fs viewpoint

www.pwc.com/fsi

Using third party service providers can be a risky business. Get fewer headaches by getting on top of the problem.

Significant others:

How financial firms can manage third party risks

pwc

Executive summary

Third parties have been the source of countless problems for financial institutions. But with the right approach to managing risk, firms can turn third parties into strategic assets.

How are financial institutions responding to demands for stronger oversight of third parties?

To find out, we surveyed financial institution leaders to better understand how their third party risk management functions operate and where they're making investments. PwC's 2014 Third Party Risk Management Survey draws on insights from executives and managers across the United States to identify key trends and leading practices in the industry.

Third parties: a growing burden

In today's environment, it would be nearly impossible to find a financial institution that doesn't contract with third parties to perform many essential functions. Over the last decade, use of third parties has indeed helped institutions to grow revenues, cut costs, and improve the customer experience.

However, these proven upsides have come with equally apparent downsides: more frequent operational setbacks such as major service interruptions, mishandling of customer or employee data, and non-compliance with laws and regulations. Many of these issues have originated with third party service providers.

The costs include not only monetary losses, but also loss of reputation and market share. Add to that the potential for regulatory enforcement actions and hefty regulatory fines, and the numbers begin to climb.

Turning liabilities into assets

Do the benefits of using third parties outweigh the downside risks, as well as the extra costs and time needed to manage and oversee them? PwC's experience and our 2014 Third Party Risk Management Survey indicate that they can—if a firm has a robust third party risk management (TPRM) program in place. Such a program can help a firm fulfil its obligations to customers, shareholders, and regulators. Ultimately, it may even make using third parties less risky than keeping those functions in-house.

45%

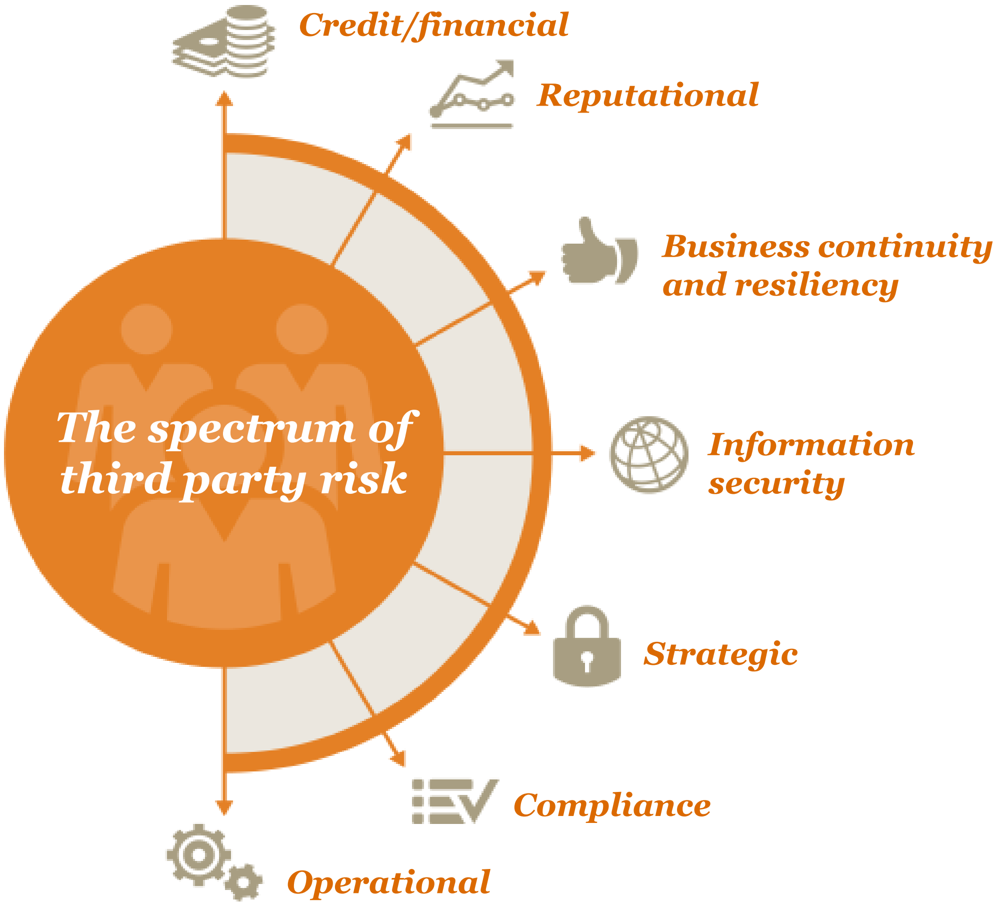
of financial services CEOs plan to enter into at least one new joint venture or strategic alliance over the next 12 months.

Source: PwC, "18th Annual Global CEO Survey," January 2015.

Point of view

The evidence is piling up: it's time for financial institutions to take a more systematic approach to managing third party risk.

Figure 1: Using third parties comes with a broad spectrum of risks.



Increased use of third parties

Over the past several years, financial institutions have increased their collaboration with third parties to perform a growing number of functions—not just printing checks, collecting payments, and processing data. This is partly in response to higher customer expectations for service.

