



Third-Party Risk Management in Financial Services

Defining the best-in-class third-party risk management practice

Jimit Arora, Partner
Archit Mishra, Senior Analyst
Ronak Doshi, Senior Analyst

Copyright © 2016, Everest Global, Inc. All rights reserved.



This report has been licensed for exclusive use and distribution by Everest Group, IHS Markit, NTT DATA.

Executive Summary

Third parties play a critical role in the financial services ecosystem. However as financial institutions increase dependence on them to deliver critical business processes and services, the complexity of oversight also increases. Third-party relationships are under increasing scrutiny by regulators globally, including the U.S. Office of the Comptroller of the Currency (OCC), Financial Industry Regulatory Authority (FINRA), the UK Financial Conduct Authority, the Prudential Regulation Authority, and the Monetary Authority of Singapore. Key findings of this research are:

- The lack of standardization with regards to collecting and distributing due diligence data lead to duplicate efforts, creating costly and inefficient processes
- The standardization of technology infrastructure for Third Party Risk Management (TPRM) enables enterprises to drive efficiencies in the entire TPRM value chain and automate several tasks
- Financial services firms can benefit from industry collaboration in the field of TPRM to adopt modern technologies as well as mutualize costs
- Shared utilities help firms to reduce costs, improve vendor information collection process, provide real-time visibility & continuous monitoring of risks, and equip financial services firms with data and analytics to respond to regulators' demands
- Shared utilities empower financial services firms to gain competitive advantage by reducing costs of several non-core activities such as vendor information collection and due-diligence
- Financial services firms need to overcome challenges of change management, perceived loss of control, and security of vendor information to drive adoption of shared utilities

Introduction

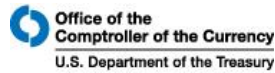
Global banking and financial services firms are focusing on a triple mandate of “run-the-bank” (focus on efficiency for cost savings), “manage-the-bank” (focus on risk and regulatory compliance for penalty avoidance), and “change-the-bank” (focus on transformation for growth) initiatives. “Manage-the-bank” initiatives are focused on ensuring regulatory compliance and managing risks. Since the financial crisis of 2008, the regulatory pressure on banks have intensified and have moved beyond the bank’s operations to include risks emanating from third parties. To stay ahead of competition and ensure compliance, avoid fines/penalties, and manage business risks, financial services firms are focusing on containing costs of compliance and adopting disruptive business models, and mutualizing costs through shared utilities. In this research we highlight the importance of efficient TPRM practices and define the best-in-class operating model of a TPRM practice.

Regulators are taking on rigorous interpretation of third-party risks. Laws and standards such as Sarbanes Oxley Act, the Gramm-Leach Bliley Act (SSAE 16), and the Foreign Corrupt Practices Act of 1977 (FCPA), as well as Payment Card Industry Data Security Standard (PCI DSS) requirements impact the way financial services firms handle their TPRM practice. Exhibit 1 on page 4 provides few additional examples of rules, regulations, and guidelines impacting TPRM.

EXHIBIT 1

Examples of rules, regulations, and guidelines impacting TPRM practice

Source: Everest Group



- **OCC BULLETIN 2013-29:** Third-party risk management guidance
- **Advisory Letter 2000-12:** Risk management of outsourcing technology services
- **Bulletin 2001-47:** Third-party relationships
- **Advisory Letter 2001-8:** Standards for safeguarding customer information
- **Bulletin 2002-16:** Bank use of foreign-based third-party service providers



- **Board Of Governors Of Federal Reserve System, SR 13-19 / CA 13-21:** Guidance on managing outsourcing risk
- **SR 004 (SUP),** Outsourcing of information and transaction processing
- **SR 0017 (SPE):** Guidance on the risk management of outsourced technology services



Federal Deposit Insurance Corporation:

- **FIL-44-2008:** Guidance for managing third-party risk
- **FIL-49-99:** Notification for compliance with the Bank Service Company Act
- **FIL-50-2001:** Bank technology bulletin on outsourcing



- **European Union (EU) Regulation 2016/679, General Data Protection Regulation (GDPR):** Ensuring compliance of third parties' accessing data
- **Payment Services Directive 2 (PSD2):** Regulates third-party payment service providers with access to payment account information



- **Rule 31-90:** Scope of a firm's obligations and supervisory responsibilities for functions or activities outsourced to a third-party service provider



- **Enhanced Cyber Risk Management Standards (2016)**
- **Thrift Bulletin 82:** Third-party arrangements



- **CFPB Bulletin 2012-03:** Obliging to Federal Consumer Financial law when working with service providers



OSFI
BSIF

- **OSFI Guideline B-10:** Federally Regulated Entities (FREs) retain ultimate accountability for all outsourced activities



- **FFIEC administrative guidelines:** Implementation of interagency programs for the supervision of technology service providers (October 2012)

Third-party: Definition

All entities that provide or perform services on an enterprise's behalf are called third parties to that enterprise. For e.g., firm X is developing a mobile app for a retail bank's customers. In this example, the bank is first party, the customer is the second party, and the software firm developing the mobile app is the third party.

