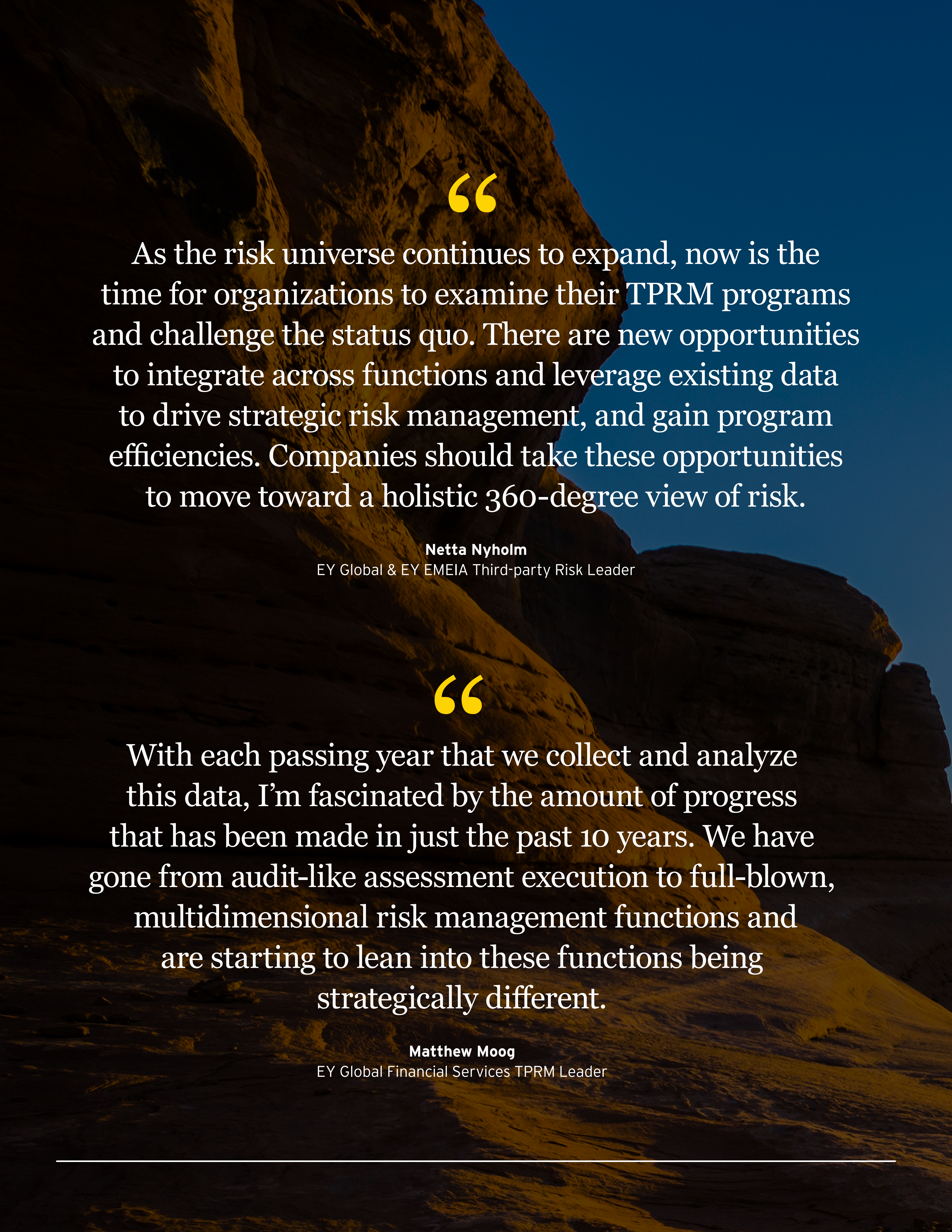
How can finite resources tackle an infinite risk universe?

