OLIVER WYMAN

POINT OF VIEW

MANAGING THE EXTENDED ENTERPRISE

ENABLING EFFECTIVE AND TIMELY THIRD PARTY RISK MANAGEMENT

AUTHORS

Elizabeth St-Onge, Partner

Swati Sawjiany, Partner

The Global Financial Crisis exposed the need for improved and more stringent risk management practices at Financial Institutions (FIs) world-wide, specifically operational risks focused on people, processes, data and systems. In addition, it's no longer enough for FIs to control their own business activities, or even those of immediate providers; today, operational risk management must include the complete ecosystem of providers, solutions, vendors and partners involved (even second-hand) in the institution's operations.

Internally at various institutions, the management and governance of third party relationships fall under the purview of multiple functions within Lines of Business, Risk, IT, Information Security, Procurement, Compliance etc., ideally with oversight from Executive Committees and Board of Directors. This layered and matrixed web of ownership makes Third Party Risk Management (TPRM) even more complex.

MARSH & McLENNAN COMPANIES

FIs are also facing increasing pressure from the regulators, to ensure a commensurate level of risk management and discipline with third parties (defined by the OCC as business arrangements between a bank and another entity, by contract or otherwise) as they do with internal functions and activities. ***This paper provides a framework for CROs, COOs, CIOs, CISOs, CPOs, and CCOs of FIs to collectively transform Third Party Risk Management (TPRM) capabilities in order to address regulatory concerns and maintain a strategic and competitive approach to delivering products and services.***

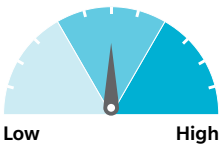
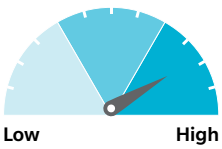
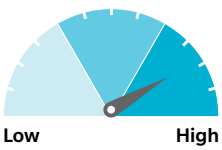
THE IMPORTANCE OF THIRD PARTY RISK MANAGEMENT (TPRM) TO YOUR INSTITUTION

Sustained cost pressures have led FIs to shift core and non-core business activities and/or solution development to third parties and external vendors – increasing the complexity of already intricate supply chains. Additionally, many FIs use third parties for competitive reasons: to acquire innovative solutions, to outsource commoditized services, to obtain expertise not available in-house, etc. Whether for efficiency, effectiveness or competitive reasons, FIs must carefully evaluate the trade-offs between these goals and the management and oversight requirements of each relationship.

With the benefits of outsourcing to third parties and the use of external vendors for various services and technology, come significant and often unidentified risks – operational, regulatory, business and reputational. This is especially true when these vendors are smaller than the FI (e.g. FinTech firms) and/or located overseas where it is more difficult to monitor the activities and quality control processes of the third parties. A subset of FIs is beginning to view strong TPRM as a strategic capability that can materially diminish the likelihood of operational risk exposures/losses due to damaging third party related events. Additionally, for larger more complex FIs, that need to set aside capital to account for operational risks, TPRM may also provide opportunities for capital relief.

Basel II defines seven Operational Risk event types that FIs need to manage and mitigate, spanning a broad spectrum of risks and having a substantial impact on the FI's business operations. Exhibit 1 provides an illustrative list of Operational Risks in each category.

Exhibit 1: Illustration of types of risks identified for each Basel II event category

OPERATIONAL RISK CATEGORIES	TOP RISK (NOT EXHAUSTIVE)	PRIORITY LEVEL	RATIONALE
1 **Internal Fraud**	• Tax evasion and bribery • Misappropriation of assets, mismarking positions • Internal theft of data		Less relevant for third party risk management
2 **External Fraud**	• Cyber security risks and hacking damage • External theft of data, fraud, forgery and robbery		Cyber risk and system security included
3 **Employment Practices and Workplace Safety**	• Discrimination in recruiting and hiring • Compensation and benefits and termination • Employment diversity & discrimination		Captured as part of Corporate Social Responsibility (CSR)
4 **Clients, Products and Business Practices**	• Unlicensed activity, market manipulation, antitrust • Money laundering and terrorist financing • Product defects • Breach of privacy • Conduct risk • Misuse of confidential information • Conflict of interest		Conflict of interest and conduct are key risks which is currently underdeveloped
5 **Damage to Physical Assets**	• Willful damage & terrorism • Natural disasters • Accidents & public safety		Impacts Business Continuity Planning and Disaster Recovery (BCP/DR)
6 **Business Disruption and Systems Failures**	• Hardware failures • Utility disruptions • Software failures		Impacts Business Continuity Planning and Disaster Recovery (BCP/DR)
7 **Execution, Delivery and Process Management**	• Incorrect maintenance of customer records • Data entry errors, accounting errors • Failed mandatory reporting • Unapproved access given to customer accounts • Negligent loss or damage of client assets • Contract risk		Client data, documentation and protection as well as business disruption are key risks