As customers increasingly demand more customized, real-time experiences that are accessible through multiple digital channels, firms have looked to outside providers with the requisite resources and expertise. The 18th annual PwC Global CEO survey shows that more than 40% of banking CEOs see joint ventures, strategic alliances, and informal collaborations as an opportunity to strengthen innovation and gain access to new customers and new technologies.[1]

More adverse incidents

However, it is not always easy to ensure that services provided through third parties remain seamless and aligned with brand standards and strategies. As the use of third parties has grown, so have the number and severity of publicized security breaches, compliance issues, and service interruptions traceable to them. Boards of directors are increasingly worried about the number and type of activities their firms outsource and how well their firms manage the risks arising from these third party relationships (see Figure 1).

[1] PwC, "18th Annual Global CEO Survey," January 2015.

Regulators have taken steps to help ensure that financial institutions keep third party risks firmly in check.

57%

of survey respondents have an accurate inventory of all third parties that handle sensitive firm, employee, and customer data.

Source: PwC, "2014 Global State of Information Security Survey," September 2014.

Stricter regulations over how financial institutions manage third party risk

Regulators are also concerned. Several US regulatory agencies have significantly raised standards for oversight of third parties in recent years.[1] Moreover, they have reiterated the range of third party relationships that the regulations cover to eliminate categorical exemptions.

These regulators particularly target business-critical functions such as payments, clearing, settlements, custody, and IT.[2] They also require that oversight and due diligence—as well as the involvement of a firm's board of directors—be commensurate with the risk and complexity of the third party relationship.

Beyond third party risk

Regulators have made it clear that financial institutions cannot outsource their controls, and that they expect firms to hold their third parties to the same high standards that firms themselves must meet.

Firms need to consider how their third parties are handling a wide range of issues:

- **Customer complaints**—The Consumer Financial Protection Bureau in the US, as well as foreign regulators such as the Financial Conduct Authority in the United Kingdom, have increased their scrutiny of the programs that firms use to address customer complaints.
- **Cybersecurity**—Regulators have cited banks, broker-dealers, investment advisers, and insurance companies for weak cybersecurity controls at their third parties. One report found that nearly one in three banks surveyed did not require their third party providers to notify them of cybersecurity breaches.[3]
- **Resiliency**—Regulators are also intent on improving the *resiliency* of financial institutions and their third parties. They want to see processes in place not only to lower the risk of failure, but to reduce the impact of a failure on the broader economy by sustaining critical operations during the resolution process.

[1] These include the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Federal Financial Institutions Examination Council (FFIEC), New York State Department of Financial Services (NYDFS), the Securities and Exchange Commission (SEC), and the Financial Industry Regulatory Authority (FINRA).

[2] The OCC refers to these as "critical activities" in its OCC 2013-29 advice bulletin.

[3] These include the New York State Department of Financial Services, "Report on cyber security in the banking sector," April 2015.

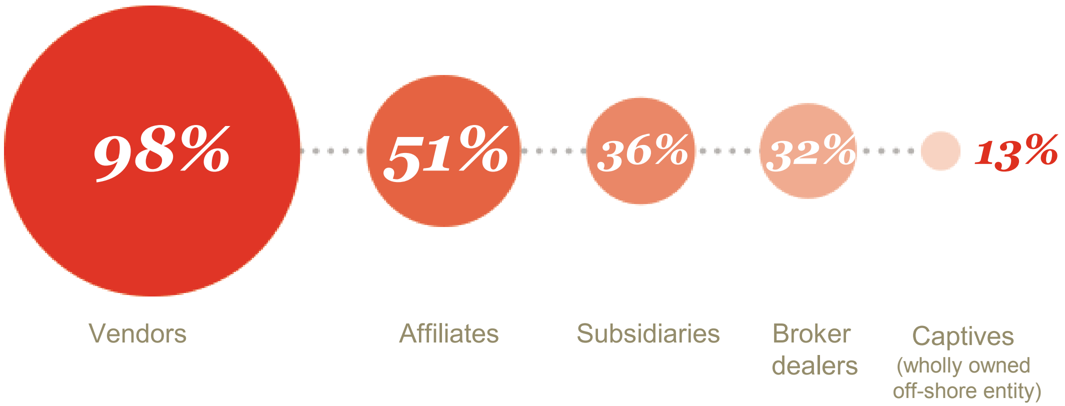
Even after years of growing reliance on third parties and increasing regulation, oversight at most financial institutions still has far too many gaps.

PwC's 2014 Third Party Risk Management Survey results show that most firms have not updated their TPRM programs to address tougher regulations.

While one of the main requirements in recently updated regulatory guidance bulletins is identifying business-critical functions, nearly two out of every five of our survey respondents have not completed this essential first step.

Figure 2: Many respondents include only vendors in their TPRM programs.

Q: What is the scope of your TPRM program?



Source: PwC, "2014 Third Party Risk Management Survey." December 2014.

Similarly, our research indicates that financial institutions are not adequately monitoring "fourth parties"—the subcontractors of their third parties. A full 45% of respondents said that they rely on third parties to monitor their subcontractors—without performing additional checks to review the results. Another 6% either don't know if their third parties use subcontractors, or have no visibility into how subcontractors are monitored.