EY global third-party risk management survey highlights 2021

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

Building a better
working world

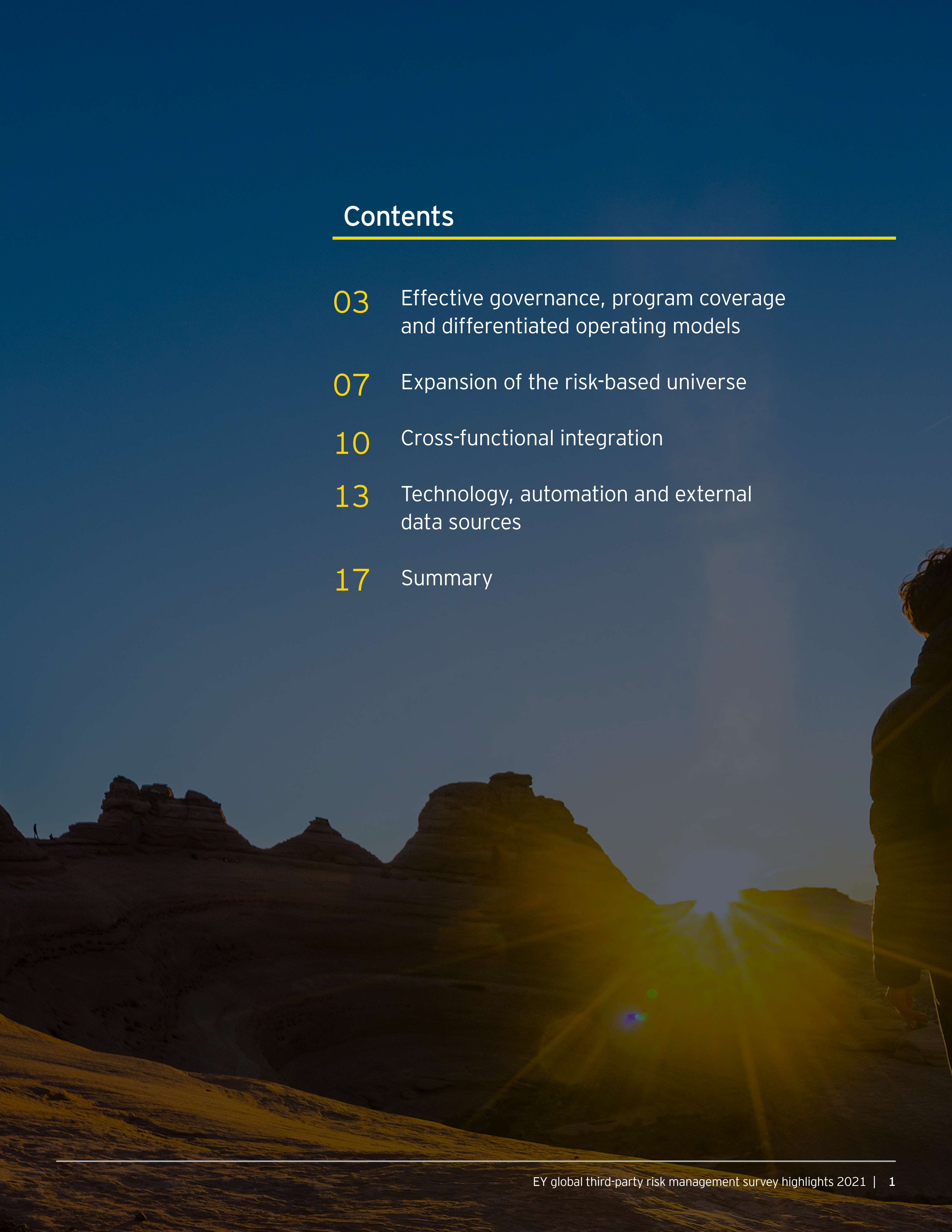


As the risk universe continues to expand, now is the time for organizations to examine their TPRM programs and challenge the status quo. There are new opportunities to integrate across functions and leverage existing data to drive strategic risk management, and gain program efficiencies. Companies should take these opportunities to move toward a holistic 360-degree view of risk.

Netta Nyholm
EY Global & EY EMEIA Third-party Risk Leader

With each passing year that we collect and analyze this data, I'm fascinated by the amount of progress that has been made in just the past 10 years. We have gone from audit-like assessment execution to full-blown, multidimensional risk management functions and are starting to lean into these functions being strategically different.

Matthew Moog
EY Global Financial Services TPRM Leader



Contents

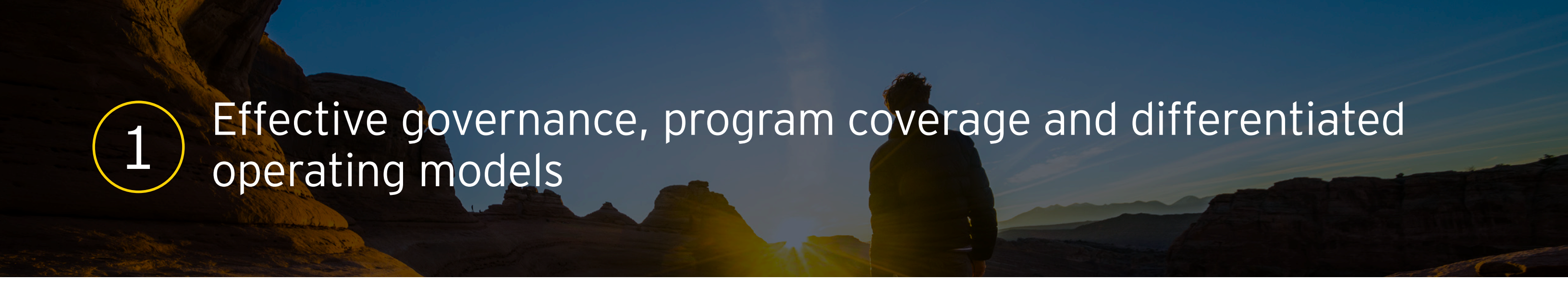
This EY global third-party risk management (TPRM) survey explores how organizations across industries are protecting their business against third-party risk. In today's world, companies need to work with multiple third parties to stay agile and competitive, but each third-party relationship adds potential risk, including cyber risk, regulatory risk and brand risk.

This EY survey covers organizations from around the globe across a broad range of sectors, including 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. Based on the survey responses, TPRM programs have grown and gained maturity in several sectors, especially in the public sector and higher education, which were home to the newest TPRM programs with an average operation timeline of 2.4 years.

The COVID-19 pandemic and emerging risks are highlighting the importance of and dependency on third parties within an interconnected business environment. As companies cautiously emerge from the trials of the past year, they have a driving need to work smarter, not harder, as they face an expanding risk universe with limited resources. With this need in mind, the EY global TPRM survey results reveal some notable trends and opportunities within:

1. **Effective governance, program coverage and differentiated operating models**
2. **Expansion of the risk-based universe**
3. **Cross-functional integration**
4. **Technology, automation and external data sources**

These trends highlight the current focus of organizations as they navigate the changing TPRM frontier. While the territory may be uncharted, signposts point the way. Companies are aware of the various tools and enablers that can maximize their TPRM efforts, but they need practical knowledge on how best to use them. Strategic investment in TPRM processes and technologies can unlock efficiency and value while accelerating maturity in key areas. Enhanced connectivity and transparency along the end-to-end third-party life cycle can drive improved decision-making, speed of delivery and lower organizational cost.



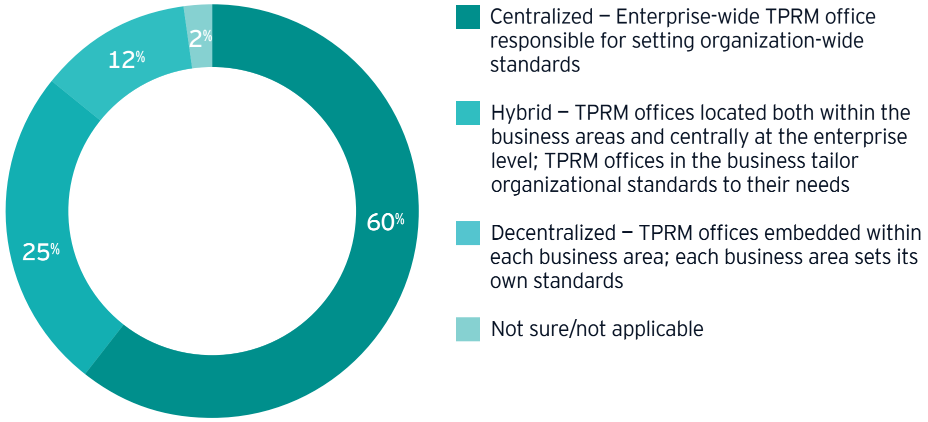
1 Effective governance, program coverage and differentiated operating models

To keep pace with the expanding risk universe, organizations require a foundation of smart governance and program execution. Unfortunately, it appears that resourcing and funding constraints have hit their limits even as the scope of TPRM programs continues to expand. In our most recent survey, released in 2020, respondents expected to increase their spend across multiple categories, from governance and oversight to policies and standards. But in this year's survey, organizations say they are less willing to increase their budgets – each of the spend categories saw an average reduction of 13%. Ultimately, organizations need to find different, more efficient ways to manage the third-party risk landscape in self-funded ways.

