



# Third-Party Risk Management (TPRM)

**Let's do this.**

NATIONAL BANK OF CANADA



# Global trends in TPRM

Significant changes in the external environment (i.e. technology, regulatory) are leading to rapid evolution in the risks related to Third Parties.

## Operating Model

- Further formalizing a consistent approach to TPRM that is comprehensive, materiality based and with clear roles and responsibilities, starting with the Board to the Business Units. The operating model is substantiated by specific frameworks and procedure documents.
- Including considerations for compliance with General Data Protection Regulation (GDPR) in third party sourcing, due diligence and ongoing monitoring by verifying that third parties gathering personal information from EU citizens obtain appropriate consent.
- Ensuring that all key third party risks are considered and assessed throughout the end-to-end lifecycle – from pre-deal to off boarding.
- Providing the Board and Management with an aggregated view of all third party risk exposures (including remediation plans for high risks and due dates) to enable effective risk oversight and decision making.

## 4<sup>th</sup> Parties and more...

Beyond 3<sup>rd</sup> party risk, leaders are subject to 4<sup>th</sup> (5<sup>th</sup>, 6<sup>th</sup>, etc.) risks. Most 3<sup>rd</sup> parties use their own contractors, and most organization have no legal contracts with these 4<sup>th</sup> parties.

Risks related to information security, such as data breaches, can be significant outcomes of 4<sup>th</sup> party risks.

## Blockchain

Organizations in blockchain-enabled ecosystems are streamlining vendor qualification, onboarding, validation and monitoring by getting immediate access to current and accurate pre-verified supplier data and questionnaires.

Blockchain serves as the decentralized data layer that guarantees trust via cryptographic security, and privacy via permissioned access.

## Outsourcing

Some large players are partially or completely outsourcing their 3<sup>rd</sup> party risk monitoring activities. This is done in an effort to reduce costs and improve their flexibility and efficiency.

## Machine Learning

The use of machine learning to analyze 3<sup>rd</sup> parties, and more importantly, automatically and continuously update the details of partners' risk exposures, has developed into mature tools and software that are consistently improving. Some leading uses and capabilities of machine learning tools include:

- Management of AML, leveraging Financial Crimes technology and human expertise
- Sanctions and reputation of all parties (employees, clients, providers, suppliers, etc.) by scanning for sources such negative news, social media, court appearances,
- Automated exclusion of false positive results

## Adoption of Technology

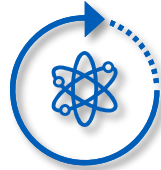
Technology solutions are used to support a centralized TPRM operating model and enable an end-to-end risk management approach of 3<sup>rd</sup> parties for pre- and post-contracting activities.

# Business need for a structured TPRM



## Manage Existing and Emerging Risks

- Manage the various **emerging risks related to third party activities** (e.g. privacy, cybersecurity, climate change etc.)
- Protect reputation, data as well as corporate assets and intellectual property
- Manage regulatory and compliance risks
- Implement **risk based approaches** through an effective third party risk management program that aligns with overall strategic objectives



## Innovation

- Manage risks related to non-traditional third parties, such as technology start-ups and Fintech companies, which are **increasingly delivering critical services to organizations**
- Need to maintain adequate balance between innovation and risk as emerging standards, such as Open Banking, enable unprecedented innovative services.
- Understand interconnected service delivery impact on resilience (as multiple Third Parties are involved **in delivering a single customer experience**)
- Incorporate utilities, scoring tools, and other technologies to augment TPRM headcount to **achieve automation and efficiency**