Furthermore, regulators are concerned that the quality of risk management of third party relationships may not be keeping pace with the level of risk, given the number, complexity, concentration and depth of these relationships – not to mention the rapid emergence and sophistication of new risks such as Cyber and Information risk. The OCC, FRB, FFIEC, FDIC, CFBP, FINRA, and Basel Committee have all stepped up their focus on TPRM – requiring FIs to have a sophisticated understanding of regulatory requirements across these multiple agencies. Exhibit 2 lists examples of supervisory expectations.

Exhibit 2: Overview of key US regulatory guidance on TPRM

> *A bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships.*
>
> *– OCC, 2013*

> *A bank can outsource a task, but it cannot outsource the responsibility.*
>
> *– FDIC, 2011*

> *...bank management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking. A bank's failure to have an effective third-party risk management process that is commensurate with the level of risk, complexity of third-party relationships, and organizational structure of the bank may be an unsafe and unsound banking practice...*
>
> *– OCC, 2013*

> *A bank's use of third-parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws.*
>
> *– OCC, 2013*

> *The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations.*
>
> *– FRB, 2013*

The expectation is that FIs practice effective operational risk management regardless of whether the bank performs the activity internally or through a third party. In essence, per the FDIC, the FI **"can outsource a task, but it cannot outsource the responsibility for the task"** to a third-party vendor – making all vendors part of the **"extended enterprise"** of the FI. Supervisors have increased their scrutiny of business practices by third and fourth parties

(vendors to an FI's third party) to address concerns associated with consumer protection and the safety and soundness of the industry.

Beyond the operational and regulatory risks posed by third party relationships, there are also real business and reputational risks. These risks can be due to fines, operational remediation efforts, customer settlements (brought on as a result of inappropriate actions of third parties), and financial support to critical third parties in the event of economic stress. FIs have paid out significant fines for mismanagement of third parties. Furthermore, the economic impact is not just limited to fines, as problems can result in higher operational risk capital charges and longer-term remediation efforts.

In December 2015, the Basel Committee on Banking Supervision issued a consultative document for identifying, assessing and addressing "Step-in Risk", arising from a bank's relationships with shadow banking entities. "Step-in risk refers to the risk that a bank will provide financial support to an entity beyond, or in the absence of, its contractual obligations should the entity experience financial stress."

This has implications on a bank's TPRM practices, as it may require the bank to demonstrate that it can provide financial support to an entity without degrading its own capital position.

KEY QUESTIONS TO EVALUATE YOUR TPRM MATURITY

There is no silver bullet or "one size fits all" approach to TPRM – requirements for governance, organization, management and reporting will depend on the size of the FI, its risk appetite, existing vendor management practices, the nature and extent of third party relationships, and current operational capabilities. However, TPRM does require a disciplined, integrated and holistic framework and approach to ensure that the same risk management expectations that the FI enforces upon itself are mirrored by its third parties.

CROs, COOs, CIOs, CISOs, CPOs, and CCOs need to ask hard questions about their understanding and ability to assess the current TPRM maturity level and identify specific areas that may require further investigation and refinement. Unless you are fully knowledgeable and confident with answers to the questions below, we recommend a review of your TPRM framework and practices.

