Third party risk management (TPRM)

COVID-19 impact on third party resilience

March 2020

EY
Building a better working world

Contents

1. Executive summary – The impact of COVID-19 on third parties

The rapid spread of the COVID-19 is impacting economic growth and market volatility is increasing. This has impacted the industry through weakening investment returns and a potential adverse impact on the capital position of financial institutions around the world. From a TPRM perspective, it remains key to understand third party inventories and continue to risk assess third parties to recognize their criticality for continuity of services.

The immediate TPRM actions

- Evaluation of **Critical and Tier 1** relationships for technology infrastructure challenges and financial health concerns
- Send a series of **focused questions** about their response to COVID-19, business impact and their planning for the future
- Critical global dependencies and **location analysis** as all countries go into and out of lock down scenarios
- Geographical load balancing of non-technical capacity and considerations for **long term resource stress**
- **Laptop allocations** and other infrastructure needs, which need to be provided internally before addressing third-party needs and remote access capabilities

Additional procurement concerns

- Firms are experiencing **issues with conducting risk assessments** and on-site supplier assurance
- **Information security concerns** change within distributed working scenarios
- For offshore entities, where suppliers have centres in less developed countries, there is **limited confidence in the backbone infrastructure**
- Review of material Master Service Agreements and **contracts for Service Level Agreements** and credit/penalty scenarios for enhanced close monitoring and governance
- Short and long term evaluation for stringency vs. leniency in **enforcing contract obligations** given working circumstances

Financial risk exposure

- Consider potential impact to third party's P&L due to volatility in earnings, increased costs and loss in revenue
- Assess third party's liquidity and capital impact due to global economic downturn
- Evaluate your own exposure to third party business interruption, supply claims and event cancellation claims

Non-financial risk exposure

- Understand third party landscape servicing your critical technology and cyber operations to prepare, sense, and respond to most forms of disruption
- Understand third party resilience; confirming alignment with your own plans, and how to communicate the "end" of the pandemic

How EY teams can help

- Now: **Impact assessments** for remote work, security operations, third and fourth party readiness for critical vendors and supporting contingency programmes, **including regulatory responses** and process work-arounds (including automated access provisioning)
- Next: Testing to assess remote infrastructure and capabilities; including **stress testing for financial impact and resilience**
- Beyond: **Enhancing** your TPRM framework through enhanced awareness, reporting, technology and collaboration, learning from COVID-19

1. Executive summary – Key C-Suite questions related to third party resilience

To navigate this challenging environment, firms should focus on better communication, enhanced consumer relationships and more transparently with customers and investors. In order to do so, it's important that senior members of organizations consider the following questions in relation to third parties and their resilience:

Questions related to third party resilience	
1.	Can you map your key third parties to impacted jurisdictions and industries?
2.	Do you have standardised questions to ask of your third parties and who is reviewing their responses?
3.	Do you have clear policies regarding the presence of third parties onsite and are you clear which of your third parties can operate remotely?
4.	Do you know, talking to relationship managers, IT and facilities, which services you can't afford to lose?
5.	Are you clear which of your third parties preform any part of a critical economic function?
6.	Do you have a method of understanding the supply chains of your third parties and where the second order effect may arise?
7.	Can you quickly tell how many contracts, third parties, employees and other key relationships might be affected?
8.	Does the "Force Majeure" or hardship clauses in your standard terms and conditions or key contracts apply to this crisis?
9.	When evaluating alternative third parties, are there exclusivity clauses in current third party contracts that may complicate switching?
10.	Can you determine the your third parties' financial viability or attitude to the crisis facing your organization?
11.	Have you already given any consideration to the reintegration of third parties after COVID-19?
12.	Do you think the new normal will be different compared to the previous normal (working models/behaviors)?

2. Background – The unexpected outbreak of COVID-19 is having a significant impact on global third party chains

The COVID-19 outbreak has over 700,000 confirmed cases which is higher than previous recent disease outbreaks such as Ebola, MERS and SARS combined.