## Operational Efficiencies

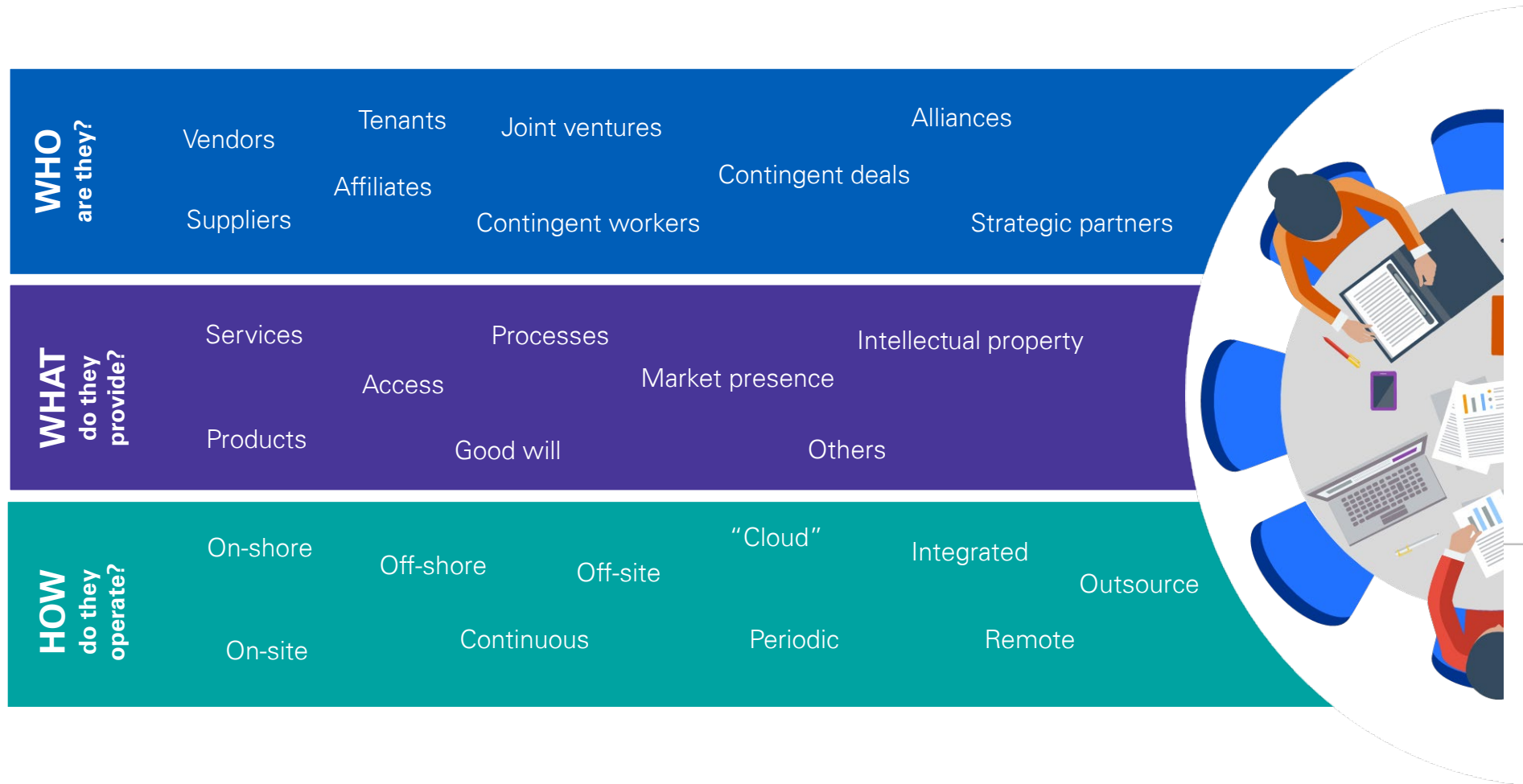
- **Consistent management and integration** of risk activities **across different organizational** functions throughout the life cycle of a Third Party
- Minimize service disruptions or delays by effective oversight of Third Parties
- **Increase efficiencies** to go to market faster (e.g. optimizing processes and enabling technology)



## Global Operations

- Greater understanding of the **network of Third Parties** across an organization and **across different geographies**
- Increased **consistency of practices** over the treatment of Third Parties
- **Cost-effective and sustainable approach** to Board reporting via a comprehensive view of Third Parties, strategy, trends, and issues

# A broad definition of 'third parties'



## Examples of third parties:

- Cloud Providers
- Payment processors
- Document Storage
- Professional Services
- Agents of your business
- Fintechs
- Data and System Providers