Spending continues to be concentrated in the core program itself (e.g., the TPRM team, external consulting), with 33% of organizations surveyed spending over US$500,000. The second largest spend is in assessment execution, with 22% spending over US$500,000. As TPRM programs identify automation opportunities and other cost efficiencies while driving a risk-based approach throughout the program, the historical drawbacks around centralized programs are being diminished. Ultimately, organizations are using a centralized model – compared to 50% in our 2020 survey.

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

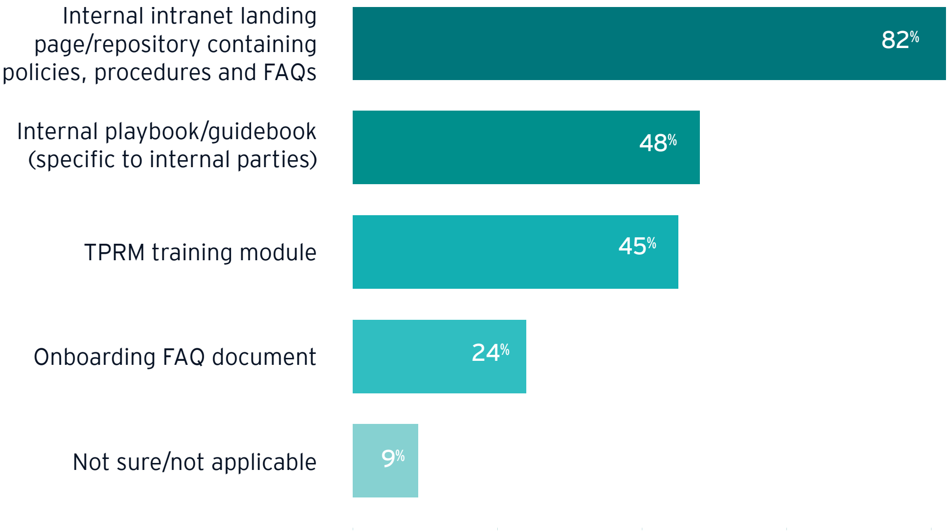
TPRM program structure



However, this increase in centralization has revealed a lack of awareness across organizational functions. Companies are still struggling to find the right approach and resources to effectively execute change management activities. For example, fewer than half of respondents had a TPRM training module to communicate expectations to internal stakeholders, with 82% instead relying on intranet pages, policies, procedures or FAQs. As organizations continue to evolve at a rapid pace to address emerging technologies, new data capabilities and an ever-changing world, this passive education approach is simply not sufficient. This potential disconnect offers an opportunity to better engage stakeholders throughout the third-party life cycle so they understand the TPRM value proposition, along with their operational role and responsibility.

Q How do you mandate and communicate TPRM expectations to internal stakeholders (e.g., contract owners, relationship managers)?

Mandate and communicate TPRM expectations



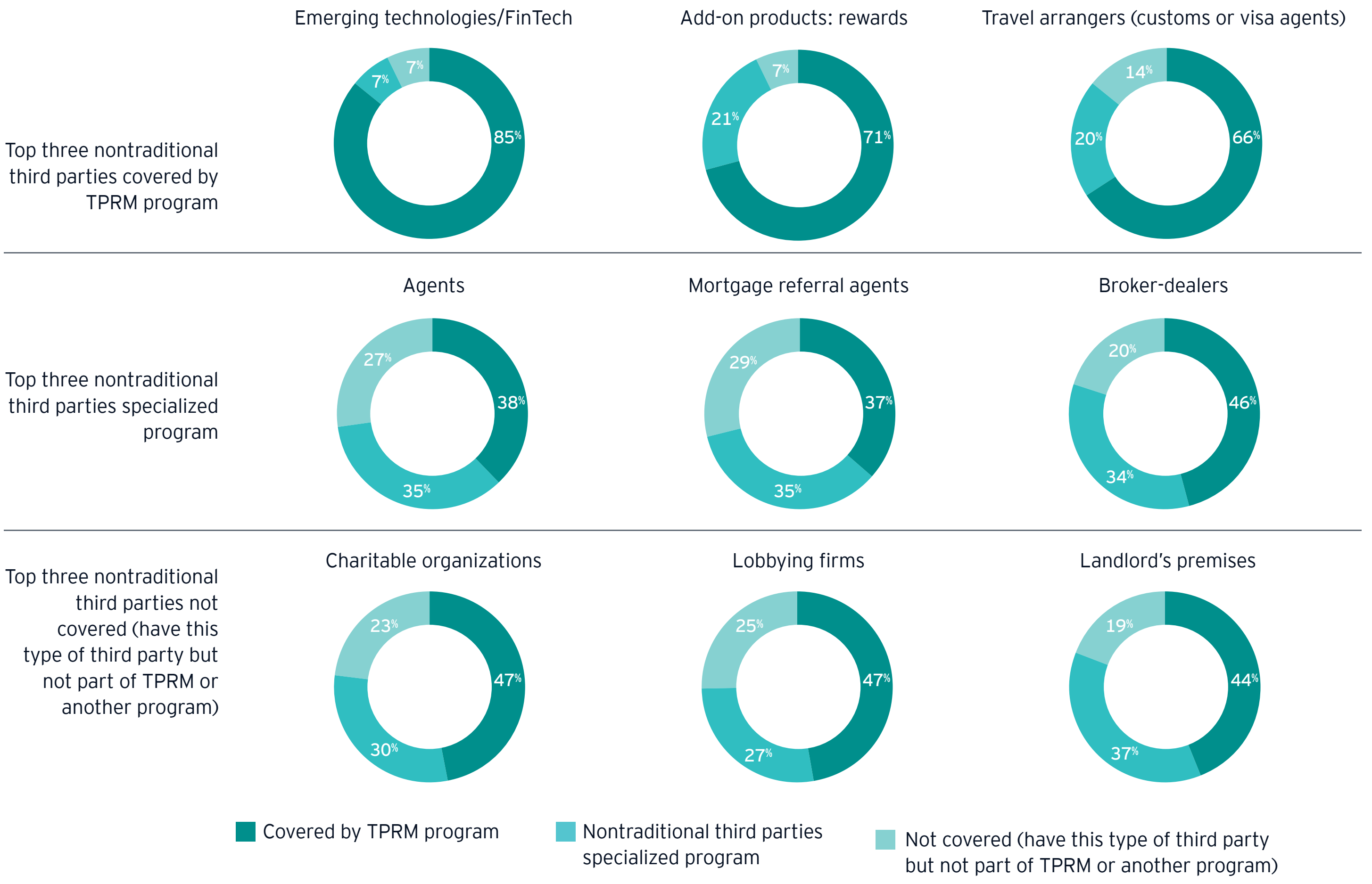
The two most common areas of focus for reviews by both internal audit and regulatory bodies were third-party assessments followed by oversight and governance. Strong governance and program execution are the backbone of good risk management, and internal and external reviewers are continuing to focus on those areas.