Enterprises enter into third-party relationships for various reasons:

EXHIBIT 2

Examples of rules, regulations, and guidelines impacting TPRM practice

Source: Everest Group

Reduce costs

Third-party firms specializing in a task can help reduce costs for certain activities when compared to doing it in-house

Enhance capability

Partnering with third-party firms helps enterprises to tap into innovation and reduce time-to-market

Improve focus

Firms can focus their resources on core activities while delegating the non-core activities to third-party firms

Access talent

Firms can access talent and specialized skills by engaging in third-party relationships improving flexibility and agility to respond to customer and business needs

Third-party risks

Third-party vendors play a critical role in the financial services ecosystem, however there are certain risks that financial services firms need to manage when they engage with vendors. Third-party risks emanate from relying upon outside parties to perform services or activities on behalf of an enterprise. Regulators expect enterprises to be responsible for all activities, regardless of whether performed by a third-party or internal resources. Therefore, it is important for enterprises to manage risks from third-party relationships.

EXHIBIT 3

Type of risks that a financial services firm needs to manage while engaging with third parties

Source: Everest Group

Type of risks	Impact of risk
Financial	Value loss, investor loss, customer loss, and capital cost increases
Reputational	Brand value loss, unwanted press & media exposure, and decline in consumer confidence
Operational	Breakdown in internal processes and systems
Information security	Loss of data records, breach of internal systems
Strategic	Customer loss, pricing pressure, and business loss
Compliance	Regulatory impairment, regulatory fines & penalties, litigations, and increase in regulatory scrutiny
Business Continuity	Service quality issues
Economic risk	Foreign exchange impact, increase in costs, loss of revenues, and profitability issues
Country risk	Investment losses, increase in regulatory scrutiny, and fines

Third-Party Risk Management (TPRM): Definition

Third-party risk management refers to a structured approach to identify, manage and mitigate risks arising from parties other than the financial services firm or the end-consumers

A TPRM practice contains the following components:

- **People:** Team of risk professionals, auditors, and compliance experts
- **Governance and process:** Manage, oversee, and perform efficient TPRM
- **Data:** Consistency, quality, and correctness of data for all vendors. Defining the type of data to be collected for different vendors is based on their importance and risk classification
- **Tools and technology:** Enablers to remove manual effort and automate TPRM functions

EXHIBIT 4

Key components of a TPRM practice

Source: Everest Group

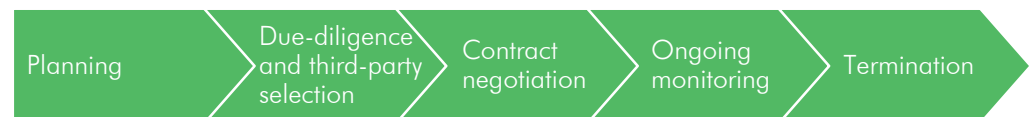
People	Governance	Process/tools	Data
<ul style="list-style-type: none"> ● Risk and audit professionals ● Training ● Change management 	<ul style="list-style-type: none"> ● Policy & procedures ● Management oversight ● Alignment with operational risk ● Program management ● Transparency ● Communication 	<ul style="list-style-type: none"> ● Risk classification ● Risk management ● Reporting, metrics, and scorecards ● Technology solutions 	<ul style="list-style-type: none"> ● Data collection ● Data cleaning ● Organizing data ● Data validation ● Data analytics

The above components have a direct impact on the success of different stages of the TPRM process value chain as shared below:

EXHIBIT 5

Value chain of activities in a TPRM practice

Source: Everest Group



Technology is a core enabler at every stage of the TPRM value chain and across the four components. Financial services firms vary in their approaches to perform the various TPRM functions based on the maturity of processes and sophistication of the underlying TPRM technology adopted. Technology is key to supporting and even completely automating workflows, analyzing & collating risk data, reporting, and managing issues. The overall maturity of the process and technology stack helps enterprises reduce costs of performing TPRM functions and also improves the overall time it takes to onboard a vendor. Current third-party risk management infrastructure varies considerably among financial institutions. While some are on the forefront of leading practice, others lag behind and need to catch-up.