## Not third parties:

- Customers
- Regulators

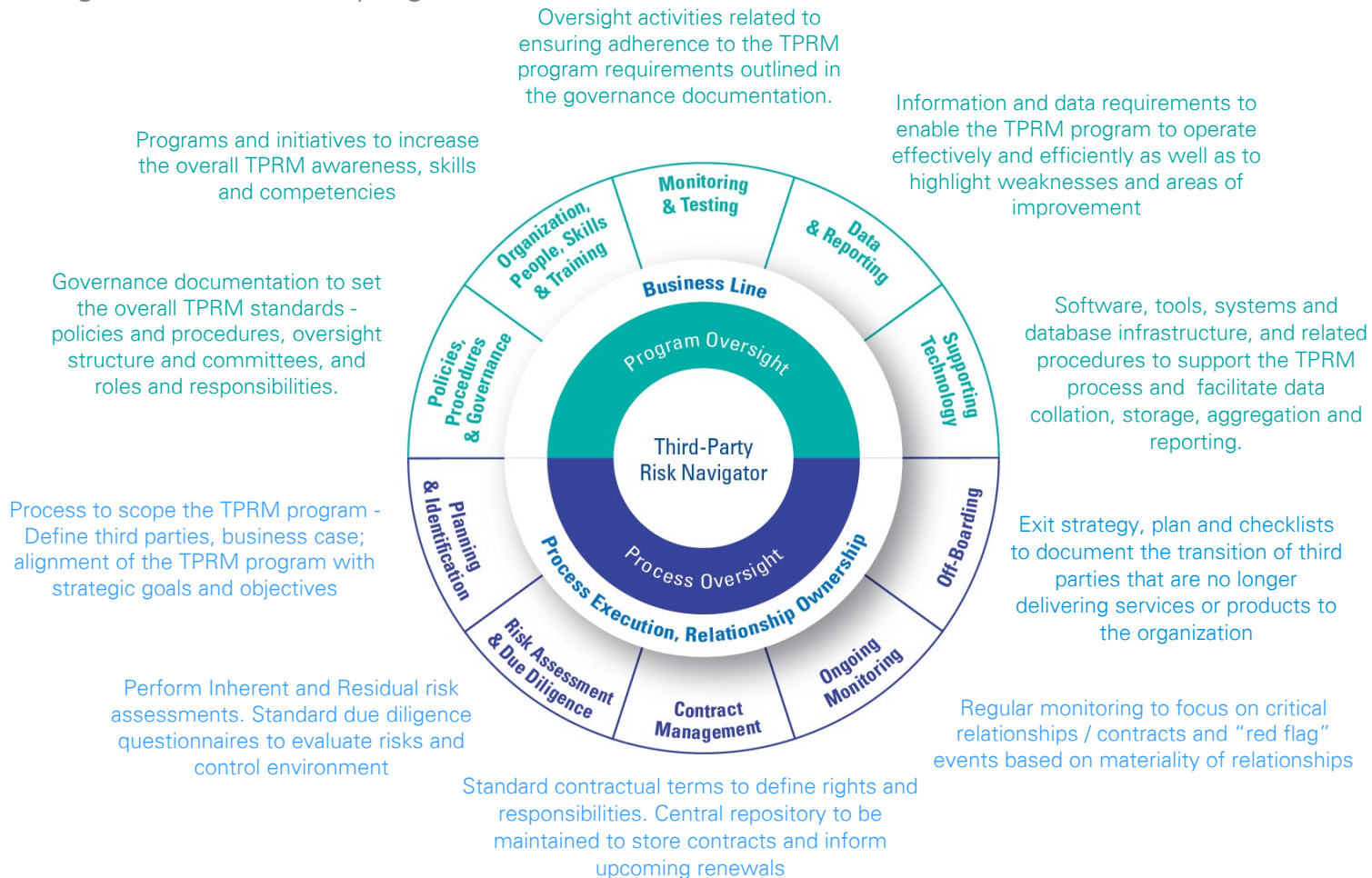


Remember risk is assessed at the level of the service being provided



# TPRM Overview & Objectives

Our Third Party Risk (TPR) Navigator framework is built along the three lines of defense model to provide a holistic framework to identify risks, strengths and weaknesses of an organization's TPRM program



## Key Objectives

- Provide the Board and Senior Management with the appropriate level of information (aggregated and materiality based) to determine the **organization's tolerance and exposure to third party risks**
- Embed a **structured and consistent approach** to coordinate and execute the management and control of third party risks (e.g. criticality criteria, questionnaires) throughout the end-to-end third party life-cycle (pre and post contracting)
- Provide **clarity on internal roles and responsibilities** for managing third party relationships and associated risks in line with 'good governance' principles (e.g. independence)
- Gain greater visibility **over key (material) third party risks** and focus resources on third parties that deliver services that are critical to the organization's strategy
- **Reduce inefficiencies / redundancies** from fragmented approach to managing and evaluating third parties' risks
- Help the business **consolidate, streamline and analyze third parties** for cost savings and more negotiating power with vendors
- Ensure that TPRM is designed effectively to **provide continued confidence to stakeholders** that risks are well managed

# Potential areas of third party risks

## Regulatory/Compliance Risk

- Regulatory requirements
- Theft/Crime/Dispute Risk
- Fraud, Anti-bribery and Corruption/Sanctions
- Compliance with internal procedures and standards
- ESG requirements

## Strategic Risk

- Service delivery risk
- Expansion/roll-out risk
- Mergers and acquisitions
- Alignment to outsourcing strategy
- Intellectual property risk

## Subcontractor Risk

- Applicable across all risk areas

## Concentration Risk

- Supplier concentration across critical services
- Industry concentration (incl. subcontractor)
- Concentration of critical skills (i.e., tech support)
- Geographic concentration
- Reverse concentration

## Technology/Cyber Risk

- Information security
- Cyber security
- Data privacy/data protection

## Financial Viability

- Financial risk from lending to a third party
- Liquidity risk
- Credit Risk

## Operational/Supply Chain Risk

- Business continuity
- Disaster recovery
- Physical security
- Operational Resilience
- Performance management (incl. SLA's)
- Model risk
- Human resources risks (conduct risk, etc.)

## Reputational Risk

- Negative news
- Lawsuits (past and pending)
- Brand of the third party
- Key principals/owners of the third party
- Workplace safety