The current COVID-19 pandemic has caused **disruption** through **all sectors** with various degrees of impact. It is time for companies to **rapidly assess, recover and respond quickly** through numerous obstacles and challenges that will stand in the way. Through the **chaos of recovery**, it will be very easy to overlook the root cause and gaps within a supply chain that may have **paralysed businesses** during this unpredictable major event in the first place. Building towards **a resilient third party chain** will be at the **epicenter** of future discussion for years to come.

"94% of the Fortune 1000 are seeing coronavirus supply chain disruptions.

"Coronavirus raises fears of US drug supply disruptions 14% of the facilities that make active pharmaceutical ingredients are in China.

"European companies face coronavirus hit to supply chains
Italian auto supplier warns car groups' production lines may be brought to a standstill.

"Oxford Economics warned that the spread of the virus to regions outside Asia would knock 1.3% off global growth this year, the equivalent of $1.1t in lost income.

2. Background – but COVID-19 is only the latest in an increasing number of unexpected disruptions hitting third party chains, impacting overall business performance

Natural events

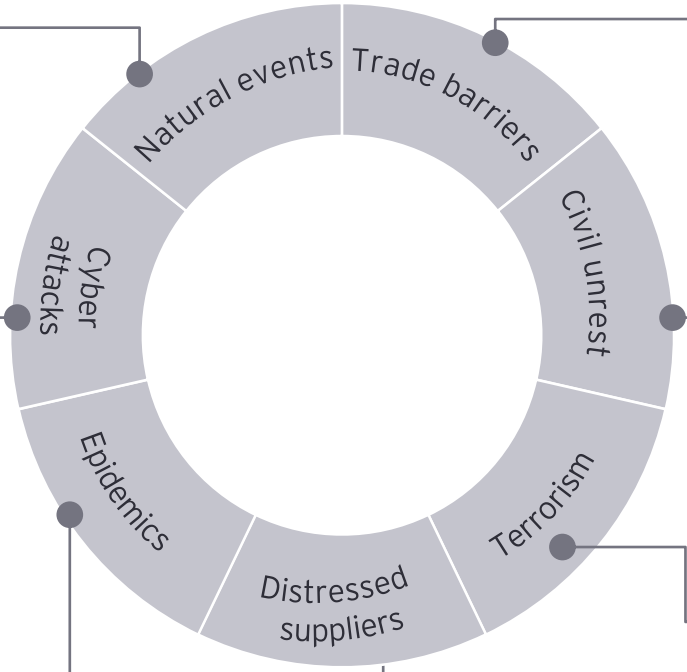
- $210b Tohoku earthquake in Japan halts production for Toyota, GM and Nissan

Cyber attacks

- WannaCry ransomware attack losses could reach $4b
- 50% increase in attacks from 2018, makes Supply Chain more vulnerable

Epidemics

- Covid-19 outbreak expected to cause a ~$400B dent in the global economy in two years- an estimated 8X bigger impact than SARS



Trade barriers

- US $63b tariffs on EU autos and auto parts, place strain on decades' old Global Supply Chain

Civil unrest

- March at La Escondida, Chile copper mine reduced global copper capacity by 5%

Terrorism

- Border restrictions after Paris Attack led to $3.5m increase to Belgium shippers in 1st month

Distressed suppliers

- Crop disease, dry weather and government policy changes cause cocoa shortage for food manufacturer

3. Key challenges – EY clients have to execute now, and prepare for the next and beyond as a result of COVID-19 challenges

The rapidly evolving threat around the COVID-19 virus is raising concerns among many organizations across the globe. The interconnected landscape of today's business environment with third parties pose serious risk of disruption that can result in significant loss of revenue.