Exhibit 3: Key questions to assess TPRM maturity

1	Is there an operating model and sourcing strategy in place, which is based on an evaluation of business needs (e.g. cost savings, competitive/innovative) **and** risk management imperatives?
2	Do you have transparency into the landscape of third and fourth parties used across the institution as well as associated risks the organization is exposed to?
3	Have you recently reviewed processes/activities for criticality and examined whether the risks associated with those activities are commensurate with the mitigation strategies in place? Does the use of third parties for these activities present an acceptable risk-reward trade-off?
4	Does your enterprise risk management framework account for all third party risks? Do you measure TPRM as a key component of your firm's operational risk thresholds and risk appetite?
5	Does your enterprise risk management framework specify the rigor required for contracting, monitoring and business continuity planning, depending on criticality of the third party's risks?
6	Have you established a clear governance structure with sufficient Board engagement, and comprehensive and timely TPRM reports and metrics?
7	Is there clarity of ownership and a 3 lines of defense model for TPRM? How are Lines of Business, Risk, IT, Information Security, Procurement, Compliance, Legal and Regulatory Affairs coordinating on this front?
8	Are practices and procedures for TPRM explicitly documented and followed? Is TPRM information easily accessible via a central repository and reporting tools?
9	Do you have visibility into all third parties with whom client data is shared? Are you confident in their ability to secure the data and in their business continuity plans and Cyber/Information Security?
10	For third parties dealing directly with clients, are you able to affirm that their conduct and controls mirror yours and are sufficiently rigorous?

TPRM CHALLENGES FACED BY FINANCIAL INSTITUTIONS TODAY

FIs have started improving their governance and management processes for TPRM, yet requirements are incredibly complex and evolving. Institutions have been slow to make progress given the sheer magnitude of the task at hand. With multiple thousands of third party relationships (not to mention fourth parties), many FIs are uncertain about where and how to address a task of this size (and cost).

We have identified key TPRM issues FIs need to tackle in order to realize strategic business benefits (e.g. efficiency) and satisfy regulators, the Board and Executive Management, not to mention clients, to whom third party relationships should be invisible, but who often feel the impact when things go wrong.

1. **Disconnect between Enterprise Risk Management and TPRM:** Third parties can have a significant impact on the operational, regulatory, business and reputational risk profile of an FI and need to be considered and incorporated within the FI's broader ERM framework. Since TPRM is often managed individually by each business unit (BU), the business/contract owners may undervalue risk requirements and exposures in favor of business/competitive priorities. A BU may "accept" a vendor's risk profile based purely on its siloed relationship with the vendor (without a view on vendor concentration risk or

the total exposure the bank may have to that vendor). In such situations the bank's TPRM practices are typically misaligned with and often disconnected from the firm's enterprise risk management framework and Risk Appetite statement. Additionally, regulators require that senior management and the Board have transparency into the risks posed by material third party relationships. Thus, a siloed and disconnected TPRM approach hinders objective and timely measurement of third party risk.

2. **Narrow scope of TPRM:** TPRM is often focused only on business continuity or information security at the point of contracting. However, regulators view TPRM as a broad set of operational risks (e.g. execution and delivery failure, gaps in business practices and processes, breaches in consumer financial protection practices and ethical behavior, external theft and fraud, technology infrastructure issues, financial continuity, etc.) and across the end-to-end vendor life-cycle (i.e. category planning and management of services/products purchased, vendor due diligence, third party risk assessment, selection, contracting, monitoring and termination, disaster recovery).

   To be effective, the TPRM process should ideally start even before any vendor/provider is being considered or assessed. In fact, the criticality or risks presented by a process/activity/product should be understood in order to determine if the institution is even willing to consider using a third party. The Risk Appetite statement of the institution should include guidelines for assessing this type of intrinsic risk.

   This expanded scope of TPRM requires heightened engagement and monitoring of third party risks by the FIs Board and senior management, particularly when evaluating critical activities. The OCC provides guidance by stating that **"A bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws."**

3. **Lack of a risk-based approach to vendor management:** Regulatory guidance is based on the premise that an FI's TPRM practices should be commensurate with the level of risk and complexity of the vendor relationship/activity. In other words, more rigorous oversight and management of third-party relationships is needed for critical activities, significant bank functions/shared services, or other activities that could cause a bank to face significant risk if the third party fails to meet expectations. FIs with less mature TPRM capabilities typically apply the same baseline level of governance, processes, controls and resources to all third party activities, regardless of materiality and risks. The implications of such an undifferentiated and non-prioritized approach to TPRM are immense as they relate to governance and management focus.