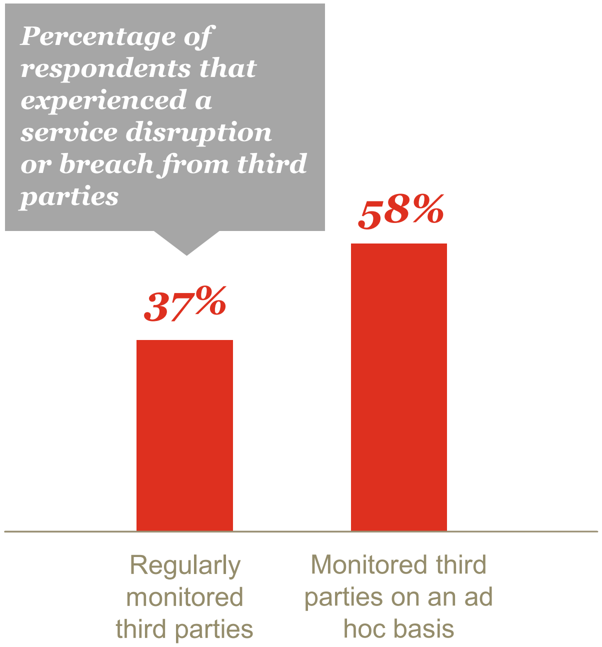
Even the scope of many TPRM programs seems problematic. In its most recent guidance bulletin, the OCC particularly highlighted its definition of third party relationships, which is "any business arrangement between a bank and another entity, by contract or otherwise."[1] As seen in Figure 2, however, barely half of our survey respondents said that their oversight programs include affiliates. New regulations relating to business continuity arising from the Dodd-Frank Wall Street Reform and Consumer Protection Act underscore the importance of having backup plans for *all* business-critical functions, not just those provided by third parties.

We also found that boards of directors are not sufficiently involved in oversight and governance of third party risk management. Only 55% of respondents said a board committee participates in TPRM oversight and governance, while some regulators explicitly expect the board to perform these functions for all third party relationships involving business-critical functions.

[1] OCC, "Third Party Relationships," October 2013.

A surprising number of financial institutions are still relying on an ad hoc approach to manage their third party relationships.

Figure 3: Financial institutions that did not perform regular monitoring of third parties experienced more disruptions or breaches.



Source: PwC, "2014 Third Party Risk Management Survey." December 2014.

Our survey also showed that many firms still do not have an enterprise-wide, standardized framework for third party risk management. In some cases, these deficiencies have resulted in compliance issues, security breaches, or problems for customers.

Consider these survey findings:

- 33% of respondents that performed regular on-site visits of third parties experienced a service disruption or breach. For respondents that did not perform on-site visits or performed them only on an ad hoc basis, the percentage of disruptions rose to 50%.
- 37% of respondents that regularly monitored third parties with ongoing due diligence activities experienced a service disruption or breach. For respondents that did not perform this regular monitoring, the percentage of disruptions rose to 58% (see Figure 3).

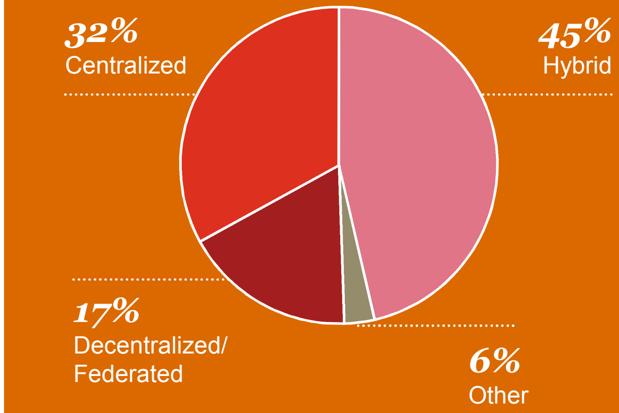
Limited reporting was another common issue that survey participants reported. Many respondents used scorecards to monitor service quality and manage issues, but did not as consistently monitor other important factors such as risks, costs, and customer complaints.

Which TPRM program structure should you adopt?

As seen in **Figure 4**, financial institutions use a variety of TPRM program structures. Culture and geography are two major factors that often influence an organization's decisions when selecting a model.

For example, a global company operating across multiple regions may find that a decentralized or hybrid model suits its purposes better than a centralized one. However, even with a decentralized model, a centralized TPRM office can help ensure that policies, procedures, and training are implemented consistently across the organization. A centralized TPRM office can also provide integrated reporting across third party relationships.

Figure 4: What model does your organization use for its TPRM program?



Source: PwC, "2014 Third Party Risk Management Survey." December 2014.

What leading practices have we seen financial services firms use to improve their TPRM practices?

While the TPRM framework will vary from firm to firm, some common elements are critical to success. These include third party stratification, insight into subcontractors, a centralized issues and complaints management database, and a centralized TPRM office to oversee the program.

Focus on the riskiest services

We consider stratification—analysis of third party relationships to identify those services requiring more extensive oversight—a particularly important first step on which other processes will depend. By focusing on the inherently riskiest relationships involving the most critical functions, firms can both control their TPRM costs and direct valuable and limited resources to where they are most needed.