1 Now
Solve the now

- Help manage the immediate operational resiliency challenges linked to your third parties

2 Next
Manage this year

- Monitor the financial stability of your critical and important third parties

3 Beyond
The current crisis

- Learn from COVID-19 and enhance your TPRM delivery models to future proof your third party operations

Key Client Challenges related to Third Party Risk Management	
	► The extent to which critical third parties can continue to operate under significant stress for prolonged periods of time ► Increasing concerns over data security or data leakage due to third parties moving to remote working/access ► Difficulties to obtain holistic third-party universal view to fully understand dependencies and vulnerabilities ► Inability to conduct appropriate third party risk assessments and supplier assurance activities ► Do not have the capacity or technical capabilities to conduct the required on-going monitoring activities on third parties ► Meeting existing regulatory/Internal Audit deadlines or complying with on-going regulatory requirements ► Ethical considerations, including how to manage small- and medium- sized third parties with the variation of demand through the pandemic

4. Now: Third party operational resilience

The interconnected landscape of today's business environment poses serious risk of disruption that can result in significant loss of revenue. Organizations need to evaluate the ability of their critical off-shore presence and third-parties to continuously support critical functions such as IT, human resources, payroll, financial reporting, cybersecurity and others.

How EY teams can help?

EY COVID-19 Third-Party Risk Management Assessment offering provides a rapid, scalable and automated assessment to evaluate and monitor third-party risks due to COVID-19. This will help enable the organization to assess the impact to their critical third parties and understand how they are responding to continuously support key IT and business operations in a rapid and efficient manner. As a result of COVID-19, it is increasingly important for these assessments to take place rapidly and dynamically.

The approach includes three phases:

1. Plan

Identify and prioritise third parties providing critical services to your organization.

Confirm third-party status and services, and any reach outs performed with internal third-party relationship owner(s).

Leveraging TPRM technology, launch the COVID-19 assessment questionnaire to third-party contact(s).

2. Assess

Gather information from third parties to understand the impact and how they are responding to COVID-19. The assessment includes the following areas but not limited to:

- Business continuity / pandemic plan
- Remote access for Work-From-Home (WFH) resources
- Network security and operations management
- Security event management
- Dependency on fourth parties

3. Respond and monitor

Summarise and review the third-party responses.

Evaluate the impact and ability of third-parties to support the organization's critical functions.

Develop recommendations and report on evaluation results.

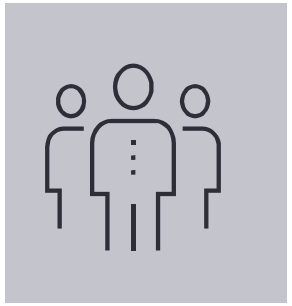
Support the triage and monitoring of agreed key actions.

5. Next: Third party financial resilience

At a time when industries are severely stressed, contingency plans developed in better times are proving to be ineffective. In this environment, firms are subjected not only to the financial health of immediate third parties, but also to the collective financial positions of all those which their third parties rely. With complex supply chains and deteriorating market conditions, the risks today are an order of magnitude greater than in prior years. Firms need to deploy significantly greater resources toward identifying third parties experiencing financial duress, and even more, finding the best ways to deal with these heightened risks.
As a direct result of COVID-19, firms will also need to consider existing financial arrangements and refund procedures if third parties cannot continue to operate.

Life cycle of a distressed third party

An effective program of identifying and managing the risks of a distressed supply chain can be described in three principle or workstreams

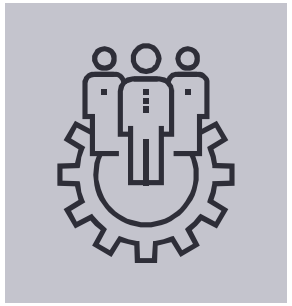


Early warning screening system

Operational, financial and qualitative metrics used to profile third parties based on risk level

Troubled third party risk assessment

Detailed risk assessment and mitigation planning for third parties which pose significant risk