4. **Fast evolving and emerging ecosystem of vendor related risks:** The scope of TPRM is not purely limited to third parties. As criticality and complexity of vendor relationships increases, regulators are keen to ensure that FIs understand and mitigate risks posed by fourth and fifth parties (i.e. vendors providing services and products to their vendors). A weak link in the chain, such as a customer data leak by a fourth party, could have major implications on the bank's risk and business profile.

   FIs are themselves grappling with and starting to address rapidly emerging and evolving risks with their third parties such as Cyber risk, conduct and risk culture (i.e. alignment of vendor employees' ethics/principles/incentives to those of the FI), exposure to patent disputes, etc. Ensuring that third (and fourth/fifth) party vendors adhere to the firm's standards and requirements is proving to be a major challenge and in many instances is eliminating potential partners from consideration. The issue is particularly acute when FIs are dealing with start-ups or FinTech firms that provide innovative products/services but do not have the infrastructure to meet the FI's TPRM requirements. The industry is

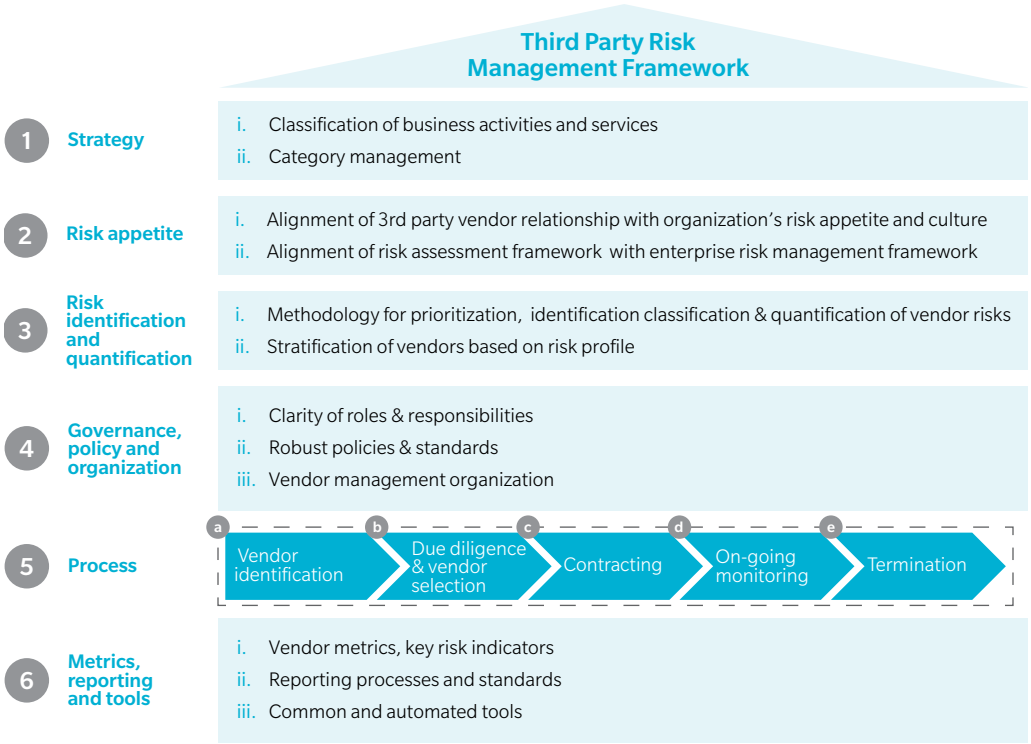
challenged by competing demands between enforcing rigorous TPRM practices while pushing the envelope on innovation.

5. **Fragmented TPRM operating model:** Historically, Non-Financial Risks (NFR), including Operational and Third Party Risks, have been managed in silos across several functions. As a result, the TPRM operating model - vendor management practices, governance, organization, processes, controls and infrastructure - varies significantly from one business unit and function to another. This variability prevents effective and timely identification, measurement, mitigation and escalation of third party risks. Institutions with a decentralized/federated vendor management model (BUs and functional groups are accountable for overall vendor relationships and empowered to make decisions on third party management) face an uphill task of establishing and consistently executing TPRM governance, standards and policies across the firm. The federated model is most common at medium and large FIs and its effectiveness necessitates robust governance and reporting mechanism with well-defined and often prescriptive standards and policies, for BUs/functions to adhere to.