Program coverage and scope

TPRM program coverage has also continued to expand through inventory management of nontraditional third parties. From last year's survey to now, services such as charities, agent banks and sponsorships were covered by the TPRM program in at least 10% more companies. Respondents are also setting up more specialized coverage programs, evidenced by an increase of more than 10% in programs for broker-dealers, joint ventures and mortgage services. To enable this expanded inventory and coverage, organizations are developing strong service catalogs to properly route engagements to the right level of oversight.

Nontraditional third parties

For each of the following types of nontraditional third parties, are the third parties covered by your TPRM program/function?



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

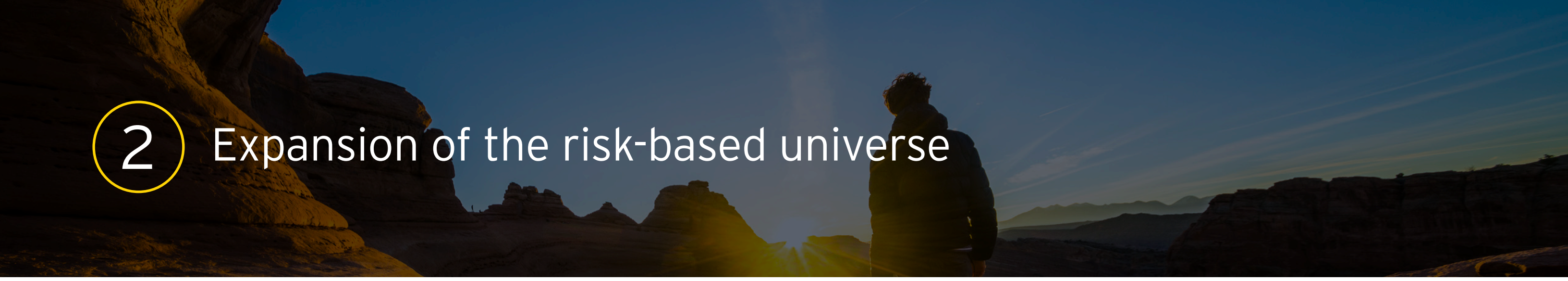
Operating models leveraging external support

As operating models change, so do decisions on delivery structures. This year's survey found that respondents are leveraging multiple forms of external support. Of the organizations surveyed, 43% use managed service providers to execute their TPRM function, and 46% expect to use more managed services over the next two to three years. Similarly, 59% of respondents currently use market utilities or sector-based consortiums, and over one third of respondents expect to increase their use over the next two to three years. These operating models are helping companies do more with reduced spend and resources. In parallel, internal talent is being retained and enabled to focus on differentiating risks and high-value activities.

Q Does your organization use the following for the execution of your TPRM program/function?

TPRM execution

Attribute	2021 results	2020 results
Co-sourced arrangements	43%	24%
Managed services	43%	31%
Market utilities/sector-based consortiums	59%	29%



2 Expansion of the risk-based universe

Over the next two to three years, the amount of effort required to effectively manage third-party risk is only going to increase, largely due to an expanding risk universe, increasing supply bases, more complex relationships, additional market capabilities and increasing regulatory focus, especially on anything deemed critical to a country's infrastructure. With finite budgets and hours in a day, organizations will need to thoughtfully determine where and how resources can best be deployed.

Working smarter, not harder, in this context emphasizes the importance of inventory scoping, tiering and criticality. The third-party landscape continues to grow, so companies are significantly raising the bar to entry for the scope of their program (respondents indicated an average 25% of total third parties are in scope for TPRM programs vs. 47% in last year's survey). Organizations are making progress in using a risk-based approach for assessing third parties, decreasing the number of control assessments performed. In fact, responses show that 9% of the third-party population has been control assessed versus 26% in 2020. Through the challenges of the pandemic, organizations are learning what truly matters to their business and where the risk is present — and they are applying their finite resources in areas such as resiliency, technology infrastructure and third parties critical to the enterprise.