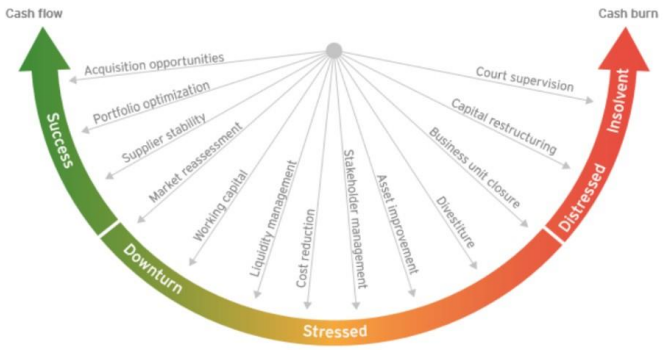
Distressed third party management

Further evaluation and review of distressed third party with a view to protecting supply

Companies need to think in terms of both near- and then longer-term actions. Companies need to be prepared to, where necessary, take more dramatic action.

The EY Stress Pendulum gives an indication of the typical stability monitoring and risk mitigation processes which exist to support companies in such adversity as a result of COVID-19

Stress pendulum



6. Beyond: Learning from COVID-19 and the future of TPRM

1

Enhanced awareness and reporting

COVID-19 has brought a dramatic insight into the business continuity and operational resilience of third parties. We expect organizations to adopt an approach to TPRM that is **increasingly data driven, proactive and action oriented**, drawing on the strengths of machine learning (ML) and artificial intelligence (AI). Client will be facing rejuvenated regulatory pressure, which will consider the proportional and appropriate management of third parties.

2

Technology

Organizations are increasingly looking to the technology to **improve the end to end TPRM programme** across the three lines of defence, and also help tackle the nth party challenge. COVID-19 has highlighted the need for enhanced BAU TPRM activities, naturally enabled by technology, whilst technology will be able to support with root-case analysis and simulations.

3

Collaboration

Any incident emphasizes the need for increase collaboration, both internally (between functions and divisions) and externally (across the industry). Internal and sector-based external utilities which more efficiently manage third party risks, and at a lower cost, will continue to feature.

7. Key Contacts

Kanika Seth
Partner, Ernst & Young LLP
EY EMEIA FSO TPRM Leader
kseth@uk.ey.com

James Ellery-Gower
Senior Manager, Ernst & Young LLP
EY EMEIA FSO TPRM
jgower@uk.ey.com

Shriparna Ghosh
Senior Manager, Ernst & Young LLP
EY EMEIA FSO TPRM
sghosh2@uk.ey.com

Appendix

Now: Third party operational resilience – What can you do?

TPRM lifecycle

Execute rapid end-to-end TPRM processes on behalf of the client

Integrate all EY leading methodologies and enablers

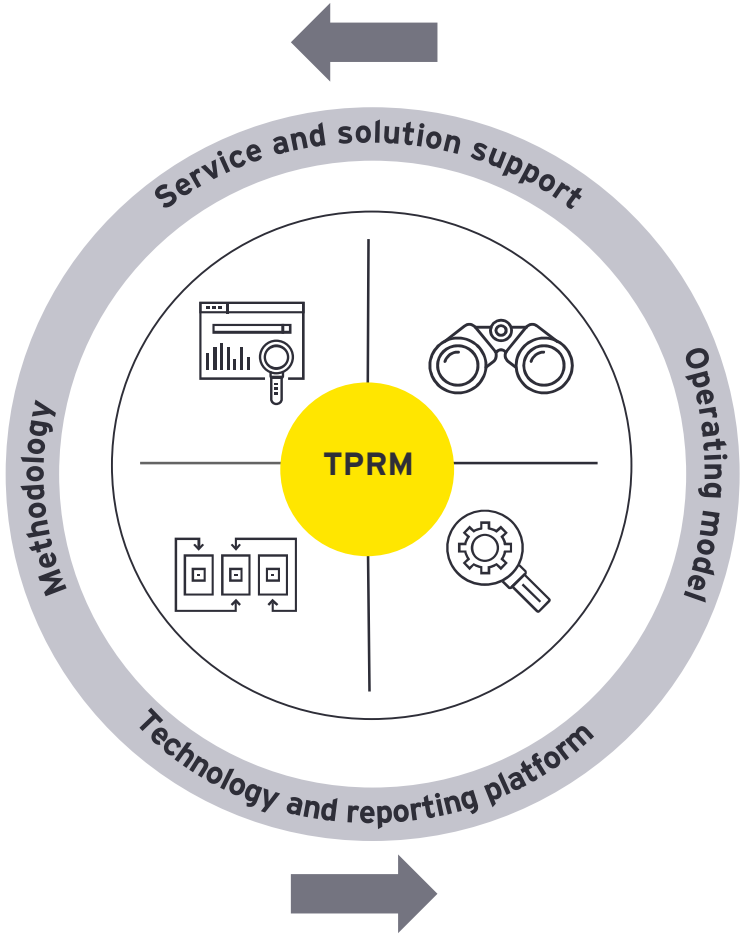
Supported by a technology platform, (for client, third parties, EY)

