TPRM evolution and trends for 2021 and beyond

June 8, 2021

Building a better working world

Your speakers

Rolan Moldes

Ernst & Young LLP

Senior Manager

rolan.moldes@ey.com

+1 510 520-8879

Busola Oyefesobi-Ero

Ernst & Young LLP

Senior Manager

busola.oyefesobi-ero@ey.com

+1 858-535-7795

Rolan is a recently promoted managing director in the Consulting Services practice of Ernst & Young LLP. He currently serves as the US-West Third-Party Risk Management regional leader with more than 16 years of consulting experience focused on assisting clients to address IT and business risks and compliance challenges across industries.

Busola is a senior manager in the Consulting Services practice of Ernst & Young LLP and has more than nine years of controls and risk assessment experience. She focuses on assisting clients assess and evaluate business and operational risks in their current environment to determine the appropriate controls, oversight and monitoring required in order to mitigate risks and limit exposure.

Session objectives

- Understand third-party risk management trends
- Identify key actions that you can take to evolve your third-party risk management program / function

Agenda

- Welcome
- TPRM overview
- TPRM trends
- Key actions to evolve your TPRM function / program

Polling question # 1

Question:

What is your current functional area within your organization?

A. Information security / IT

B. Internal audit

C. Enterprise risk management

D. Legal / compliance

E. Other

2

TPRM overview

Polling question #2

Question:

How familiar are you with the concept of third-party risk management (TPRM)?

A. Very familiar

B. Somewhat familiar

C. Limited familiarity

D. Not familiar

Why the increase focus on TPRM?

Extensive dependence on third parties

- Growing competition to perform work faster
- Significant disruption impact on revenue and reputation
- Third parties are engaging fourth parties to support their operations and activities

Complex and ever-changing risk landscape

- Increased data protection obligations and evolving regulatory landscape (e.g., GDPR, HIPAA, CMS, NERC CIP, FCPA, OCC, CFBP, FDIC, FRB)
- Digital and social media influence
- Unforeseen disruptions (e.g., pandemic, earthquake)

Lack of third-party risk governance

- Lack of transparency of third-party population and related risks
- Unclear roles and responsibilities related to third-party management
- Lack of oversight related to third-party issues management and reporting

Technology and information shifts

- People and technology costs have grown year-over-year, shifting the institutional focus from manual activities to third-party technology solutions such as Software as a Service (Saas), robotic process automation (RPA), and artificial intelligence (AI)

TPRM defined

The growing dependence on third parties, for companies across a diverse range of industries more heavily than ever before, introduces significant new levels of risk to organizations. The leading organizations of the future must be able to transform uncertainty into confidence by developing trust with third parties.

TPRM

Definition

Third-party risk management provides a function for management to identify, evaluate, monitor and manage the risks associated with **third parties** and **contracts**.

Risks associated with third-parties

Geopolitical risk

Risk of doing business in a specific country and includes legal, regulatory, political and socio-economic considerations

Reputational risk

Risk that the organization's brand and reputation is impacted should an event occur at the third-party

Financial risk

Risk that the third-party cannot continue to operate as a financially viable entity

Digital risk

Risk that is associated with the third-party's digital business processes, resulting in errors

Regulatory and compliance risk

Risk that a third-party fails to comply with a required law or regulation, thus causing the organization to be non-compliant

Cyber risk

Risk that an organization's security is compromised due to deficiencies in the cybersecurity controls of the third-party

Privacy risk

Risk that an organization's data is lost or compromised due to deficiencies in the privacy controls of the third-party

Environmental, social and corporate risk

Risk that the third-party is unable to sustain its growth because of certain practices negatively impacting its value over a period of time

Fourth Party risk

Risk to the organization by parties engaged by your third-parties to support their operations and activities, including on your behalf

Operational risk

Risk that a third-party fails to meet the organizational needs from a service or product delivery perspective due to deficiencies in the third-party's operations

Business continuity and resiliency risk

Risk of third-party failure affecting the continuation of business as usual for the organization

3

Current TPRM Trends

Polling Question 3

Question:

Which of the following TPRM current trends are you familiar with?

A. Majority of organizations have a centralized TPRM program / function structure

B. At least a quarter of organizations have experienced at least one data breach, loss and or outages within the past 12 months

C. Organizations highest risk third parties are reassessed (risk/control assessment) on an annual basis

D Many organizations rely on the contractual terms established with the third party to assess/monitor fourth parties

E I don’t know / unsure

What is the fix?
What organization can do

To manage third-party risks, it is critical to establish foundational components within TPRM.