## Legal Risk

- Jurisdiction of law
- Terms and conditions of the contract



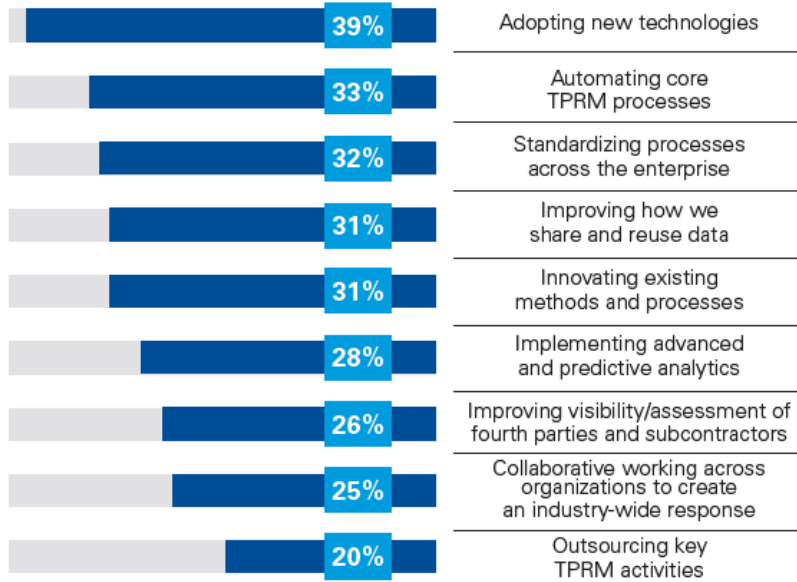
## Country Risk

- Geopolitical risk
- Climate sustainability

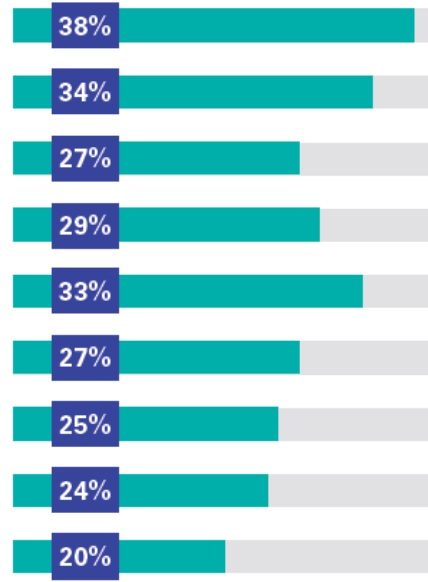
# TPRM Industry Perspective



## Next 12 months



## Next 3 years



Source: Third Party Risk Management outlook 2020, KPMG International 2020

## Where are financial services firms on their TPRM journey?

### 1. Pre financial crisis

- Lack of industry consensus on target operating model for TPRM programs



### 2. Initial program build subsequent to regulatory guidance (2013–2019)

- Regulatory-driven remediation
- Headcount and volume of risk assessments increase dramatically
- TPRM programs reach business as usual status
- Integration efforts with the broader enterprise risk management and operational risk priorities



### 3. Tuning and streamlining (2019 and beyond)

- Consensus builds to streamline and right-size TPRM programs
- Experimentation with new operating models
- Regulatory focus shifts to operational resiliency and affiliate risk management
- Industry adoption of third-party utilities



# An effective TPRM framework is built on 4 pillars

To holistically transform a TPRM program across these four pillars, businesses need to drive a constant cycle of program uplift, process optimization and innovation – agree on the vision, build the model, optimize and evolve.



## Governance

57% say they are a long way from having an enterprise-wide agreement for services that can and cannot be outsourced.

- Do you have a single leader of your TPRM program?
- Is there a formally defined reporting structure, including clear roles and responsibilities?
- Have you established an outsourcing and third party strategy, and a defined risk appetite?
- Are the TPRM policies and standards aligned to the risk appetite?
- Is the scope and focus of the TPRM program formalized?



## Process

67% say TPR assessments are carried out by numerous resources across the organization, as opposed to one person or team.

- Are TPRM activities consistently executed?
- Does your team possess the right mix of skills, expertise and capacity?
- Have you established a risk-based approach aligned to the risk appetite?
- Do you perform risk assessments prior to engagement?
- Do you continuously monitor your third parties over the lifetime of contracts?
- Have you considered fourth parties?



## Infrastructure

24% are using automation to enhance efficiency by carrying out routine tasks.

- Does your technology architecture support efficient workflow, task automation and reporting?
- Does your infrastructure enable a documented and well-understood audit trail?
- Is your service delivery model aligned to the operating environment (centralized vs. distributed)?
- Are TPRM activities and technology integrated with core processes (e.g. procurement, legal, finance), and into existing risk oversight functions and activities?



## Data

Less than 50% are very confident in their electronic inventories of third- party contracts, risk monitoring and reporting, and inventories of third parties.

- Do you collect real-time data?
- Have you established a comprehensive data model?
- Have you established internal and external data feeds?
- Are third party risk profiles updated in real-time for changes to their risk and control environment?
- Do you track performance against SLAs and KRIs in real time?
- Have you established a process for data-driven decision making?

To make this happen, there are **four key steps** businesses must take: **agree on the vision, build the model, optimize and evolve.**










# Where Organizations Fail in Designing and Implementing TPRM

A successful TPRM program, crucial to the success of organizations, should have access to the latest trends, information and the right practices in place to ensure the right level of oversight. When these elements lack, we see shortfalls that come in various forms:

Points of Failure	Description
Ineffective Risk Operating Model (Viewing risk in silos vs. an integrated approach)	An efficient and effective strategy for governing and defining risk in third-party relationships is only possible when risk management functions are integrated for a more robust impact, and roles and responsibilities are clarified.
Insufficient due diligence when onboarding new Relationships and off boarding procedures	Companies must engage in “risk based due diligence” and perform a holistic assessment of the third-party partners and sub-contractors. Procedures needs to be established to outline offboarding of third parties
Absence of ongoing risk monitoring	Expectations for third party reporting should include criteria, frequency and key metrics. It is important that such requirements are not static and are frequently adjusted to reflect the changing environment.
Insufficient safeguards for third-parties in your network	Effective and proactive information security practices are critical to keeping a company’s information safe, and are often inadequate when it comes to third-party risk management.
Thinking your paper program keeps you safe	Without a robust implementation and review methodology, even well-designed policies and programs may prove unfit in the event of a reputation-damaging risk event.