1. Plan

- Assessment intake process facilitated by either the EY baseline methodology or directly using the organization's existing methodology
- Third-party's product and service risk profiling using a targeted scope COVID-19 questionnaire

2. Assessment execution

- Rapid assessment planning and coordination
- Execution of remote global third-party risk assessments in 5+ risk areas including Information Security, Privacy, Business Continuity and Regulatory Compliance
- Residual risk calculation



4. Monitor

- Development of service risk profile reassessment timeline (e.g., every 2 years)
- Establishment of third-party risk assessment monitoring approach (based on residual risk rating)
- Data mining looking for supplier chain linkages

3. Respond

- Risks and findings monitoring, from registration to closure
- Evaluate the impact and ability of third-parties to support the organization's critical functions

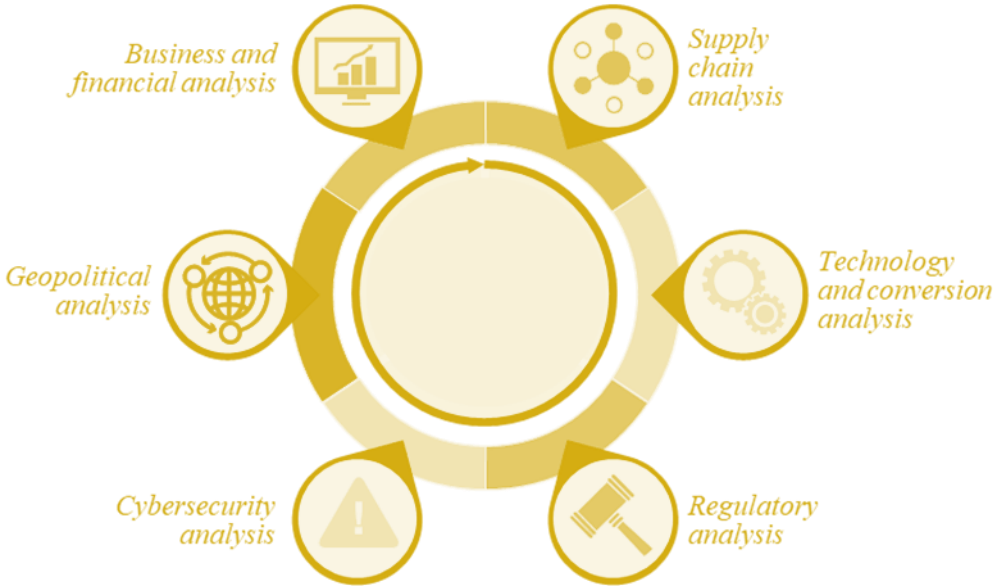
Next: Third party financial resilience – What can you do?

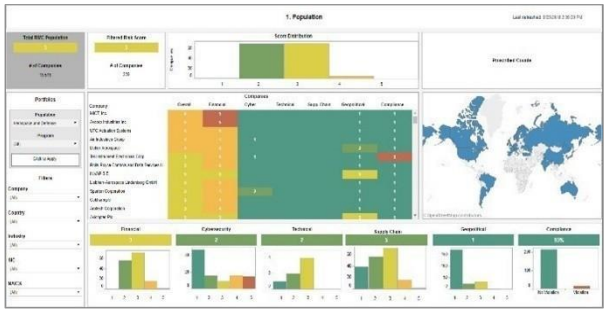
What is BRETA?