BEST PRACTICES IN TPRM AND MANAGING THE EXTENDED ENTERPRISE

A best practice TPRM framework comprises six dimensions that encompass the end-to-end third party management process from strategy, risk appetite, category planning and management, due diligence and vendor selection, contracting, and on-going monitoring to termination of the third party relationship as needed.

Exhibit 4: Oliver Wyman TPRM framework



Below are the steps required to ensure effective TPRM that aligns business needs with risk management requirements.

1. **Establish a robust risk-based vendor management strategy**

   FIs should strategically evaluate the materiality and criticality of the **business activity** and determine suitability of a third party arrangement for that activity. This entails a review of the business benefits needed to outweigh the estimated oversight/control costs, and the potential operational risk exposures the FI needs to manage. A comprehensive perspective on the impact of outsourcing on the firm's customers and employees should also be performed (e.g. privacy, information security, service/quality levels, BSA/AML).

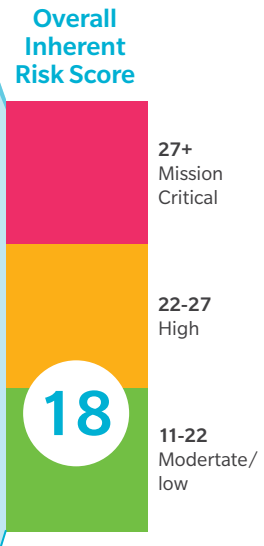
2. **Ensure comprehensive understanding of third party related risks, and alignment with institution's ERM framework**

   The decisions made on third party relationships should ensure alignment with the firm's risk appetite and transparency into resulting risk exposures. Subsequent steps in the process include evaluating trade-offs for business decisions, identifying risks related to third party engagement and documenting the analysis. The nature of specific risks for each business activity should inform the control frameworks needed across the TPRM process.

   More sophisticated institutions, with mature procurement capabilities, are developing comprehensive strategies, by adopting a fully integrated approach where TPRM is considered a key component of the category management strategy and is closely linked to the firm's ERM framework and Risk Appetite statement.

Exhibit 5: Illustrative example of inherent risk quantification
Based on Oliver Wyman client and industry examples

RISK DIMENSIONS	SCORE (1-5)	WEIGHTING	TOTAL
Business activity criticality/materiality of business activity • Based on FI dependency on service, as well as overall materiality of service to FI operations and strategy • Financial impact • Minimum thresholds also defined by spend • Includes Business Continuity Risk	1	4	4
Information security • Based on whether the services requires access to sensitive information, and on volume of data – Confidential information (could harm clients or FI if lost) – Proprietary information (cause minimal loss to clients or FI if lost) – Public information (freely available information)	2	4	8
Other risks • Based on severity of other risks associated with the service, including likelihood: – Financial – Reputational – Regulatory – Legal (also likely to be in residual risk category) – Geographic (also likely to be in residual risk category)	2	3	6



3. Establish mechanism for prioritizing and quantifying third party risk

Many institutions manage and prioritize third parties based on spend, not based on the risk exposure to the firm. We recommend that FIs establish a consistent methodology for identifying and quantifying third party risks across the spectrum of inherent risk types – risks that are inherent to the business activity. Additionally, risks that are related to third parties (over and above inherent risks) are categorized as residual risks, requiring risk-appropriate mitigation plans. As TPRM practices mature, they will enforce a new level of discipline and quantification that did not exist in the past. FIs with mature enterprise risk management standards are beginning to incorporate TPRM metrics and KPIs in their operational risk dashboards and Risk Appetite statements – often as an extension of their own metrics since the underlying operational risks (processes, data, fraud, cyber) are the same whether they exist internally or through a third-party.