Many institutions automatically assign the same risk to all services a third party performs, even though services may vary considerably for different business units and functions. We believe a firm should look at individual services a third party performs to make sure the risk assessment is in accordance with the nature and complexity of the products or services provided. This would include factors such as criticality, data sensitivity, concentration risk, and the number of business units involved.

Don't forget about subcontractors

An effective third party risk management program needs to have insight into "fourth party" subcontractors that third parties are themselves using and managing, in order to ensure that the firm understands how the subcontractors are delivering their products or services. They may find, in some cases, that there are contractual issues that keep them from fully applying their risk policies to subcontractors.

For example, a firm may not be able to insert a "right to audit" clause for fourth parties into an outsourcing agreement if the third party does not have such rights in its subcontractor relationships.

Establish a central office to administer and oversee the program

We believe that a central third party risk management office is another key ingredient in a successful TPRM program, particularly as firms expand nationally and globally. This central office should administer the oversight process, ensuring standardization and central reporting, together with a thoughtful approach to training and change management.

Leading firms are also using offshore and onshore delivery models to help standardize assessments and extend the office's reach to third parties by providing services in remote locations. They can also greatly reduce overall program costs by providing a monitoring and reporting utility service to the "three lines of defense" (business unit operations, risk management/compliance functions, internal audit).

Track TPRM issues and customer complaints in central databases

As part of the process, the TPRM office should use a central repository or database for initial due diligence, ongoing monitoring, and re-assessments. This helps maintain proper identification, management, tracking, reporting, and oversight of issues related to third parties.

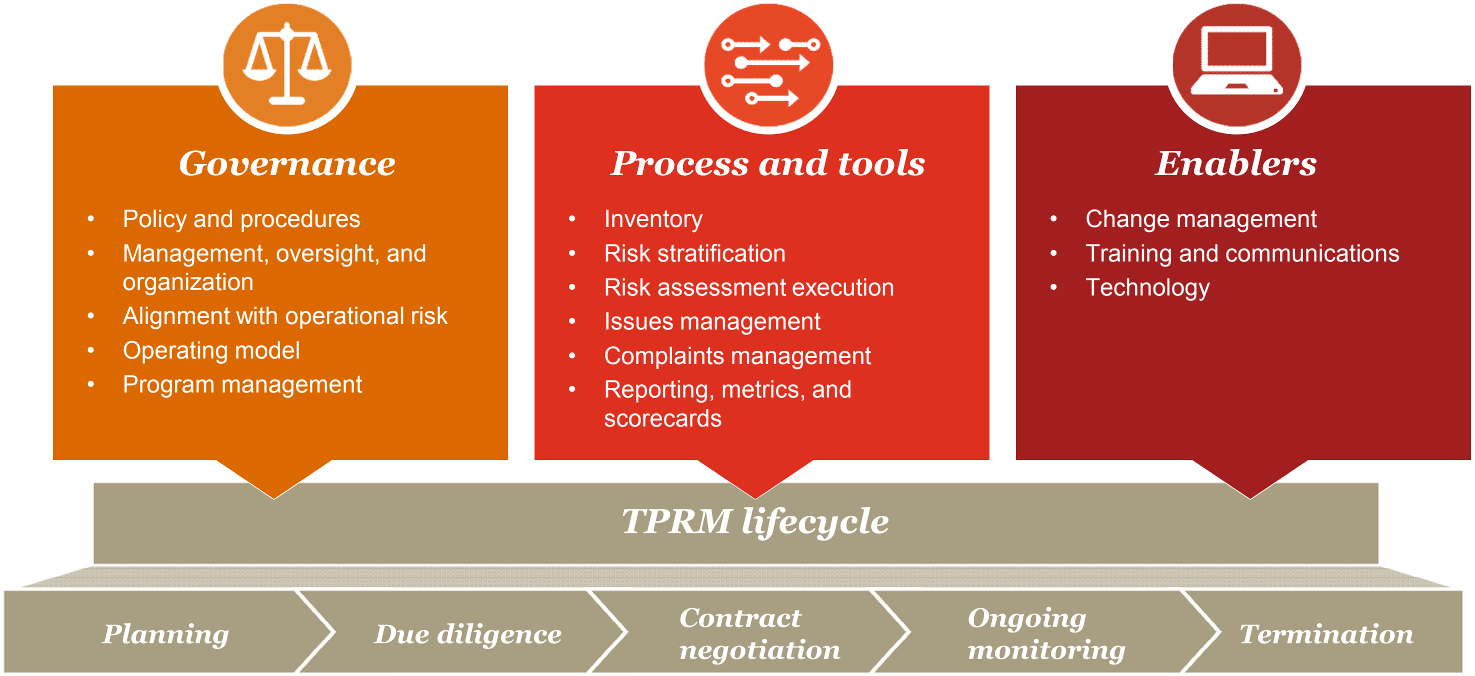
We suggest financial institutions adopt a coherent, well-thought-out third party risk management program to reduce risk exposure and help contain operational costs.

Leading practices like stratification and a central TPRM office should be part of an overarching TPRM framework. Firms should integrate this framework with their operational risk policies. We suggest that the TPRM framework incorporate three main elements: governance, processes and tools, and what we call "enablers."