EY business relationship and economic threat analysis (BRETA) capability focuses on identifying and triaging business, economic and operational-related risks across a client's ecosystem of business relationships (customers, suppliers, joint ventures, partnerships, etc.). BRETA leverages the firm's experience across six disciplines (financial, technical, regulatory, supply chain, cyber and geopolitical) to provide a multi-dimensional view of risk and potential mitigation strategies.

How is it used?

The automated tool assists clients with threat screening, exploratory analysis and risk scoring of individual entities or sub-populations. This differentiated capability uses publicly-available data sources to produce comprehensive reports. The reports feature interactive visualisations of market trends, business relationships, location and geographic data, market transactions and automated aggregation and analysis of key indicators of financial health to rapidly identify where threats or vulnerabilities exist.





TPRM market dynamics: key trends of 2020

1 Resilience of third parties

Significant business disruption as a result of COVID-19 highlights the need for organizations to have a clear understanding of the resilience of their third parties

2 Growing market interest

TPRM started off being a focus for financial services due to regulatory requirements and has since moved to other regulated sectors

3 Board level attention

Third party risks are being discussed at the board level, and more board members are becoming aware of the topic and need

4 Expanded risk landscape

Organizations have expanded their risk focus from IT/information security risk to a broader, more inclusive risk landscape

5 Integrated TPRM function

Organizations are setting up an integrated TPRM function comprised of procurement, supply chain, legal, compliance and IT

6 Operating model evolution

Organizations are reducing in-house reliance and moving toward co-source arrangements or fully managed services

7 Common frameworks

Organizations are moving toward standardising third party assessment methodologies and processes

8 Technology-enabled Intelligence

There has been a movement from manual activities to on-premise technologies to utilising software as a service cloud based solutions, where risk data is increasing being used to provide procurement and supply chain insights

TPRM framework: It is become more important than ever to deliver robust third party risk management, utilising an enterprise-wide framework

A TPRM function is comprised of six functional components that enable efficient, consistent and enterprise-wide execution.

The **operating model** defines clear roles and relationships supportive of consistent, risk based application of all functional enterprise-wide TPRM process.

Risk models help ensure monitoring activities are reflective of the inherent/residual risk associated with third parties and their services – essential in quantification and illustration of TPRM programme value.

Monitoring is the periodic assessment and management of risk and service performance relative to a third party and the services provided once contracted.

Risk assessment and due diligence are essential.to understand the third parties control environment around identified risks (e.g., enterprise resilience, cyber security, regulatory compliance, etc.)

Oversight and governance is the component that oversees the function to ensure that the relationships and activities are managed effectively. This consists of the following sub components: reporting, issue management and escalation, internal and external programme liaison, quality assurance and policy adherence.

Technology and data enable TPRM processes to reduce overall function cost. Additionally, the use of technology increases data integrity and drive seamless and reliable reporting.

Enterprise-wide **policy and procedures** establish clear roles and responsibilities for all functional owners through the execution of the end-to-end TPRM lifecycle. More mature functions embed service/risk management within third party management policy/procedures for stream-lined integration and execution.

41% of firms said primary ownership of the TPRM function falls within procurement (1st line of defense) – 2018 TPRM survey

Regulatory requirements: The EBA outsourcing regulatory requirement provides a framework to assess, govern and monitor third parties

Core Considerations:

Regulatory Deadline

- Finalised version of EBA guidelines were made available March 2019
- The guidelines apply from 30 September 2019 to all outsourcing arrangements entered into on or after this date
- Complete documentation for all existing contracts must be completed by first renewal date of each contract, but no later than 31 December 2021

Proportionality

- Institutions are expected to apply the principle of proportionality to achieve the requirements, by applying governance that aligns with the nature, scale and complexity of the operations
- Management body of the institutions retains full responsibility for the regulatory requirements