# COVID-19: TPRM Considerations

As the COVID-19 pandemic continues to grow with significant impact on the global economy, organizations relying on third parties to provide critical services are taking immediate actions to determine the possible risks these parties may present to their businesses in order to mitigate potential impacts from COVID-19.

Key Risks		Key Considerations	Potential Response Strategies
	<b>Business continuity and resiliency risk</b>	<ul style="list-style-type: none"> <li>- Are the third party's business continuity measures working for my organization in the current situation?</li> <li>- Is the third party effectively executing business continuity plans and providing urgent deliverables?</li> </ul>	<ul style="list-style-type: none"> <li>- Identify third parties critical to business as usual</li> <li>- Obtain and review third party business continuity and pandemic plans</li> <li>- Review vendor concentration at your organization</li> <li>- Obtain evidence of going concern from key third parties</li> </ul>
	<b>IT and Cyber Risk</b>	<ul style="list-style-type: none"> <li>- Does the third party have the technology capabilities to continue providing services in situations like mandatory work from home?</li> <li>- Are information and cybersecurity risks being adequately addressed by the third party?</li> </ul>	<ul style="list-style-type: none"> <li>- Review third party cyber response strategy to COVID-19</li> <li>- In consideration of above response strategy, review potential information security and data privacy impacts</li> </ul>
	<b>Key person risk</b>	<ul style="list-style-type: none"> <li>- What steps have been taken to manage the key person risk at the third party?</li> </ul>	<ul style="list-style-type: none"> <li>- Identify backup personnel for third party relationship</li> <li>- as well as critical talent pool impacting third party deliverables</li> <li>- Ensure pandemic plan strategy addresses internal third parties (e.g. contractors)</li> </ul>
	<b>Fourth party risks</b>	<ul style="list-style-type: none"> <li>- How much does my organization know about third party's reliance on its suppliers and vendors?</li> </ul>	<ul style="list-style-type: none"> <li>- Review the vendor inventory and contracts to identify and confirm fourth parties</li> <li>- Discuss potential impact of fourth party business disruptions with your third party service providers</li> </ul>
	<b>Inadequate service provider monitoring</b>	<ul style="list-style-type: none"> <li>- How can my organization effectively monitor third parties, including their financial stability and performance?</li> </ul>	<ul style="list-style-type: none"> <li>- Establish critical short-term milestones and risk indicators for the third parties</li> <li>- Schedule relationship meetings or calls with key third parties</li> <li>- Stay aware of potential implications to third parties</li> </ul>

# KPMG's TPRM Service Offering

KPMG offers an extensive suite of TPRM services to support your organization in the end-to-end TPRM lifecycle based on the current and target maturity.

## Foundational Services

Focus on the Program Oversight areas of TPR Navigator to ensure a strong foundation. These foundational elements enable a consistent, risk-based approach to TPRM across organization.

- ✓ Provide benchmarking of TPRM against leading practice
- ✓ Designing TPRM Operating Model to define target-state
- ✓ Define outsourcing risk philosophy in alignment to the organization's strategy
- ✓ Establishment of TPRM Framework, policies and other governance documents
- ✓ Auditing of TPRM Framework and performing vendor reviews
- ✓ (+...)

## Tech. Enablement & Automation

Spans across the Program and Process Oversight areas for efficiency and precision. The focus is on enhancement through technology solutions and automation to accelerate processes, reduce errors and promote standardization.

- ✓ Technology transformation and enablement
- ✓ Strategic alliances with major technology service providers
- ✓ Incorporating data analytics and monitoring tools to capture risk events in a timely manner
- ✓ Blockchain enablement in TPRM
- ✓ (+...)

## Lifecycle Execution Services

Focuses on the Process Oversight areas of TPR Navigator for robust TPRM operations. Services range from improving individual components of TPRM to holistic Third-Party Risk-as-a-Service

- ✓ Cyber Security analysis
- ✓ IT General Control Assessment
- ✓ Business Continuity assessment
- ✓ Fraud risk assessments
- ✓ Climate change risk assessment
- ✓ Reputation Risk Assessment
- ✓ Regulatory Compliance evaluation
- ✓ (+...)