Third-Party Risk Management (TPRM): More important than ever

As financial services firms expand globally, they engage with a number of third parties and it becomes increasingly important to manage these relationships effectively for the reasons presented below:

"We have more than 22,000 active relationships." - Felipe Prestamo, Senior Vice President and Head of the U.S. Compliance Services at TD Bank

- **Complexity and multiplicity of vendor relations** – Global financial services firms today have thousands of vendor relationships that are spread across the globe and are subject to different regulations and business practices in their own geography. As the firm grows, partner ecosystem will become even more diverse and complex
- **Increasing regulatory pressure** – Excessive risk taking and routine lapses have led to new set of regulations to protect consumers from adverse impacts of third-party relationships
- **Increase in fines for non-compliance** – Cost of non-compliance is on the rise. As shown in Exhibit 6, several financial services firms have been levied fines for breaches / non-compliance arising out of third-party relationships. Regulators have introduced specific regulations targeting third-party relationships
- **Advent of new technologies** – Digital disruption and demand for more personalized customer experience are influencing financial services firms to partner with new third-party vendors

EXHIBIT 6

Costs of failures of TRPM – paying for third-party missteps

Source: OCC; Washington Post; and U.S. Government Consumer Finance Protection Bureau

Company	Year	Regulator	Fine	Violation
Capital One	2012	CFPB	US\$210 million	Unfair practices such as deceptive marketing / unfair billing which were handled by third-party providers
Discover Bank	2012	CFPB	US\$14 million	
American Express	2012	OCC	US\$9.6 million	
JPMC	2013	CFPB	US\$20 million	
Citibank	2015	CFPB	US\$35 million	

Third-Party Risk Management (TPRM): A source of competitive edge

A robust TPRM program can help financial services firms gain additional benefits beyond being compliant and managing overall risk:

EXHIBIT 7

Benefits of a TPRM practice

Source: Everest Group



Improve customer experience by reducing service disruption and data breaches



Gain end-to-end view of the scope of services from outsourcing vendors



Efficient Vendor Management (VM) enables vendor rationalization initiatives



Drive down outsourcing costs through improved VM & contract negotiation



Improve risk management through continuous monitoring and focus diligence



Risk stratification helps identify high risk vendors for faster countermeasures

Third-Party Risk Management (TPRM) practice optimization model

Globally financial services firms are striving to establish effective processes and systems to manage third-party risks and regulatory compliance. However, a majority of the financial services firms have an approach that is ad hoc and fragmented. Thus, companies face several challenges to perform risk identification, segmentation, and continuous monitoring that is cost effective from the enterprise’s point of view and ensures that it is able to unearth and take preventive/corrective actions for potential risks that may result into security breaches, bribery, money laundering, regulatory violations, and so on.

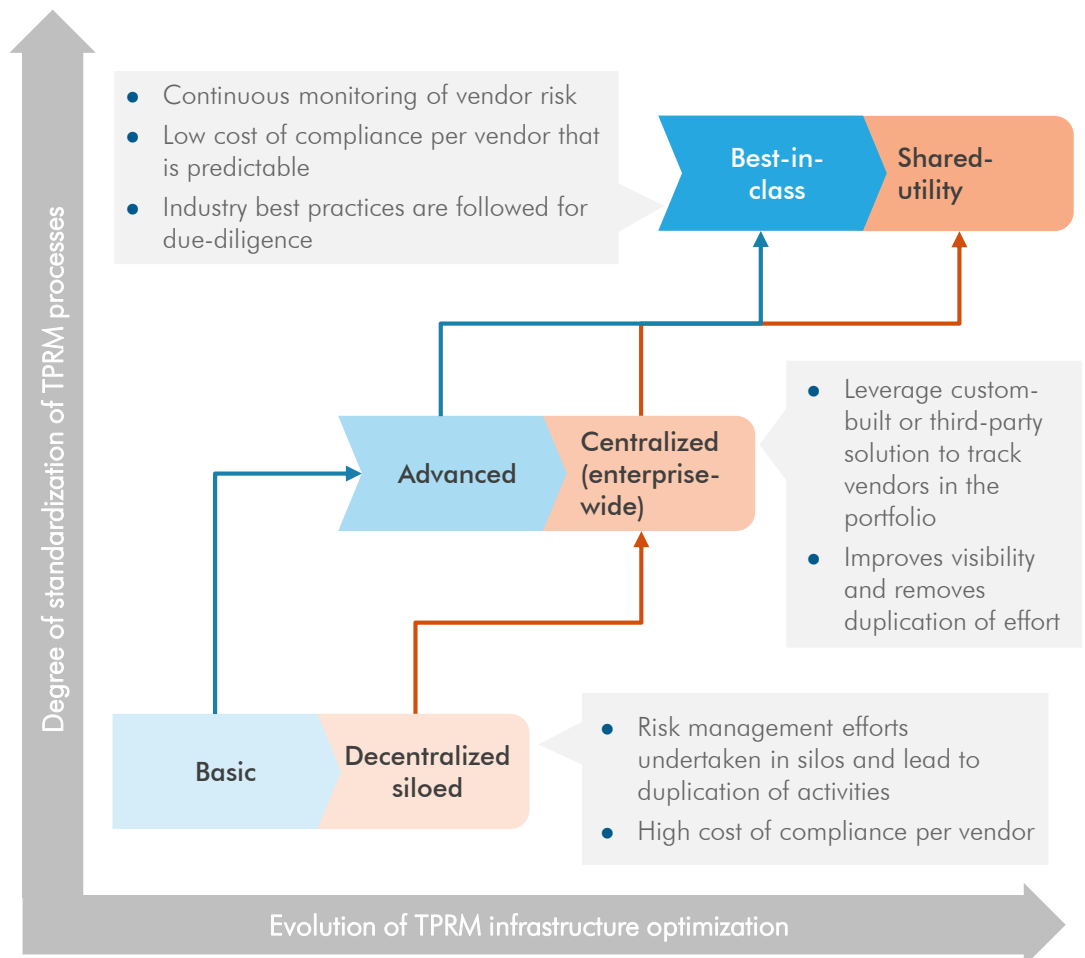
There are a few firms that started off with no TPRM program and leapfrogged the competition through “program optimization”. Based on the optimization of TPRM infrastructure as well as degree of standardization of TPRM processes, we can categorize TPRM operating model into the following three types:

- Decentralized siloed
- Centralized (enterprise-wide)
- Shared-utility

EXHIBIT 8

Maturity levels of TPRM practices

Source: Everest Group



Financial services firms need to move from a transactional and “check-the-box” compliance view of TPRM to a robust and strategic program for due-diligence and third-party governance.

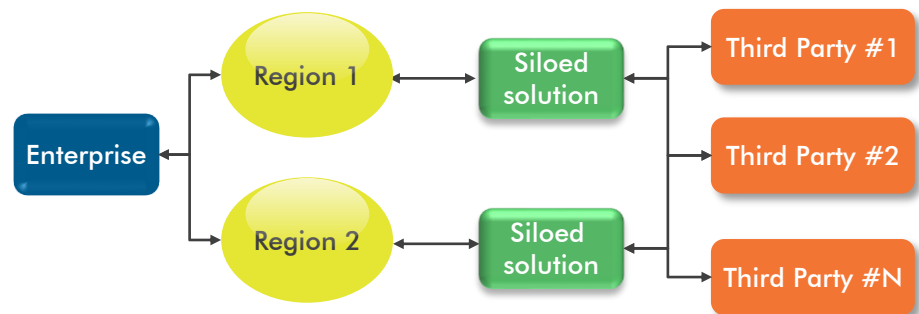
Financial services firms use a variety of TPRM program structures/models depending upon factors such as culture, scale, and geography.

1. **Decentralized siloed model:** Small- and medium-sized firms as well as large global firms with business units operating in silos adopt a decentralized model. Third-party relationships are maintained by different departments / regions / Lines-of-Business (LoBs) operating independently. Third parties submit compliance data to TPRM managers for that particular region/department/LoB, which in turn is used by the TPRM system for risk assessment and compliance/audit purposes.

EXHIBIT 9

Illustration of information flow in a typical decentralized siloed TPRM model

Source: Everest Group

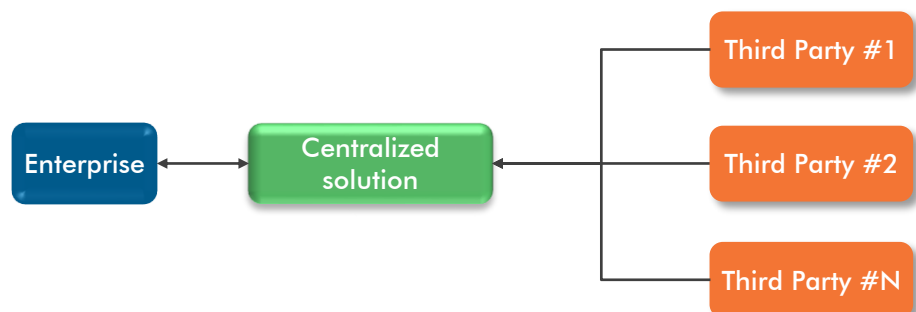


2. **Centralized model (enterprise-wide):** As firms mature their TPRM practice, they have a centralized office to oversee third-party risk management processes and ensure standardization, central reporting, and faster vendor onboarding. Typically due-diligence is done through a centralized platform (in-house or off-the-shelf solution) and ownership of collecting, analyzing, and evaluating the third-party data that lies with the enterprise

EXHIBIT 10

Illustration of information flow in a typical centralized (enterprise-wide) TPRM model