Outsourcing arrangements

- Institutions are required to establish if an arrangement with a third party falls under the definition of outsourcing, and if this constitutes the outsourcing of a critical or important function

Outsourcing to cloud

- EBA outsourcing standards for cloud service providers have been applicable since 1 July 2018 and have been embedded into EBA outsourcing guidelines to set the supervisory expectations for services outsourced through cloud

EBA emphasizes the following aspects of outsourcing arrangements by institutions

The institution retains full responsibility and accountability for complying with applicable regulatory obligations

Institutions are required to have an outsourcing policy in place

Institutions should identify, assess and manage conflicts of interest

Institutions are required to have Business Continuity Plans available with regard to the outsourcing of critical or important functions

The internal audit activities should cover the independent review of outsourced activities following a risk based approach

Institutions should maintain a register of all outsourcing arrangements, critical or otherwise

Pre-outsourcing analysis should be performed for all outsourcing arrangements covering:

- Assessment of the criticality of importance
- Due diligence
- Risk assessment

The respective rights and obligations of the institution and service provider should be clearly allocated and set out in a written agreement

Institutions are required to monitor the performance by the service provider with regard to all outsourcing arrangements

Institutions should have a clearly defined exit strategy for all outsourcing of critical or important functions

Institution should provide the relevant authority with the register of outsourcing arrangements

Regulatory requirements: The PRA consultation paper requires an enhancement of the oversight of third parties to help improve their operational resilience

Case for change

- **Greater reliance** is being placed on third parties and increasingly on technology providers, e.g., Cloud
- **Firms face increased risks,** e.g., storing, processing and/or sharing of customer data, long chains of service providers, regulatory reporting
- The evolving nature of **Outsourcing and TPRM brings benefits,** opportunities and potentially enhanced resilience if managed appropriately

Key objectives of the CP

- Modernises expectations
- Facilitates greater resilience
- Clarifies PRA expectations
- Final policy expected in the second half of 2020

Key concepts

- **Definitions** – material vs. non material outsources
- **Intra group** – no less risky than external arrangements
- **Governance** – responsibility cannot be outsourced
- **Data Security** – detailed requirements around security
- **Access, audit and information rights** – risk based approach and concept of pooled audits
- **Sub-outsourcing** – emphasis to assess this risk
- **Business Continuity and Exit** – importance of defining and testing approaches for stressed scenarios

TPRM market dynamics: EY FSO TPRM 2019 survey – The survey highlights the key challenges facing organizations and their response

Operating model

58% of organizations reported having a **centralised structure.**

38% of organizations reported having a **hybrid structure.**

Cybersecurity

38% of organizations had a **data breach** caused by a third party over the past 2 years.

52% of organizations had an outage caused by a third party over the past 2 years.

Tools and technology

40% of organizations have a TPRM technology platform. Over half of those that have links to **external threat intelligence data** or supplier data.

37% of organizations that use tools/technology as part of their TPRM programs indicate that technology across the organization is not integrated and requires **manual reconciliations** to report out of multiple systems.

Resourcing model

20 resources, on average, are **dedicated to supporting** the TPRM program/function.

54 resources within the business, on average, provide support to the TPRM program/function.

Execution

41% of organizations expect to use more of **managed services** to execute their TPRM program/function in 2–3 years.

65% of organizations expect to use more of **market utilities/exchanges** to execute their TPRM program/function in 2–3 years.

57% of organizations expect to use more of **sector-based consortiums** to execute their TPRM program/function in 2–3 years.

Fourth-party management

70% of organizations rely on the contractual terms established with the third party to assess/monitor fourth parties

Inherent risk

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

Assessments

83% of organzsations reassess (risk/control assessment) critical third parties on an annual basis

EY thought leadership: examples

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.

EYG no. 001562-20Gbl

EY-000119124-01 (UK) 03/20. CSG London.

ED MMYY

ey.com/