## Risk Intelligence Services

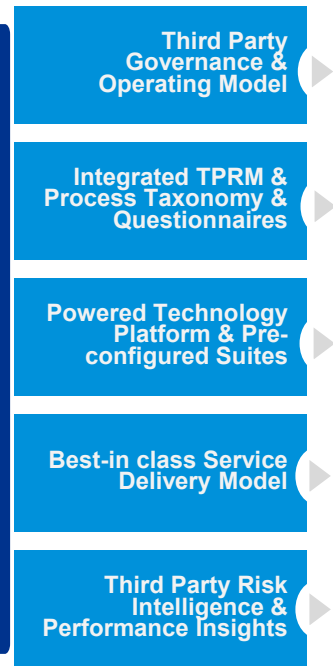
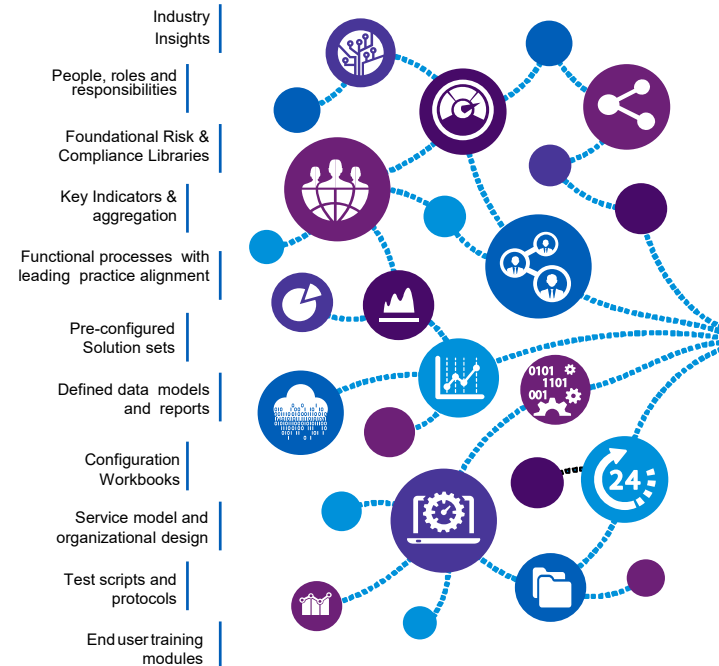
The focus is for organizations moving towards the mature end of the TPRM spectrum. It enables the use of data analytics, artificial intelligence and other emerging technologies for enhanced management, monitoring and reporting of third-party risks.

- ✓ Cognitive Technology Capabilities
- ✓ Data Analytics Capabilities
- ✓ Sanctions screening and transaction monitoring
- ✓ Emerging technologies including Blockchain, Robotics, Artificial Intelligence and IoT
- ✓ (+...)

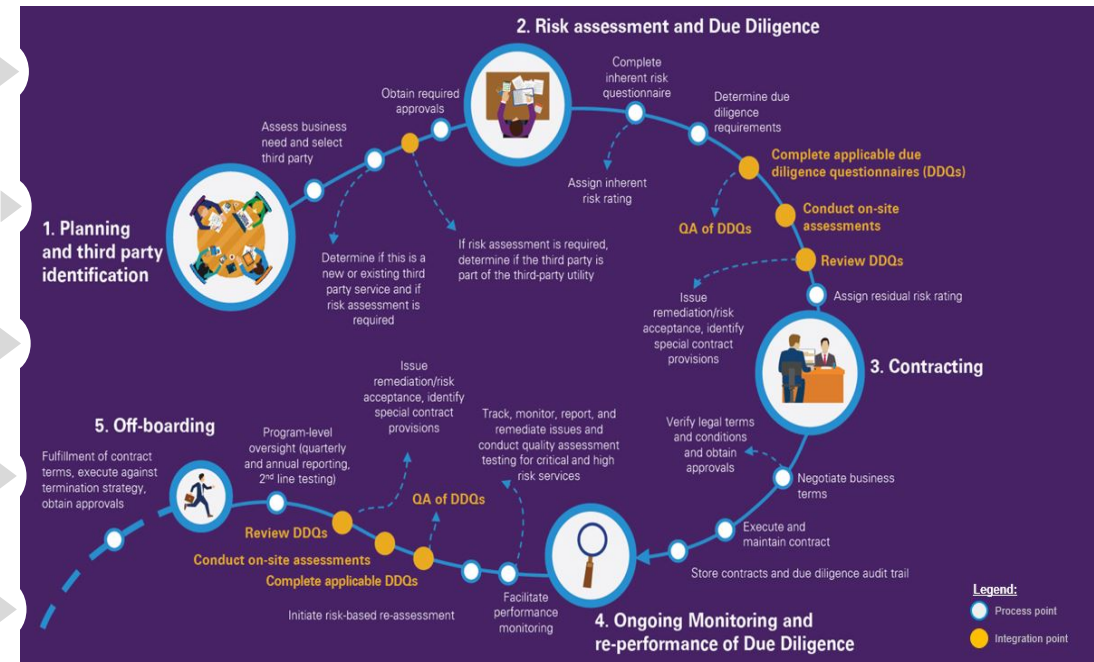
# Technology Transformation and Enablement

KPMG delivers a future-ready program transformation enabling clients jump start their transformation leveraging our target operating model and streamlined future state processes that are pre-packaged for use in leading cloud platforms

## Transformation Accelerators



## KPMG Technology Transformation



KPMG TPRM  
technology  
platforms &  
partners

### TPRM Process Automation

**MetricStream**  
PERFORM WITH INTEGRITY™

**servicenow**

**RSA** Archer GRC

**coupa**

### Third Party Risk Intelligence

**DOW JONES**

**BITSIGHT**  
The Standard in SECURITY RATINGS

**coupa**

**trdc**  
Smarter Screening

### Advanced AI Process Automation

**MetricStream**  
PERFORM WITH INTEGRITY™

**servicenow**

**sas**

**Microsoft**  
**Power BI**





# KPMG's TPRM Thought Leadership



**The problem**  
KPMG recognizes that organizations don't have the capacity, investment support or skills to effectively manage the diverse number of suppliers found in today's large corporations. This results in:

- the potential for a large (or public) cyber security breach, attributed to the cyber practice findings of a vendor
- lost value within commercial relationships (KPMG assesses estimates this can be up to 50%)
- increased risk exposure of supplier service failure or non-compliance, and
- failure to adhere to contractual obligations.