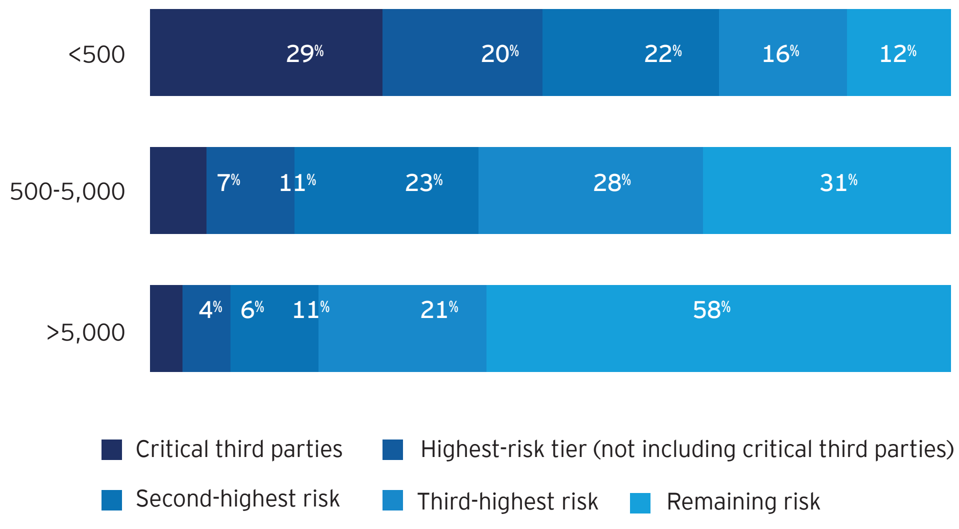
Third-party volume

2020	2021
47%	25%
total third parties in scope	total third parties in scope
26%	8%
of third parties assessed	of third parties assessed

In terms of tiering, organizations are continuing to reduce the number of third parties classified as critical (organizations with more than 5,000 third parties have classified less than 5% of their population as critical). Fewer third parties are falling into high-risk categories as well, with respondents classifying an ever-increasing number of in-scope third parties within their "remaining risk" ranking versus a baseline of 26% last year. These expedited changes are likely a by-product of pandemic-related cost pressures and focus on third-party resiliency, prompting companies to re-evaluate and reassess their tiering criteria to focus on the third parties that matter most and have the largest impact on the organization. Respondents noted that their three most important criteria in defining critical third parties were criticality of services provided, sensitivity of data involved in providing services, and business continuity and resiliency.

Q How many third parties are in scope for your TPRM program/function in each of your organization's risk tiers/ranks?

Third-party risk scale

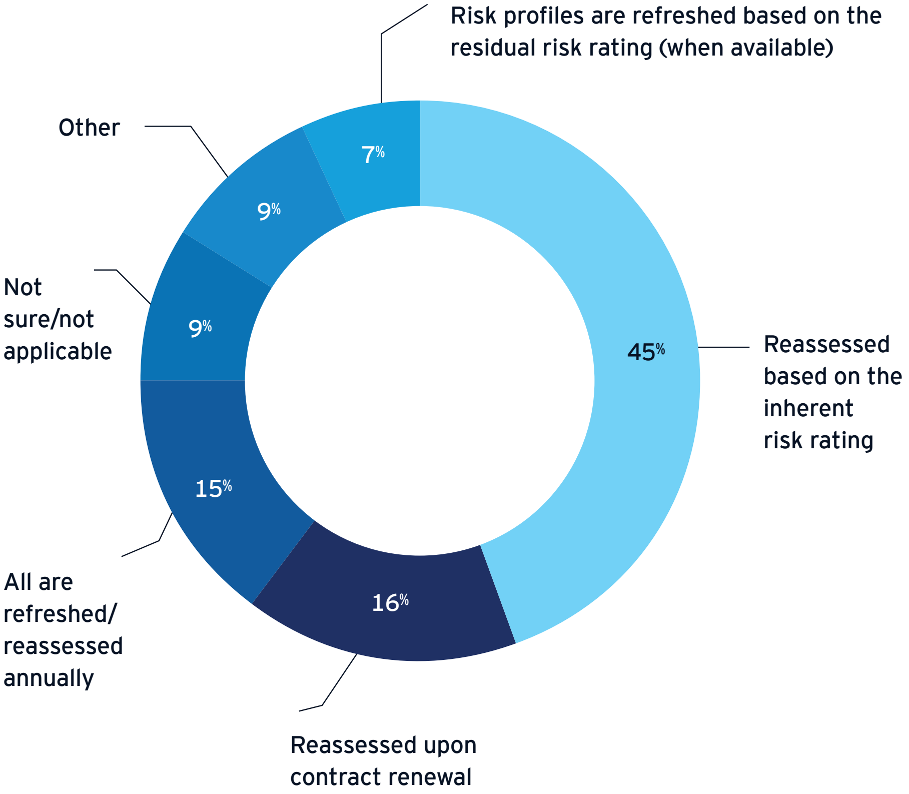


Methodology

More and more companies are moving away from reassessing inherent risk only when signing contracts. Instead, organizations are employing a risk-based approach using the inherent risk value, or residual risk when available. Companies are also reducing non-value-added activities by opting out of assessments on their lowest-risk tier — 37% responded "not assessed" for this category, consistent with last year. This streamlined approach allows organizations to deploy resources on the greater risks and maintain an accurate inventory.

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

Assessing inherent risk of third party

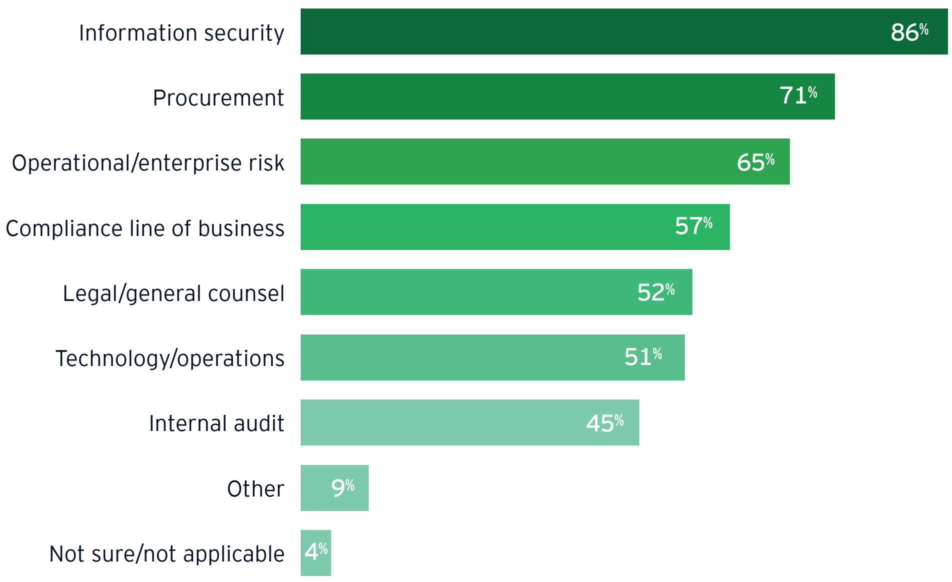


3 Cross-functional integration

While most TPRM programs align with a few internal functions, such as information security and procurement, many other functions are left to their own devices as they assess third parties within silos. As they work with third parties, many functions are collecting similar questions yet not communicating with each other, leaving an organization unaware of the collective view of risk. Organizations that are able to bridge this gap with an integrated risk management approach will find it significantly easier to be resilient in times of uncertainty.