Governance helps define the operating model for the TPRM program, which should include a central TPRM office as well as policies, procedures, and standards for day-to-day program management and business operations. The TPRM program applies across the entire lifecycle of each third party relationship—from the planning and due diligence phases through contract negotiation, ongoing monitoring, and termination.

A single third party inventory, risk stratification, monitoring plans, scorecards, and assessment are **processes and tools** that capture and monitor the inherent and residual risk of the services third parties provide.

To make the entire TPRM program work, we recommend that institutions adopt three essential **enablers**. The first two, change management and training and communications, promote stakeholder buy-in. An effective program also needs the right supporting technology, which can include contracting, risk assessment, and other tools that facilitate documentation and reporting.



Governance

- Policy and procedures
- Management, oversight, and organization
- Alignment with operational risk
- Operating model
- Program management

Process and tools

- Inventory
- Risk stratification
- Risk assessment execution
- Issues management
- Complaints management
- Reporting, metrics, and scorecards

Enablers

- Change management
- Training and communications
- Technology

TPRM lifecycle

Planning → ***Due diligence*** → ***Contract negotiation*** → ***Ongoing monitoring*** → ***Termination***

Beyond better risk management, effective TPRM programs can also deliver valuable insights that inform strategic decisions.

Figure 5: What is the estimated value of benefits received?

19% of respondents have experienced benefits greater than

$1 million.

27%	up to $1m
13%	$1m-$5m
6%	$5m-$10m+

Source: PwC, "2014 Third Party Risk Management Survey." December 2014.

Use TPRM to gain strategic insights

Many financial institutions are shocked when they realize how many third parties they have on their rosters. Thirty-eight percent of our survey respondents had between 1,000 and 10,000 active third party relationships, and nearly one-quarter of them had more than 10,000.

An effective TPRM program improves transparency for a firm—not only regarding how much its third parties cost, but also which business units use them and which markets and customer segments they serve. Armed with a more thorough, accurate view of the role third parties play across the organization, financial institutions can use data analytics to support strategic business decisions. The insights they gain can help to:

Improve the customer experience

More proactive monitoring and management of third party service quality can help firms improve the customer experience. It can also help reduce service disruptions and data breaches.

Identify new strategic partnerships

By analyzing how third parties are used across products, markets, and channels, firms may potentially identify new strategic partnerships that extend their sales and servicing capabilities.

Drive down costs

Our survey shows not only improved third party performance, but also clear financial results (see Figure 5). Better visibility helps firms become more strategic about which third parties they engage. They may be able to consolidate services with fewer providers, negotiate more competitive pricing, and identify less costly alternatives for low-value activities.

A TPRM program can also reduce oversight costs by focusing due diligence and monitoring efforts on the most critical and risky services, rather than using a "one-size-fits-all" approach.

Improve market agility

Regulators, including the OCC and the Fed, now require financial institutions to have a contingency plan for their most critical functions. In addition to expediting replacement of third parties if needed, these backup plans can improve a firm's ability to seize opportunities quickly—such as launching new services with existing third parties.

Enhance shareholder value

In the end, the right framework can help improve the bottom line in a number of ways, including reduction in compliance-related penalties, fewer service disruptions, less intense regulatory scrutiny, a smaller number of third parties, higher customer confidence, and more appropriately trained and placed resources.

Financial institutions can expect plenty of obstacles when building a strong TPRM program. We've identified key success factors that can help overcome these challenges.

Obstacles we've observed	Approaches for overcoming challenges
Difficulty getting business buy-in Any change can encounter resistance from stakeholders, particularly if the process is not smooth.	• Ensure visible executive sponsorship and strong leadership at a functional and program level. Make effective use of business unit leaders as "change agents" to drive adoption. • Collaborate with all functional and operating group stakeholders to improve transparency into the process. A designated liaison can help build relationships, increase awareness, and integrate third party risk management practices into day-to-day business processes. • Keep the TPRM program simple by leveraging existing processes, prioritizing the most critical TPRM objectives, automating where possible, and avoiding creation of special third party categories. This supports ease of use and encourages adoption. Once a strong foundation is in place, firms can evolve the program to support more sophisticated needs.
Defining the scope and focus of the TPRM program It is not always clear which third parties and partners a program should include, or which should take priority.	• Cast a wide net when deciding what types of third parties and relationships should be in-scope. For some financial institutions, regulatory guiding principles mandate inclusion of correspondent banks or indirect lending partners (such as auto or consumer finance companies). • Adopt third party stratification to save costs, minimize operational impact, and define where to place resources.

Financial institutions can expect plenty of obstacles when building a strong TPRM program. We've identified key success factors that can help overcome these challenges (continued).

Obstacles we've observed	Approaches for overcoming challenges
Overstretched operational resources Many financial institutions have pared costs in back office and other operations, making it difficult to monitor compliance with TPRM requirements.	• Focus on having the third parties do as much of the "heavy lifting" as possible to comply with TPRM policies. Shifting responsibility for administrative activities, such as completing questionnaires and maintaining current insurance certificates, can reduce the burden on the institution. • Use automated workflow technology and other strategic IT solutions to link third party information across functions such as procurement, accounts payable, finance, risk, and legal. IT solutions can also serve as a repository for third party documentation, route notifications and approvals, centralize tracking of issues, and enable dashboard reporting.
Inconsistent understanding of third party risks Not all parts of a financial firm will have an equal grasp of the issues involved in third party risk management. And unless they receive guidance, different departments will develop their own approaches.	• Agree upon a common set of terms and definitions; this helps create a consistent method for defining, managing, and measuring third party risks. • Focus on delivering consistent messages through both top-down and bottom-up communications (such as success stories and feedback) across business units, enterprise functions, and the board of directors. • Use multiple channels to provide information updates to program stakeholders. For example, a centralized website can host commonly requested tools and templates, while monthly newsletters can alert staff to updates.