Source: Everest Group

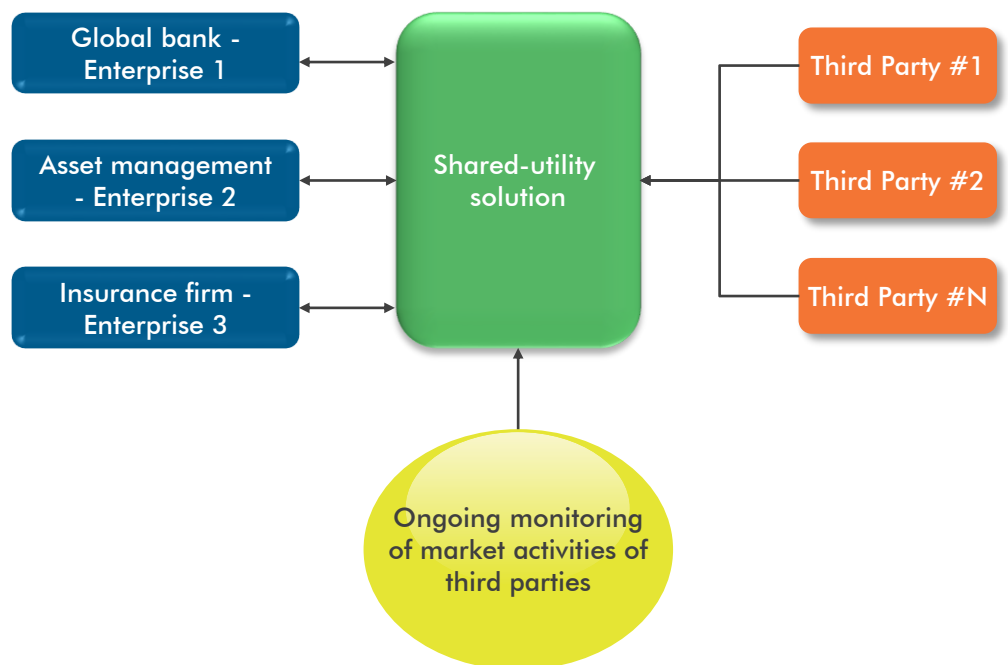


- 3. Shared-utility model:** An emerging operating model wherein firms retrieve standardized due-diligence information about third-party vendors through a central system. The shared-utility platform houses due-diligence information on third-party vendors. Standardized questionnaires allow vendors to store and reuse responses for multiple requests from different enterprises and in turn reduce duplication of efforts. The model also offers unique opportunity for enterprises to collaborate with the third-party ecosystem (peer firms and vendors) and leverage by sharing of information within the network. Enterprises gain efficiency, reduce their costs of compliance, and get real-time visibility on the third-party vendors. As shown in Exhibit 11 below, this illustration represents the optimized model for reducing risk and increasing efficiency

EXHIBIT 11

Illustration of information flow in a typical shared-utility TPRM model

Source: Everest Group



Characteristics of optimal state of TPRM practice

Exhibit 12 defines characteristics of an optimal TPRM practice. Different maturity levels are compared across a number of dimensions to describe this “optimal state” of TPRM practice.

EXHIBIT 12

Characteristics of optimal state of TPRM practice of financial services enterprises