Compounding the problem is that not all supplier governance activities are continuous and therefore difficult to budget for and resource.

**Now we can help!**  
KPMG's Risk Consulting practice provides services that help organizations identify and manage vendor risk management, designed to help protect your organization from a cyber attack due to a weakness of your first party. KPMG has developed a suite of services to supplement the vendor security risk management function within organizations. This has the advantage of providing a cost effective, flexible service for:

- all gaps in organizational skills sets
- provide specialized advisors who understand vendor security management
- match the demand and supply of supplier governance activities, and
- manage supplier risks by focusing on a wider set of suppliers based on their risk profile.



**KPMG's vendor risk management approach**  
KPMG's Vendor Cyber due diligence is comprised of three specific areas of review and analysis:

- Internal risk assessment (company management)
- cyber capability and adherence to good security practices, and
- dark web reviews

KPMG is experienced in designing and implementing requirements of cyber security into third party contracts, and the ongoing process of assessment. KPMG is also experienced in performing post-incident, or critical cyber maturity assessments to assess the maturity of a third party's cyber program to address cyber risk as a business risk.



The COVID-19 pandemic continues to grow with significant impact on the global economy triggering business continuity and crisis management response across organizations of all sectors and sizes. Organizations relying on third parties to provide critical services should also immediate actions to determine the possible risks these parties may present to their businesses in order to mitigate potential impacts from COVID-19.

**Key considerations for effectively managing your third party risks during COVID-19**

Key risk	Key considerations	Practical Response Strategies
<b>Business continuity and resilience risk</b>	<ul style="list-style-type: none"> <li>Are there any third party dependencies on your business?</li> <li>Are there any third party dependencies on your business?</li> <li>Are there any third party dependencies on your business?</li> </ul>	<ul style="list-style-type: none"> <li>Identify the critical third party dependencies on your business.</li> <li>Classify and assess third party dependencies on your business.</li> <li>Review vendor concentration at your organization.</li> <li>Obtain evidence of general business health from third parties.</li> </ul>
<b>IT and cyber risk</b>	<ul style="list-style-type: none"> <li>Is the third party at risk of becoming breached?</li> <li>Is the third party at risk of becoming breached?</li> <li>Is the third party at risk of becoming breached?</li> </ul>	<ul style="list-style-type: none"> <li>Review third party cyber response strategy to COVID-19.</li> <li>In consultation of cyber response strategy, review potential information security and data privacy response.</li> </ul>
<b>Reputation risk</b>	<ul style="list-style-type: none"> <li>What are the reputational risks to your business?</li> <li>What are the reputational risks to your business?</li> <li>What are the reputational risks to your business?</li> </ul>	<ul style="list-style-type: none"> <li>Identify the reputational risks to your business.</li> <li>Identify the reputational risks to your business.</li> <li>Identify the reputational risks to your business.</li> </ul>
<b>Supply chain risk</b>	<ul style="list-style-type: none"> <li>How much does the organization know about third party risks in the supply chain?</li> <li>How much does the organization know about third party risks in the supply chain?</li> <li>How much does the organization know about third party risks in the supply chain?</li> </ul>	<ul style="list-style-type: none"> <li>Review the supply chain and contracts to identify and control third party risks.</li> <li>Classify and assess third party dependencies on your business.</li> <li>Review vendor concentration at your organization.</li> <li>Obtain evidence of general business health from third parties.</li> </ul>

**Contact us**  
KPMG can assist with Third Party Risk Assessment to identify the highest risk areas and third parties and suggest critical mitigation actions.

**Global Team**  
KPMG Global Risk Consulting  
10000 Lakeside Drive  
Suite 1000  
Dallas, TX 75260  
USA  
KPMG@kpmg.com

**Regional Teams**  
KPMG Canada Risk Consulting  
10000 Lakeside Drive  
Suite 1000  
Dallas, TX 75260  
USA  
KPMG@kpmg.com

**Regional Teams**  
KPMG Australia Risk Consulting  
10000 Lakeside Drive  
Suite 1000  
Dallas, TX 75260  
USA  
KPMG@kpmg.com



**Today's reality**  
Businesses across every industry are increasingly compelled to rely on a robust network of third parties, such as vendors, suppliers, distributors, agents, joint ventures, alliances, subcontractors, and service providers. This network is critical to maintain a global footprint and effectively compete in the marketplace.