Without a consistent and comprehensive TPRM framework, firms risk reputational damage, incomplete monitoring efforts, and increased program costs.

Operational and reputational damage

Failure to implement the right third party risk management program may hamper a financial institution in many ways. The most worrying, of course, is the potential damage that a third party's non-compliance, mishandling of sensitive information, and operational missteps can cause to a firm's customers, business, reputation, and bottom line. The consequences can include impaired customer service and loss of market share, as well as regulatory fines and penalties. Without a good TPRM program, situations like these become more likely.

Incomplete monitoring efforts

Without a comprehensive inventory of third parties and the products and services they provide, a firm may be exposed to risks it may not even be aware of—either directly through undocumented third party relationships, or indirectly through undocumented relationships that third parties may have with their subcontractors.

Unsustainable TPRM program costs

The lack of a proper framework means that a firm will probably spend more time and resources on managing third party risk than it needs to. Without processes such as stratification to identify priorities, costs may become unmanageable for an effort that is largely ineffective.

Institutions can no longer rely on an ad hoc approach to keep track of all their third party relationships and assume that all will end well.

In today's rapidly changing financial landscape, it may be hard for financial institutions to avoid using third party partners to provide ever-more sophisticated services to customers.

A robust TPRM program can help a financial institution fulfil its obligations to customers, company stakeholders, shareholders, and regulators. In the long run, we believe a strong program has the potential to drive down risks to levels equal to or lower than those for performing the functions in-house.

Competitive intelligence

Our observations of industry practices.

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 do considerable catch-up work.

Area of focus	Financial Institution A	Financial Institution B	Financial Institution C
Governance: Third party risk management framework	● • The firm maintains a central third party risk management (TPRM) office, which monitors and oversees each program function and stakeholder group. • The lines of business (LoB) oversee critical third parties within each business. Risk managers have been assigned for significant relationships. • Structured groups within the LoB oversee performance of TPRM testing. • The TPRM program aligns with the operational risk program.	◐ • The institution has LoB governance over critical third parties specific to each business. Risk managers have been assigned for significant relationships. • A central TPRM offices oversees this process with the assistance of distributed risk operation functions across the enterprise.	○ • TPRM program oversight is informal. The firm has limited or no governance over critical third parties, and may or may not assign third party risk managers for significant relationships.
Processes and tools: Inventory of third parties	● • The firm develops a comprehensive list of third party services through data analysis of accounts payable, contract, and risk-related information. It reviews third party source systems and amends the list to reflect accurate and complete information based on data analysis and business validation. • It maintains data quality through a third party risk management system.	◐ • The firm maintains a list of third parties that receive sensitive internal or customer information, as well as those with the largest contracts. It does not conduct any procedures to determine whether or not the list is complete.	○ • The firm focuses its assessments on those third parties with the largest contracts. However, it does nothing to determine whether the list is complete or that it includes smaller third parties that have access to sensitive data.
Processes and tools: Due diligence assessments	● • The firm conducts and documents due diligence assessments for significant third party relationships prior to onboarding new service providers. Assessments typically include country, financial, and reputational risk, business continuity planning (BCP) and disaster recovery (DR) arrangements, information security, privacy, technology, legal, and compliance analysis.	◐ • The firm conducts and documents due diligence assessments for significant third party relationships prior to onboarding new service providers. This assessment consistently includes financial, reputational, BCP/DR, and security analysis, but no other type of analysis.	○ • The firm may conduct an assessment for some new third parties (or rely on a third party self-assessment) prior to onboarding new service providers. These assessments may cover financial and security analysis.

● Leading ◐ On par ○ Lagging

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 do considerable catch-up work (continued).

Area of focus	Financial Institution A	Financial Institution B	Financial Institution C
Processes and tools: Monitoring	● - The firm monitors third parties using a defined, documented, and technology-supported approach that includes monitoring plans, scorecards, assessments, and quality assurance reviews.	◐ - The firm monitors third parties using a defined, documented, and technology-supported approach that includes performance management and ongoing due diligence assessments.	○ - The firm monitors third parties only on an ad hoc basis. The monitoring may be performed sporadically, but consistently includes risk management, ongoing due diligence assessments, and issues tracking.
Processes and tools: Central issues and complaints database	● - The firm maintains a centralized repository for third party issues, remediation actions, assessment results, contracts, scorecards, and results from surveillance. - The firm leverages a standard approach for issues and complaints management, including escalation and exception management processes.	◐ - The firm maintains a centralized repository for third party issues, assessment results, and contracts.	○ - The firm maintains several repositories in various business silos that only partially cover issues, remediation plans, assessment results, contracts, and scorecards.
Enablers: Central TPRM technology solution	● - The firm has a central enterprise system that supports third party uploads; performs some automated due diligence; creates dashboards, scorecards, and other reporting; and includes two-way links to enterprise systems of record.	◐ - The firm has a central enterprise system that performs contract management, initial due diligence and some reporting, and has a one-way link to enterprise systems of record.	○ - The firm has several technology solutions and systems that may cover due diligence, some reporting, and include informal manual links to enterprise systems of record.
Enablers: Third party legal and regulatory change process	● - As part of its regulatory change process, the institution collaborates with its third party providers to modify activities, controls, and approaches, as needed, to remain in compliance with legal and regulatory changes.	○ - The firm has no system for determining whether third parties are adapting to changes in regulations.	○ - The firm has no system for determining whether third parties are adapting to changes in regulations.