TPRM foundational components

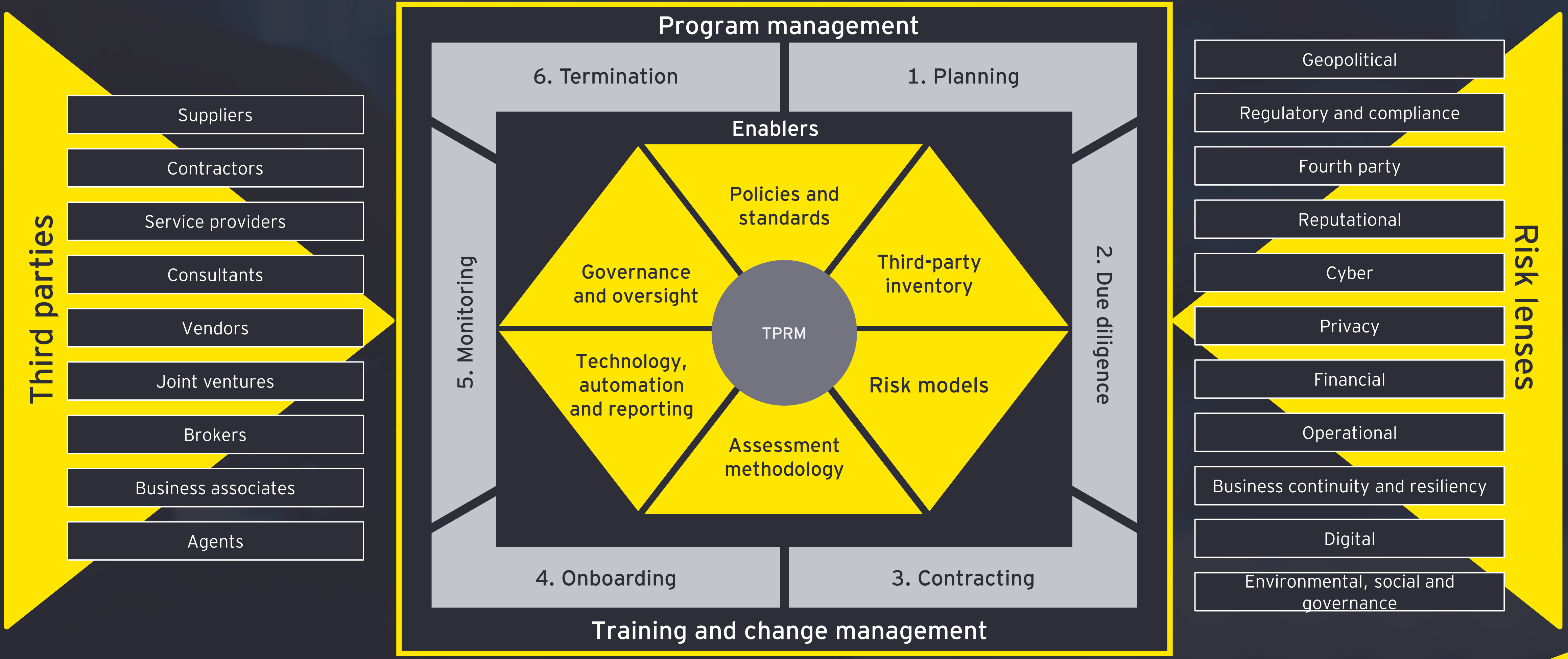
Oversight and governance	Polices and standards	Third-party inventory	Risk models	Assessment methodology	Technology, automation and reporting
The framework that defines the groups that manage the TPRM program and the way the function operates within the organization	The defined roles and responsibilities for TPRM activities, which are written and accessible	The centrally located list of all third parties, created using a data governance model and that is regularly updated, is available to all business owners and contains service-level information about the third parties	The risk criteria that are developed based on the organization's risk tolerance that informs the TPRM process to assess, prioritize and evaluate third parties	The processes by which risk is classified, ranked and reported; the assessment execution enablers; findings management procedures; and third-party assessment reports	The coordination of TPRM activities with the usage of technology to reduce duplication, speed up the selection and onboarding process, and effectively manage risks

Stakeholders

Procurement	Information security	Enterprise risk management	Internal audit	Legal and privacy	Compliance	Business units

What is the fix?
What organization can do

A holistic TPRM program provides a function for management to identify, evaluate, monitor and manage the risks associated with third parties (e.g., vendors and suppliers, intercompany relationships and fourth parties).



EY 2021 global TPRM survey highlights

In 2021 EY surveyed 162 institutions globally with a TPRM program / function in various sectors, including but not limited to banking, insurance, health science and wellness, technology, media and entertainment, and consumer products and retail. 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, compliance and finance. The purpose of the survey was to address the distinctive nature of third-party risk across industries.

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
- Technology and data
- Fourth-party risk management
- Environmental, social and governance
- Third-party risk management integration
- Reporting
- Inbound requests
- Regulatory and internal audit exams
- Non-traditional third parties
- Concentration risks
- Affiliate management
- Areas of investment and innovation

Organization, governance and oversight

As TPRM programs identify automation opportunities, standardize risk-based approaches throughout the organization and identify other process efficiencies, the historical drawbacks around centralized programs are being diminished.