Source: Everest Group

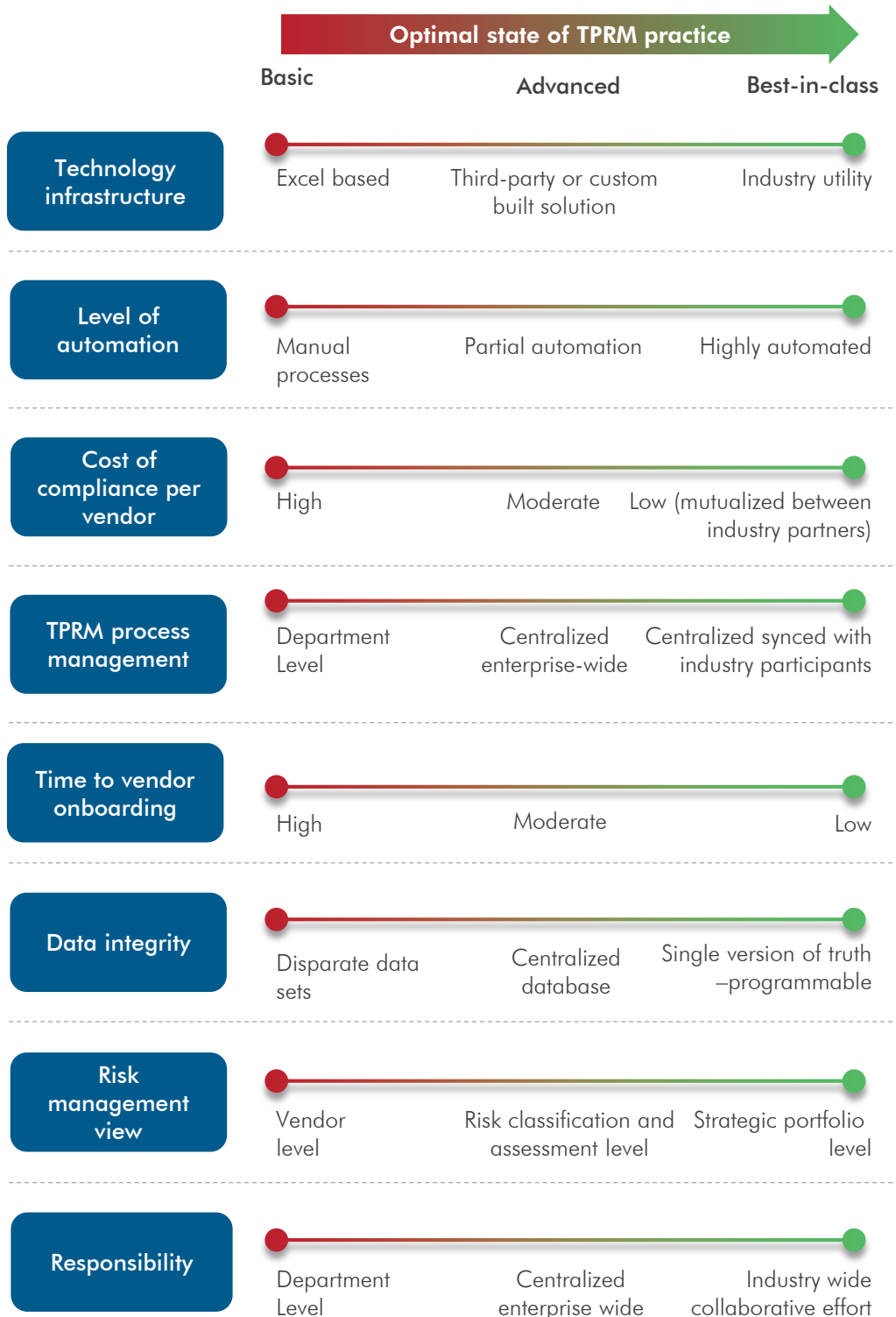


Exhibit 13 and 14 provides a detailed comparison of the different maturity levels of enterprises' TPRM operating models across a number of dimensions.

EXHIBIT 13

Comparison of different operating models for TPRM

Source: Everest Group

Focus area	Decentralized siloed	Centralized (enterprise-wide)	Shared-utility
Governance structure	<ul style="list-style-type: none"> Multiple risk managers focused on specific department/region/LoB Limited or no dedicated governance over critical third parties 	<ul style="list-style-type: none"> Centralized office monitors and oversees risk processes across the enterprise Dedicated risk managers assigned for significant relationships 	<ul style="list-style-type: none"> Smaller governance teams as infrastructure and due-diligence handled by shared-utility platform provider
Vendor discovery	<ul style="list-style-type: none"> Redundancy in vendor enrollment 	<ul style="list-style-type: none"> All departments share information however enrollment is conducted on need basis 	<ul style="list-style-type: none"> Handles comprehensive list of third-party vendors and constantly amends and updates the inventory list
Due diligence	<ul style="list-style-type: none"> Assessments lack depth and may cover financial and security analysis Background data is maintained by spreadsheets owned by each department/region/LoB 	<ul style="list-style-type: none"> Assessments cover financial, reputational, Business Continuity Planning (BCP) or Disaster Recovery (DR), and security analysis Background data is documented and maintained in a centralized database Continuous monitoring of high-risk vendors 	<ul style="list-style-type: none"> Assessments include country, financial, reputational, BCP or DR, information security, privacy, technology, legacy, and compliance analysis Background data retrieved from shared-utility platform & independent third-party data sources Near real-time monitoring

EXHIBIT 14

Comparison of different operating models for TPRM (continued)

Source: Everest Group

Focus area	Decentralized siloed	Centralized (enterprise-wide)	Shared-utility
Audit and compliance	<ul style="list-style-type: none"> • Audit and compliance process requires more time and effort to consolidate data from various spreadsheets 	<ul style="list-style-type: none"> • Information is easily retrievable from centralized system • Data is static and continuous updates require extensive data collection exercise 	<ul style="list-style-type: none"> • Data available through shared-utility platform on a as-a-service mode • Requires less effort and time for audit and compliance as data is available in standardized format
Technology maturity	<ul style="list-style-type: none"> • Manual spreadsheet-based technology for each TPRM system • Technology infrastructure maintained by each region or department 	<ul style="list-style-type: none"> • Custom-built or third-party solution • Technology infrastructure maintained in-house by the enterprises 	<ul style="list-style-type: none"> • Technology infrastructure owned by the shared-utility platform provider • Enterprises can retrieve information on “as-a-service” mode
Vendor interface	<ul style="list-style-type: none"> • Multiple touchpoints resulting in duplication since one vendor may have to submit same information to multiple offices or departments 	<ul style="list-style-type: none"> • Centralized interface for vendors, however, requires significant effort and time for vendors to respond to questionnaire from each enterprise 	<ul style="list-style-type: none"> • Single touchpoint for vendors across enterprises & eliminates need for vendors to respond to similar questionnaire from multiple enterprise

Shared-Utility model for third party risk management

As defined in the previous sections, shared-utility platforms enable financial services firms to adopt best-in-class risk management practices. Common shared-utility solutions can help firms cut operational costs and standardize their third-party risk management process. It eliminates complexities arising out of multiple, fragmented, and redundant processes for TPRM.