4. Align TPRM to three lines of defense organization and governance structure, based on size and complexity of firm

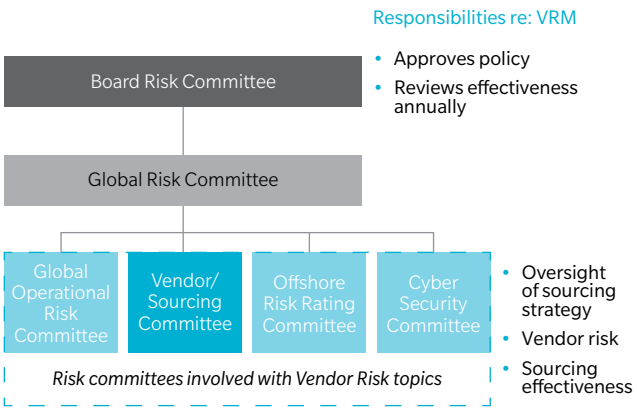
As described earlier, FIs have varying governance and organizational models for TPRM – centralized, federated and decentralized models. The latter two models in particular require stringent, consistent and comprehensive TPRM policies, standards and procedures that individual BUs and functions should adhere to. For firms that span a complex set of services/client segments and require BU-specific context, the federated model provides a balance between central control and business flexibility. Regardless of the governance and organization model, clearly defined roles and responsibilities between the 1st and 2nd lines of defense are key to successfully executing vendor management policies and procedures.

Exhibit 6: Illustrative TPRM governance models

MODEL 1: LARGE GLOBAL BANK – US HOLDING CO.
VENDOR RISK INCORPORATED INTO OPERATIONAL RISK GOVERNANCE
(DISGUISED CLIENT EXAMPLE)

- Vendor risk incorporated into the Operational Risk Committee
- Escalation of vendor risks and approvals follow the standard Operational Risk escalation paths

MODEL 2: LARGE NORTH AMERICAN UNIVERSAL BANK
DEDICATED VENDOR RISK AND SOURCING GOVERNANCE COMMITTEES
(DISGUISED CLIENT EXAMPLE)



- Governing sourcing strategy and vendor risk management through a dedicated committee with responsibility for
  - Strategic direction for sourcing and alignment with FI strategy
  - Risk management for sourcing and vendors
- Observed executive roles in an Enterprise Sourcing Committee
  - Head of Tech and Ops (CIO)
  - Head of Corporate/Shared Services

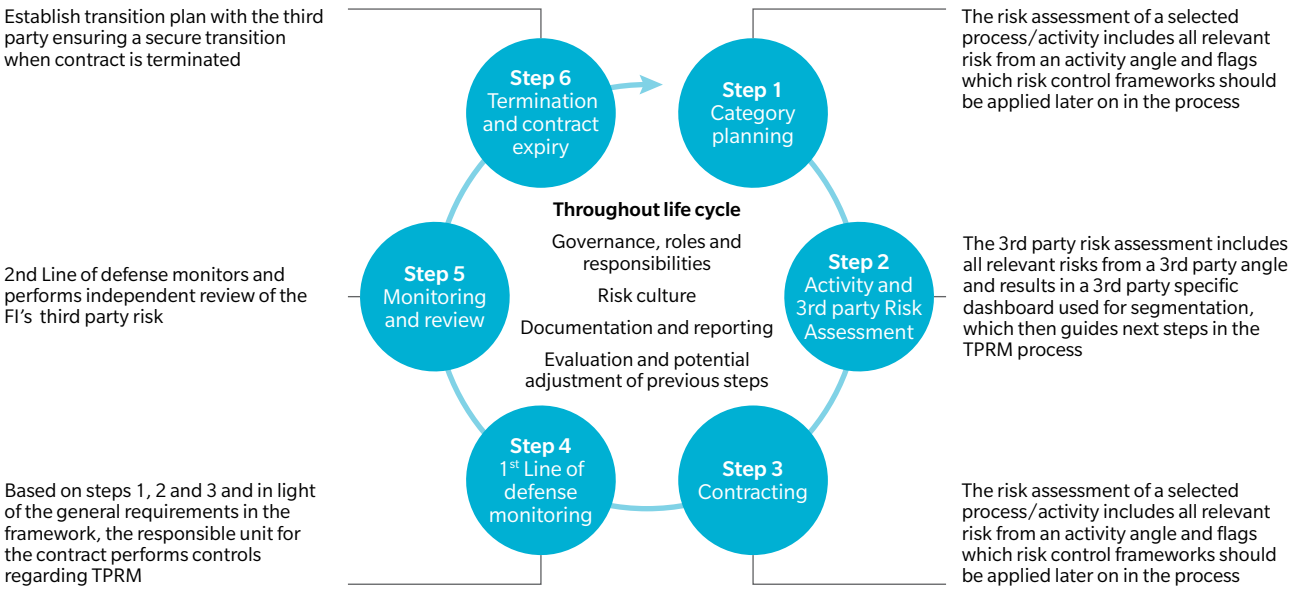
It is important to define who and where the 1st and 2nd line demarcations sit. For instance, there may not be agreement on whether the Procurement function is a first or second line function – or perhaps Line 1.5. In addition, as Cyber and Information Security become increasingly important, it may not be clear where ownership should reside: with Risk, IT, Procurement or the Business? Given the technical complexity of Cyber/Information Risk, it is often placed in IT. However it raises the concern that if IT is first line of defense for its own systems, infrastructure, Cyber and data programs, can it provide 2nd line enforcement for third parties? While there is no perfect, right or wrong answer to the organizational and governance issues involved in TPRM, it is important that senior management and the Board discuss, agree and clearly articulate (for internal and regulatory purposes) the expected governance structure, roles and responsibilities.