Q Which of the following groups access information/data that is collected as part of the TPRM assessment process in order to enhance their own processes/analysis?

TPRM data collection



Approximately 86% of respondents supply information security functions with TPRM-related data as part of their TPRM programs. However, the level of integration drops dramatically across other key stakeholders surveyed, including procurement (71%), operational risk/enterprise risk (65%), compliance line of business (57%), legal/general counsel (52%) and technology/operations (51%).

Functional integration within the TPRM program offers a tremendous opportunity to further integrate taxonomies, improve data quality and prevent unnecessary data replication, driving an improved third-party inventory. This in turn would reduce fatigue on third-party business and control functions as they respond to fewer duplicative data requests.

Improved alignment would also expedite direct and indirect spend decision-making throughout the third-party life cycle. This would offer much-needed transparency to help reduce third-party proliferation in key areas like IT and cyber and within key business processes that rely heavily on large volumes of third parties, such as claims, loan origination, part suppliers and raw material suppliers.

The difficult path to integration

Unfortunately, the path to integration presents several roadblocks. Different functions may be using different tools or technologies to collect data, and 27% to 34% of respondents either do not have dedicated technology or remain unaware of the ecosystem of available tools to enable their programs. There's no one-size-fits-all solution for enabling technology; however, organizations need to consider how to manage the full, integrated life cycle while weighing the benefits of a larger enterprise tool or a smaller, dedicated TPRM tool.

Technology tools to manage risk

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

Function	No tool used (manual)	Archer®	BWise®	MetricStream	SAP/ Ariba Risk	COUPA Risk Assess	Process Unity®	Aravo	ServiceNow	OneTrust	Lockpath	Proprietary	Not sure/not applicable	Other
Sourcing activity	18%	6%	0%	4%	14%	4%	4%	3%	6%	2%	0%	5%	16%	19%
Inherent risk assessment	19%	15%	0%	2%	1%	6%	8%	2%	6%	2%	1%	9%	8%	20%
Contract management	16%	4%	0%	1%	16%	4%	4%	1%	3%	1%	0%	7%	15%	28%
Primary third-party inventory	16%	12%	0%	3%	6%	5%	7%	2%	4%	1%	1%	7%	14%	20%
Risk/control assessment facilitation	17%	14%	1%	3%	1%	4%	9%	2%	7%	2%	1%	9%	11%	19%
Issue management	17%	19%	1%	4%	1%	1%	7%	1%	8%	2%	1%	9%	11%	19%

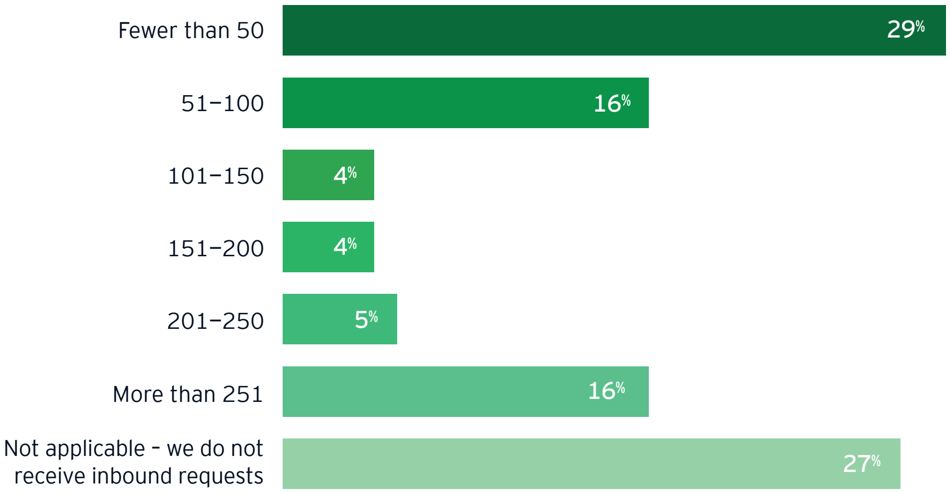
Note: Yellow shading indicates the top three technology/tools to manage risk for each function.

Inbound assessment challenges

As organizations undertake the integration of their TPRM programs, it can provide value to look at how internal functions are responding to control assessment requests from customers. Forty-five percent of the organizations surveyed facilitate more than 50 inbound assessments per year, and an additional quarter of participants don't receive inbound requests (or don't believe they receive inbound requests), showing a possible disconnect between inbound request management and internal risk management functions.