Benefits of adopting a shared-utility model for third party risk management

There are several shared-utility platform providers in the market for areas such as third party risk management, Know Your Customer (KYC), data reconciliation, and collateral management. We studied a number of third party risk management platforms to list benefits of adopting a shared-utility platform by financial services firms:

- 1. Efficiency gains:** Vendors would not have to answer similar questions from different enterprises. This reduces onboarding time for vendors who have already filled their due-diligence responses on the platform. Enterprises can leverage automation to bring in efficiency gains for repetitive tasks
- 2. Standardization:** As more financial services firms adopt a shared-utility platform, universal standards will evolve. The platform will align to upcoming regulations (global as well as country-specific) and standards such as NIST, ISO, SOX, PCI, etc., which will make it easy for firms to prepare for audits and compliance requirements
- 3. Cost per vendor:** The shared-utility platform reduces cost of compliance through a more efficient third-party oversight process. The “as-a-service” pricing eliminates capital expenditure on the infrastructure, reduces time and effort, and need for larger governance teams, thereby bringing down the operational cost per vendor
- 4. Real-time visibility and continuous monitoring:** The shared-utility platform for third party risk management provides real-time visibility and transparency, since the shared-utility platform provider retrieves third-party information from multiple market sources on a real-time basis and combines it with vendor data to evaluate risks associated with the vendor. The platform also provides opportunity for vendors to join the network to gain visibility and connect with leading financial services firms looking to partner with third-party vendors
- 5. Vendor discovery:** The shared-utility solution is a centralized data hub that provides access to standardized and aggregated third-party information to enterprises. This provides an opportunity for enterprises to discover and connect with relevant third-party vendors through a shared-utility platform

6. **Quicker vendor onboarding:** Enterprises can collaborate with third parties quickly and more effectively
7. **Configurability:** Ability to configure level of risk assessment questionnaire
8. **Ease of access:** Since the solution is hosted on secure cloud infrastructure, financial services firms can easily access vendor information from multiple devices – anywhere, anytime, providing superior user experience
9. **Scalability:** The shared-utility solution provides ability for enterprises to integrate acquisitions and manage divestments swiftly as well as in a cost efficient manner through rapid deployment
10. **Reduction in number of vendor touchpoints:** Since the solution eliminates need for financial services firms to interact with vendors to collect risk-and compliance-related information, which is now done by the shared-utility solution provider, it potentially reduces the number of touchpoints with third-party vendors

Challenges for adopting a shared-utility platform

Despite a number of benefits posed by a shared-utility solution for third-party risk management, there are few challenges as mentioned below:

1. **Perceived control issues for the enterprises:** Financial services firms may perceive the loss of ownership and control on third-party vendor information as a critical factor that may influence their decision to leverage a shared-utility platform
2. **Concerns around information security:** Growing concerns on cybersecurity and recent incidents related to loss of confidential vendor information may impose a significant challenge to the adoption of shared-utility model
3. **Reduced face-time with third-party vendors:** Vendor relationship managers and TPRM executives will have fewer interactions with the third-party vendors, which may be perceived as a risk in establishing a rapport in critical/significant relationships
4. **Resistance to change:** Moving to a shared-utility solution requires changes in the current governance model as well as in existing processes, activities, and reporting structure. The management may perceive the process to cause a lot of change fatigue, which may lead to resistance from business units

Several solutions in the market are circumventing some of these challenges by leveraging technology, partnerships, and increased participation of their financial services clients in the governance of shared-utility