Depending on the firm's TPRM capabilities, FIs may start out by leveraging existing risk management committees and forums. As the firm's complexity grows and/or TPRM matures, FIs may need to establish specific committees for operational risk management and, within that, TPRM.

5. Drive consistent TPRM processes, depending on the criticality of the business activity

Regulators expect due diligence practices to be commensurate with the level of risk and complexity of the third party relationship, requiring senior management and Board engagement for critical activities. A typical due diligence effort for key third parties could comprise more than a dozen different evaluation components - such as legal and regulatory compliance, financial condition, information security, business experience and reputation, resilience etc. This phase also requires FIs to possess increased awareness of controls for vendor sub-contracting or 4th party risk.

Exhibit 7: Illustrative vendor management lifecycle

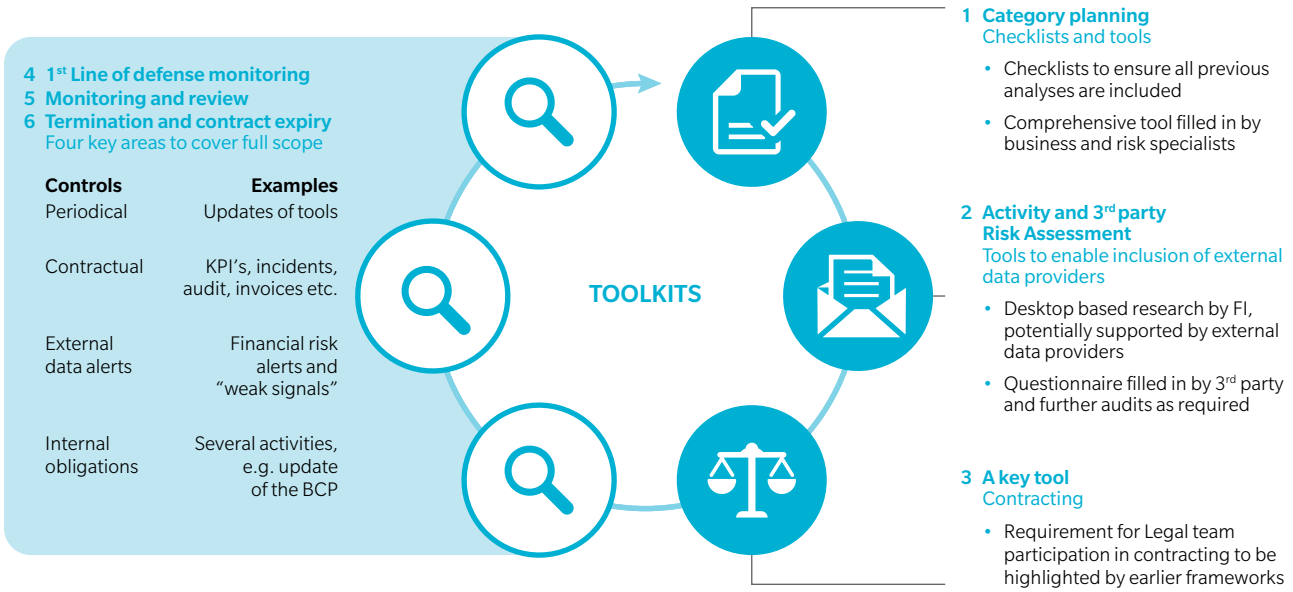


Once the institution selects a third party, management should negotiate a contract that clearly specifies the rights and responsibilities of each party. This specifically entails modifying "boilerplate" contracts for specificity and embedding measurable service level agreements (SLAs) for on-going performance monitoring. This first stage should be followed by review and approval of the contract by senior management and the Board for critical activities.