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

Inbound requests for TPRM



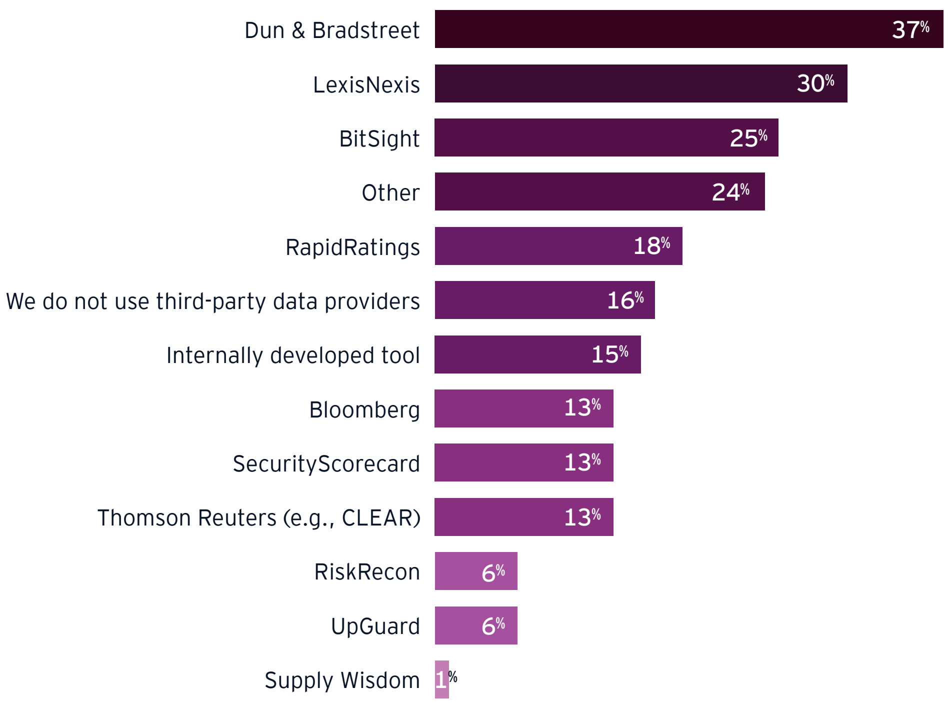
4 Technology, automation and external data sources

According to the EY Global Board Risk Survey report, many organizations are investing heavily in technology to make internal processes more efficient and create new experiences for customers. But inherent in these digital transformations is a complex web of risk factors – from bias in artificial intelligence to data breaches. Effective risk management is essential to the design and application of transformation initiatives, taking into account the wide range of potential disrupters.

And while organizations seem intrigued by emerging technologies and services, their actions have yet to match their intentions. Much of what is possible remains just that – a possibility – as companies struggle to integrate external data providers, market utilities and robotic process automation (RPA) into their TPRM processes to reduce effort and cycle times while improving monitoring capabilities.

While 84% of organizations are now using some form of external data provider, a significant portion of companies are using them only in select areas. Just over a third of those organizations consider these technologies and products to be extremely or very useful, indicating that organizations are still overcoming growing pains around how to ingest these technologies, include them in risk methodologies, and leverage them to drive both value and overall efficiency.

Q What third parties does your organization currently use to inform the TPRM process (e.g., threat intelligence, data providers), if any?



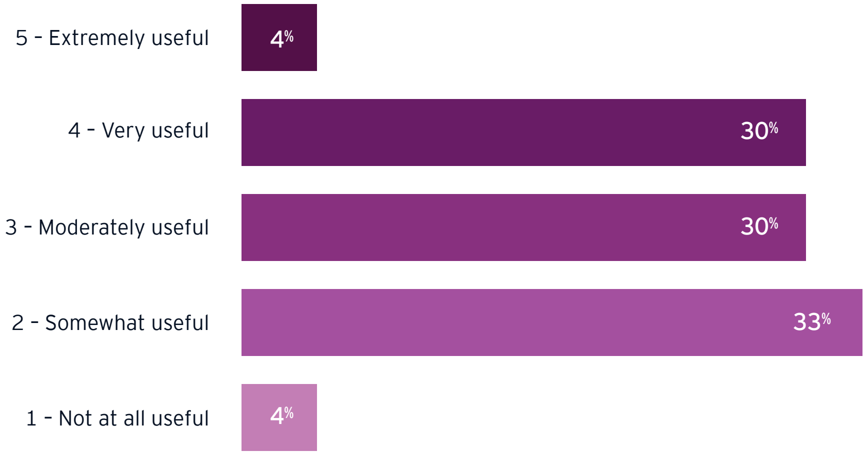
Threat intelligence

There is an opportunity to leverage externally available data sources (e.g., financial, cyber, geopolitical) to monitor key risk indicators against predefined risk appetite and risk tolerance thresholds, reducing reassessment efforts. Rethinking the TPRM risk methodology to include external data providers offers a chance to lessen assessment fatigue. In fact, 35% of respondents continue to perform annual control assessments on their lower-risk third-party segments (i.e., second-highest, third-highest and remaining risk third-party segments), and 21% of companies surveyed are not using these technologies at all in their programs. In addition, 45% of respondents do not use any external data providers at all to assess the financial health and reputation of their third parties, indicating a substantial opportunity to reduce manually intensive and point-in-time assessment activities.

Intelligence tools

The acceleration of automation and technology enablement will provide better clarity into real issues and threats, such as enterprise-wide exposure and concentrations of risk. With 64% of respondents seeing value in using risk and threat intelligence tools, companies have a chance to mature their TPRM programs to gain efficiencies while improving real-time risk oversight. There is also a significant opportunity to leverage automation to improve continuous monitoring capabilities as 34% of organizations surveyed find these market tools extremely useful or very useful.

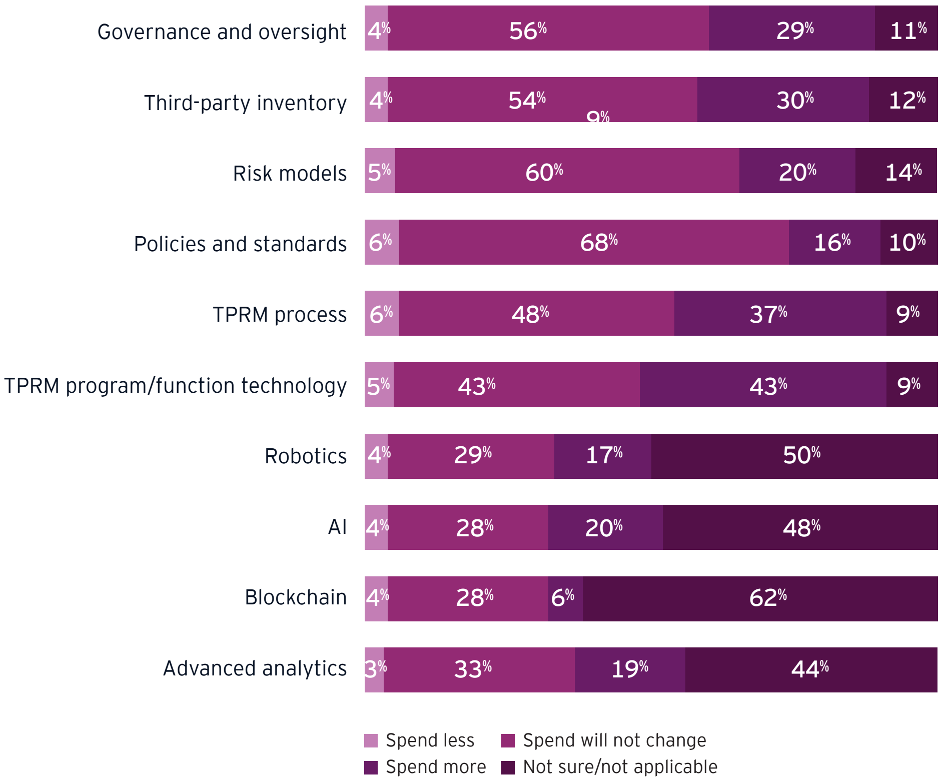
Q On a scale of 1 to 5, with 1 being not at all useful and 5 being extremely useful, how useful are threat intelligence tools at driving risk-based ongoing oversight activity?