In order to balance the counter force of maintaining or lowering spend, actual external support and interest in external support for program execution has continued to increase

60% of organizations reported having a centralized structure

46% of organizations expect to use managed service providers more in the next 2-3 years

Third-party population breakdown/risk tiering

The challenges of COVID-19, has organizations learning what truly matters to their business and where the risk is present – and they are applying their finite resources to those areas.

As organizations response to the pandemic, many noted that criticality of services is the most important criteria for determining which third parties are critical to the organization.

80% of organizations deem criticality of service provided as the most important criteria to define a critical third party

13% of in-scope third parties were deemed critical to the organization

Assessments

In trying to streamline TPRM programs / functions to spend resources on the right risks and maintain an accurate inventory, more and more companies are moving towards a risk-based approach using the inherent and / or residual risk value.

There is a general consensus across the board for performing assessments every year for critical/high, aligning with the push to reduce lower value risk management activities and focus efforts on higher risk third-party populations.

45% of organizations refresh third party inherent risk profiles based upon their inherent rating

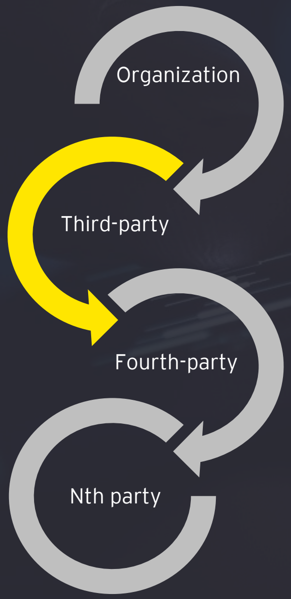
57% of organizations reassess (risk/control assessment) their highest risk third parties on an annual basis

> *Many companies have years of data about their third parties from the manual assessments, but they aren't doing anything with it. They just look at it as a compliance activity.*

Fourth parties

Typically, fourth party information is gathered during the risk/control assessment process.

The majority of third parties continue to rely on contracts and/or their third parties' own assessment programs for fourth-party coverage.



28% of organizations are not assessing or monitoring known fourth parties

65% of organizations rely on the contractual terms established with their third-party to assess / monitor fourth parties

Technology and data

As the use of technology increases, so does the opportunities for further integration and consolidation of the technology ecosystem to gain efficiency and improve business user experience. Many organizations are finding the use of external data sources very useful at driving risk-based ongoing oversight activity

70% of organizations leverage technology to manage risk

84% of organizations currently use external data sources (e.g., threat intelligence, data providers) as part of their TPRM process

All the emerging technologies – advanced analytics, AI, blockchain, even robotics – are useful to the extent that they ***drive strategic risk management*** *and not simply control assessments.*

4

Key actions to evolve your TPRM function / program

Key actions to evolve your TPRM function/program

Forward-thinking organizations must begin to address the underlying risks associated with their third-parties by asking tough questions and developing new approaches. Given the evolution and maturity of TPRM and current dynamics, TPRM programs / functions should be revaluated in order to stay current and adapt.

Identify third parties and build a comprehensive inventory

Two points of control that have been impactful for data capture:

- Pre-contract: Establish contract terms and ask the right questions during contracting risk assessments
- Post-contract: Potentially leverage a more mature third-party risk assessment in the organization (e.g., infosec risk assessment)

Understand third-party's significance to the organization, services provided, including data management

Comprehend what organization's data is shared, accessed, processed and/or stored by third-parties, how it's shared and with whom third-parties share it with

Define contracts terms for third parties and beyond

Organizations should have a defined approach for how third parties and beyond are potentially controlled through contract terms and conditions (e.g., data breach / incident requirements, right to audit clause, cloud data storage and security requirements)

Perform an ongoing monitoring of third parties and beyond

Organizations must develop a process to monitor their third, fourth and even Nth parties:

- Evaluate the riskiest or most critical third parties and focus efforts there
- Develop an automated, data-driven approach that enables assessment of third parties in a more real-time manner

Evaluate the program / function operating model

Organizations should review their current operating model to determine if their program is operating efficiently:

- Evaluate the integration with all relevant stakeholders and business units
- Are processes carried out consistently within the organization?

In brief

- TPRM is evolving from a tactical compliance exercise into a data-driven strategic business requirement
  - With the right approach, organizations can leverage the risk data for third-party performance management and rationalization efforts across the organization, retaining only the best of breed. This creates efficiencies and reduces costs
- The maturity of TPRM strategies varies among different sectors, but every company should be moving forward toward an integrated, 360-degree view of risk across business functions
- Increase the use of the right technology and risk data (internal and external) to help reduce manual efforts and streamline the program / function

Polling Question 4

Question:

Which aspect of your TPRM program / function will you revisit to continuously evolve / mature your TPRM capabilities?

A. Governance and operating model

B. Third-party tiering (high vs. low risk)

C. Risk assessment methodology including risk approach, risk model, assessment and monitoring process

D. All the above

E. I don't know / unsure

EY | Building a better working world

About EY
EY is a global leader in assurance, tax, strategy, transaction and consulting 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.

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

2011-3622364
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