While most institutions have relatively good discipline and process for managing vendor selection and contracting, processes for on-going monitoring are often much more inconsistent and ad hoc. It is important to implement monitoring standards (such as frequency, requirements, and responsibility) across the institution and leverage a central system to track and report on the process. For particularly crucial vendors and/or activities, the FI may wish to permanently station an employee at the third party location to provide daily oversight.

An institution may terminate third-party relationships for various reasons (e.g. expiration/breach of contract, desire for an alternate third party, in-sourcing of activity, etc.). Regardless of the reason, the FI needs to ensure that the relationship is terminated in an efficient manner such that activities are transitioned to another third party, discontinued or insourced with minimal disruption to the bank's business activities and customers. For critical activities, the institution should have back-up procedures that can be called upon in an almost instantaneous fashion in the event of unplanned or sudden termination of the services.

Exhibit 8: Illustrative framework of tools to support TPRM



6. Implement appropriate tools/capabilities for TPRM monitoring and reporting

This dimension of the life-cycle is the most critical from a business-as-usual perspective, spanning on-going due-diligence, on-going performance monitoring and appropriate resourcing and governance for TPRM. FIs should pay close attention to the quality and sustainability of the third party's controls, its ability to meet SLAs, performance metrics and other contractual terms, and to comply with legal and regulatory requirements. Establishing timely and effective mechanisms to measure the third party's performance and service levels is a critical part of TPRM.

New advanced capabilities for monitoring of external information sources (including social media), as well as big data predictive analytics are providing greater monitoring and (near) real-time measurement of third party risks. In fact, an institution can monitor changes to a third party's management team, financial stability, competitive positioning, operations, etc. and define sensitivity parameters for alerts on events requiring further investigation. Social media can also be monitored for any customer complaints related to services or products that are provided via third parties.

CONCLUSION

For FIs, maturing their TPRM practices and capabilities is an important and worthy investment, the benefits of which are multifold. A strong set of TPRM capabilities allows FIs to effectively and proactively manage the operational risks associated with their "extended enterprise" and safeguard against events that can severely and adversely affect their customers and business. An added but essential benefit of establishing strong TPRM capabilities is that FIs are well positioned to satisfy regulatory requirements. If managed well, FIs may also realize third party cost efficiencies and performance improvements as material benefits.

Exhibit 9: Strategic benefits from mature TPRM practices

1	**Regulatory compliance:** Achieve satisfactory compliance with regulatory guidance from supervisors on TPRM practices
2	**Risk management:** • Improve visibility into the FI's operational risk, and drive robust risk identification, monitoring, mitigation and remediation • Enable risk quantification for broader set of third party risks (i.e. beyond Information Security and BCP/DR) • Enforce stringent governance so that unwarranted residual risk is not accepted or is sufficiently mitigated
3	**Value to the business:** Generate and preserve greater value from its third party relationships (i.e. negotiations, pricing, service) and sustainably support business growth
4	**Vendor performance:** Drive a step change improvement in the consistency and quality of services/ products delivered by third parties, by instituting disciplined and comprehensive third party performance measurement, including SLAs

Depending on the your point of departure, the journey to achieve best practices will vary in complexity and investment, but the questions and steps outlined in this paper should provide a blueprint to evaluate the maturity of your TPRM capabilities, and identify next steps towards improvement.

For further information on the topic, please reach out to authors of this paper.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

ABOUT THE AUTHORS

Elizabeth St-Onge, Partner
Finance & Risk and Strategic IT & Service Operations Practices
Americas
elizabeth.st-onge@oliverwyman.com

Swati Sawjiany, Partner
Finance & Risk and Strategic IT and Service Operations Practices
Americas
swati.sawjiany@oliverwyman.com

CONTRIBUTORS

Thomas Ivell, Partner
Finance & Risk Practice
EMEA
thomas.ivell@oliverwyman.com

Paul Lewis, Principal
Finance & Risk and Strategic IT and Service Operations Practices
EMEA
paul.lewis@oliverwyman.com

www.oliverwyman.com

OLIVER WYMAN