Even with this wider use of intelligence tools, just one in five organizations surveyed are using advanced analytics, and even fewer are using artificial intelligence (AI), RPA or blockchain. However, many more organizations recognize the benefits that such technologies can provide. More than one in three respondents expect to start using advanced analytics in the next two to three years, and almost one in three plan to use AI.

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

Time investment in activities



Assessment cycle times and types

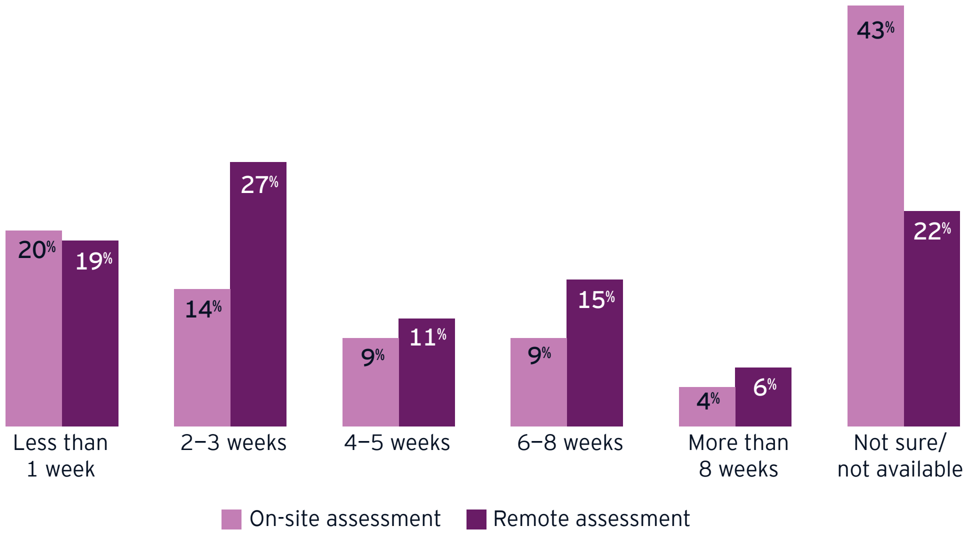
For many companies, remote assessments seem to be taking longer than on-site assessments, and technology could help. Approximately one third (32%) of respondents have remote assessment cycle times that are four weeks or longer, as opposed to 22% of respondents with on-site cycle times of four weeks or longer.

In addition, 17% of companies surveyed are still tracking and managing issues via manually intensive processes using Excel spreadsheets, and another 11% do not know how or where issues are tracked. Leveraging technology such as RPA to automate routine processes and build a more transparent workflow, including defined KPI capture points, will help programs become more efficient, improve risk management and expedite business outcomes.

When considering the impact of the pandemic, organizations have reduced their on-site assessments in favor of remote and virtual on-site assessments. Virtual on-site — screen sharing of artifacts and materials normally reviewed on site — provides similar coverage and comfort as a typical on-site assessment, which can also help reduce the assessment cycle time. As organizations find new, innovative ways to reach a similar outcome, this trend is likely to continue as it reduces both cost and cycle time.

Q Approximately how long does it take for your organization to conduct an on-site and remote assessment of a third party (end to end)?

TPRM remote assessment



Summary

The third-party risk universe continues to grow, and organizations are trying to manage that expansion by working smarter, not harder. Keeping pace requires a third-party risk management foundation of smart governance and program execution — complete with employee training, inventory scope tiering based on criticality, and operating models that include external support. As organizations work to transform their TPRM programs, they should consider improving functional integration and alignment, leveraging externally available data sources and intelligence tools, and taking advantage of new ways of working such as remote and virtual on-site assessments.

Contacts

GLOBAL

Netta Nyholm
EY Global & EY EMEIA Third-party Risk Leader
netta.nyholm@de.ey.com
+49 221 2779 16427

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

AMERICAS

Michael Giarrusso
EY Americas Financial Services TPRM Leader
michael.giarusso@ey.com
Tel: +1 617 585 0395

Vignesh Veerasamy
EY Americas West Risk Markets Leader
vignesh.veerasamy@ey.com
Tel: +1 415 425 3993

Sanjay Narain
EY Americas East TPRM Leader
sanjay.narain@ey.com
Tel: +1 212 773 7879

ASIA-PACIFIC

Chee Kong Wong
EY Asia-Pacific Risk Markets Leader
chee.kong.wong@au.ey.com
Tel: +61 3 8575 6389

Scott Mandell
EY Asia-Pacific Financial Services
Markets Leader
scott.mandell@au.ey.com
Tel: +61 2 9694 5696

EUROPE, MIDDLE EAST, INDIA AND AFRICA (EMEIA)

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

EY | Building a better working world

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

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

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

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. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2021 Ernst & Young LLP.
All Rights Reserved.

2010-3606138
EYG no. 006509-21Gbl
ED None

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

EY member firms do not practice law where not permitted by local law and regulations. Ernst & Young LLP (US) does not practice law or offer legal advice.

ey.com