● Leading ◐ On par ○ Lagging

A framework for response

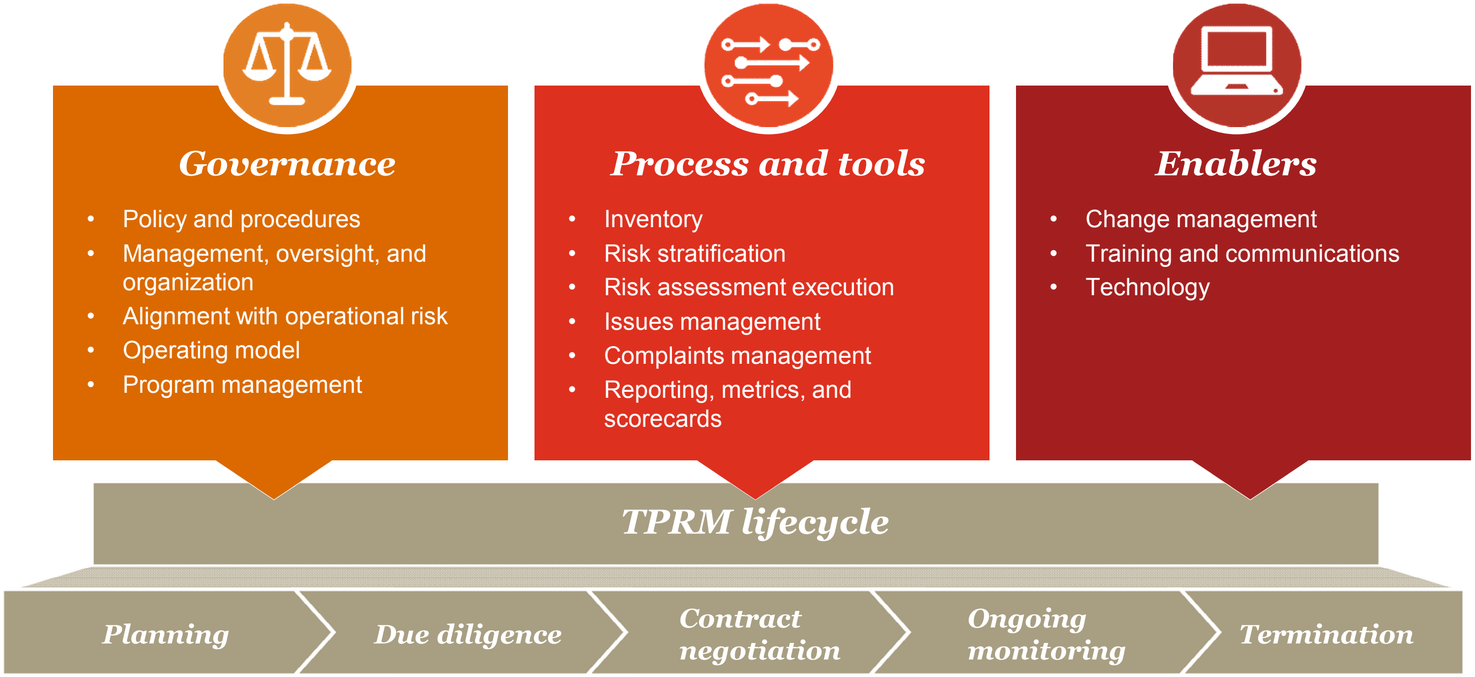
Our recommended approach to the issue.

Effective third party risk management (TPRM) requires the integration of multiple components.

We believe that to be successful, a TPRM program needs the right governance, the right processes and tools, and the right enablers in place.

- **Governance** incorporates guiding principles from senior management and regulatory guidance from federal authorities that help define a common approach to due diligence and risk management. It also assigns responsibilities for key TPRM activities.
- **Processes and tools** include the key functions that a TPRM program carries out to manage third party risk, and the mechanisms it uses to effectively perform those functions.
- **Enablers** such as technology help you run the TPRM program efficiently. Other examples such as change management, training, and communication help you gain the buy-in and support you need to meet the TPRM program's goals.

All of these components fall within the overall third party lifecycle from planning through due diligence, contract negotiation, ongoing monitoring, and termination. However, they do not have a one-to-one relationship with these phases. Governance, for example, is an important part of planning, but also part of contract negotiation and ongoing monitoring.