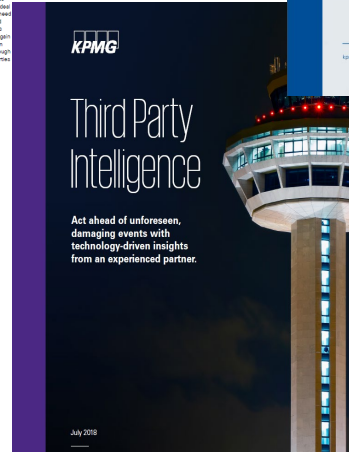
While third parties are imperative to operate globally, the risks associated with third parties cannot be overlooked. There are numerous cases where lack of proper oversight of third parties has resulted in serious consequences. Global companies have been exposed to significant risks, adversely affecting their performance and reputation.

**Complying with regulators' demands**  
Regulators across the globe expect companies to have effective oversight of their third parties. Companies have had to prioritize and enhance their compliance efforts as a result of notable enforcement actions and fines due to instances of money laundering, money laundering and anti-money laundering, money laundering and anti-money laundering, money laundering and anti-money laundering. In fact, a majority of money laundering cases are attributed to third parties. Companies have focused heavily on third-party intermediaries.

Various regulators focus on elements of the third party due diligence, risk assessment, due diligence, monitoring, and ongoing assessment as they relate to the effectiveness of compliance programs. The U.S. Department of Justice (DOJ) and the U.S. Securities and Exchange Commission (SEC) issued a joint guide that indicated how risk-based due diligence is particularly important with third parties and will be scrutinized when assessing the effectiveness of a company's compliance program. In addition, the DOJ recently provided detailed guidance around the Evaluation of Corporate Compliance Programs.

The oversight and monitoring of the third party due diligence has evolved from a reactive approach to one of alignment to a more proactive compliance program. In order to achieve this compliance, third parties risk management (TPRM) programs need to expand beyond the procurement function and encompass other departments and departments across the enterprise. These programs will also gain maturity as organizations view the organizational leverage data and an understanding of risk through technology to enhance management of third parties in a sustainable manner.

<https://www.kpmg.com/au/issuesandinsights/articlespublications/forensicfocus.aspx>





[kpmg.ca](https://kpmg.ca)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, an Ontario limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

All rights reserved. The KPMG name and logo are registered trademarks of KPMG International.

## TPRM is a strategic priority



## Companies are inconsistent in their approach to TPRM



## A risk-based approach is the number 1 'get right' for TPRM programs



76%



say TPRM is a strategic priority for their business given the direct link between reputation and the performance of third parties.

77%



50%



59%



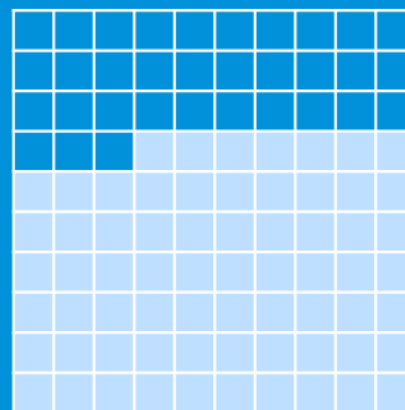
have recently been subject to regulatory enforcement and / or action in respect of TPRM.



67%



74%



urgently need to make TPRM more consistent across their enterprise.

65%



61%

believe their TPRM is undervalued

64%



72%

urgently need to improve how they assess 4<sup>th</sup> parties

59%



68%



believe they are exposed to brand and reputational risks due to inefficiencies in their TPRM program



31%



say Risk Management is responsible for TPRM.

30%



16%



say Risk Management provides the 2<sup>nd</sup> line of defence for TPRM.

21%



### Risks covered by TPRM

60%

Financial

51%

Regulatory & Compliance

60%

Operational

54%

Data & Privacy

45%

Reputation & Brand

52%



50%



do not have sufficient capabilities in-house to manage all the third party risks they face.



Source: [Global Third Party Risk Management Outlook \(KPMG International, 2020\)](#)

## Data and technology are improving TPRM's performance



## It's time to sustainably scale the TPRM program



## An effective TPRM program is built on 4 pillars



23%  
24%

are using technology to improve automation or monitoring of third parties.



60%  
61%

say technology is the most favoured investment when new funding is made available.

61%



46%  
38%

see new technology as a priority over the next 3 years

29%  
34%

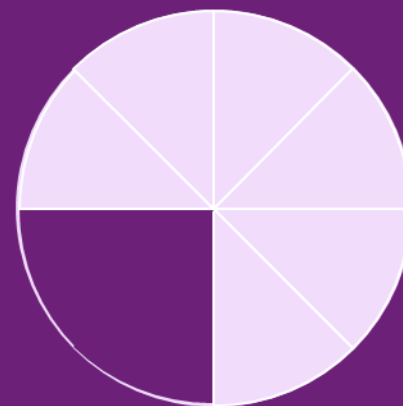
see automation as a priority over the next 3 years

62%  
51%

of businesses are working with limited budgets despite the increased focus on the use of third parties.



77%  
76%



say that funding is available or growing to strengthen and evolve their TPRM program.



### Governance



### Process



### Infrastructure



### Data

Source: [Global Third Party Risk Management Outlook \(KPMG International, 2020\)](#)