Conclusion

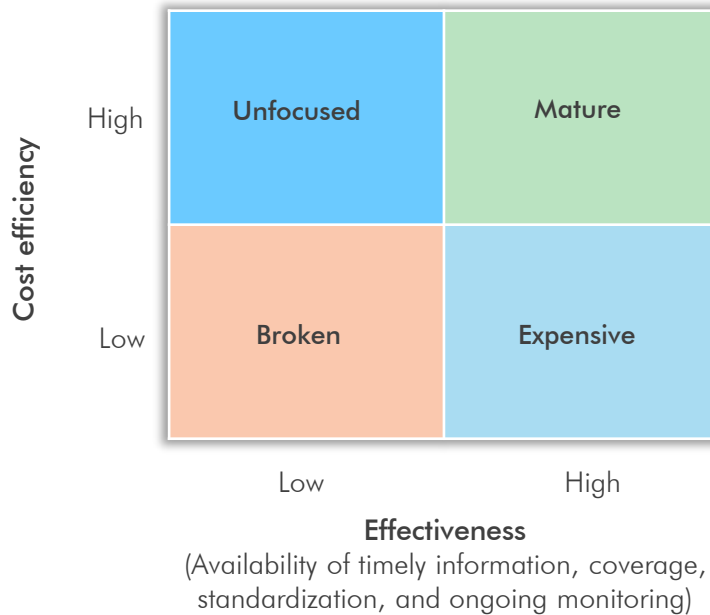
All financial services firms, regardless of size need to manage the growing complexities and scrutiny around third-party relationships. Each outsourced relationship comes with a unique set of risks, which enterprises need to proactively monitor and mitigate.

An ineffective and inefficient third party risk management system can lead to high penalties and loss of business and market reputation. Enterprises need to reflect on their effectiveness and efficiency of third-party risk management systems and accordingly take steps to move to an optimal system. The exhibit below offers a guidance for financial services firms to measure effectiveness and efficiency of its third party risk management systems.

EXHIBIT 15

Framework to measure effectiveness and efficiency of TPRM systems

Source: Everest Group



Factors such as high costs, non-standardized processes, duplication of tasks & efforts, delay in vendor onboarding, and lack of agility in existing third party risk management operating model influence the need for a shared-utility solution. Financial services firms can achieve an effective and cost efficient third-party risk management system through a shared-utility-based third-party risk management system.

Moving to an optimal TPRM system

Financial services firms should evaluate their need to move to a shared-utility solution to realize full potential of the values that a common centralized solution can bring in a third-party oversight process.

Exhibit 16 illustrates the key steps involved in implementing a shared-utility solution for TPRM:

EXHIBIT 16

Suggested steps to adopt a best-in-class third party risk management solution

Source: Everest Group




1. **Build a case for business acceptance:** First step requires building a business case for stakeholders' approval. Identify the key metrics and evaluate the total cost of ownership against the direct and indirect benefits to compare current system with the ideal mature system. Clearly bring out the inefficiencies in the current system and the loss that the financial services firm may bear in case of failure to timely assess risks related to third-party
2. **Select a third party risk management platform provider:** Enterprises need to identify and evaluate TPRM platform providers that meet their business needs. The choice of platform depends on multiple factors, of which a few are listed below:
 - Number of vendors associated with the shared-utility platform
 - Number of enterprises collaborating with the platform provider
 - Functionalities offered by the shared-utility platform
 - Ease of integration with the existing systems
 - Pricing and fees

Enterprises may also choose an outsourcing partner to help deliver end-to-end services including hosting, integrating with existing systems, and enhancing & building value-add functionalities on top of the TPRM platform.
3. **Migrate the existing third party risk management systems:** Moving to a shared-utility platform for third-party risk assessment requires sun setting the current systems and sourcing third-party information from the new platform. However, financial services firms should plan for a smooth transition and go for a phased approach:
 - Enterprises should first assess criticality of the third parties based on parameters such as strength of relationship and risk impact and start leveraging shared-utility platform to source risk, compliance, and audit related information for the less critical third parties
 - Once the stakeholders are confident of the information accuracy, completeness, and authenticity, enterprises can move to the new platform for the rest of the third parties and integrate the upstream systems with the new platform.
4. **Governance model and change management:** Financial services firms should build/redesign and implement a new TPRM office, including governance structure, reporting framework, policies, procedures, processes, and controls. At the same time, firms should plan for training and change management programs to educate the team.
5. **Enhance value derived from the shared-utility platform:** Financial services firms can build a decisioning system based on third-party risk-related information extracted from the shared-utility platform to ensure strong and robust oversight process.

About Everest Group


Everest Group is a consulting and research firm focused on strategic IT, business services, and sourcing. We are trusted advisors to senior executives of leading enterprises, providers, and investors. Our firm helps clients improve operational and financial performance through a hands-on process that supports them in making well-informed decisions that deliver high-impact results and achieve sustained value. Our insight and guidance empowers clients to improve organizational efficiency, effectiveness, agility, and responsiveness. What sets Everest Group apart is the integration of deep sourcing knowledge, problem-solving skills and original research. Details and in-depth content are available at www.everestgrp.com.

For more information about Everest Group, please contact:


 +1-214-451-3000


 info@everestgrp.com


For more information about this topic please contact the author(s):


 Jimit Arora, Partner

 jimit.arora@everestgrp.com

 Archit Mishra, Senior Analyst

 archit.mishra@everestgrp.com

 Ronak Doshi, Senior Analyst

 ronak.doshi@everestgrp.com