Governance

- Policy and procedures
- Management, oversight, and organization
- Alignment with operational risk
- Operating model
- Program management

Process and tools

- Inventory
- Risk stratification
- Risk assessment execution
- Issues management
- Complaints management
- Reporting, metrics, and scorecards

Enablers

- Change management
- Training and communications
- Technology

TPRM lifecycle

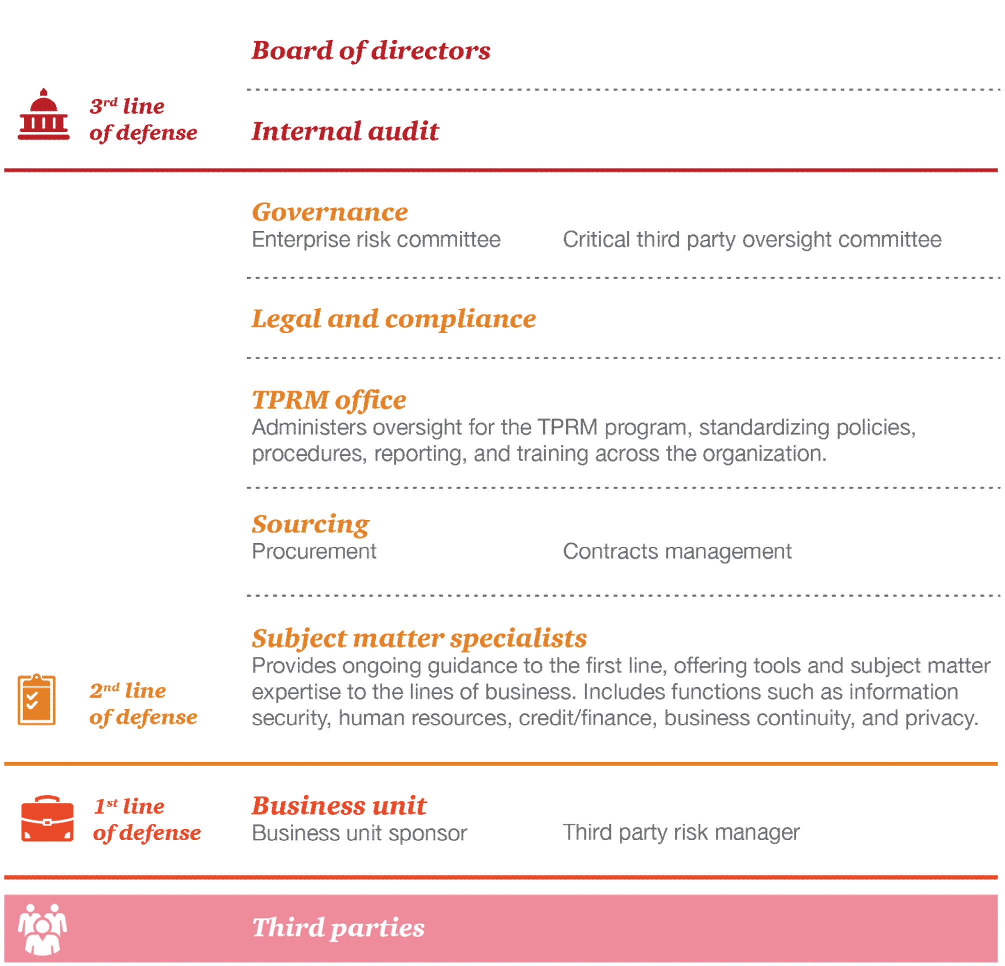
Planning → *Due diligence* → *Contract negotiation* → *Ongoing monitoring* → *Termination*

Governance

TPRM governance helps you provide overall direction for the program’s operating model and policies and procedures for day-to-day functioning. The model should lay out program management and organization, assigning specific roles and responsibilities.

In addition, the governance approach should consider how TPRM activities integrate with your other risk management functions—particularly the three lines of defense (business units; risk, compliance and legal; internal audit)—to promote consistency and quality in program activities.

Figure 6: Illustrative governance model



3rd line of defense

Board of directors

Internal audit

2nd line of defense

Governance

Enterprise risk committee — Critical third party oversight committee

Legal and compliance

TPRM office

Administers oversight for the TPRM program, standardizing policies, procedures, reporting, and training across the organization.

Sourcing

Procurement — Contracts management

Subject matter specialists

Provides ongoing guidance to the first line, offering tools and subject matter expertise to the lines of business. Includes functions such as information security, human resources, credit/finance, business continuity, and privacy.

1st line of defense

Business unit

Business unit sponsor — Third party risk manager

Third parties

Processes and tools

A successful TPRM program includes a number of processes and tools for managing and monitoring third parties throughout the five phases of each third party's lifecycle. In our experience, it's crucial for these processes and tools to include a third party inventory, risk stratification, risk assessment, issues management, reporting, metrics, and scorecards.

Inventory and risk stratification

Risk stratification focuses resources on the third party relationships that matter most, limiting unnecessary work for lower-risk relationships (see Figure 7). The first step is to create a thorough inventory of all third parties and the services they provide. It's important to have adequate checks and balances to verify the list is complete—for example, through periodic comparisons to the procurement and accounts payable systems.

Once the inventory has been established, filter the list based on the nature and complexity of the products or services provided, including factors such as criticality, data sensitivity, concentration risk, and the number of business units involved. Keep in mind that some third parties may provide a range of services, with varying degrees of risk, to different business units.

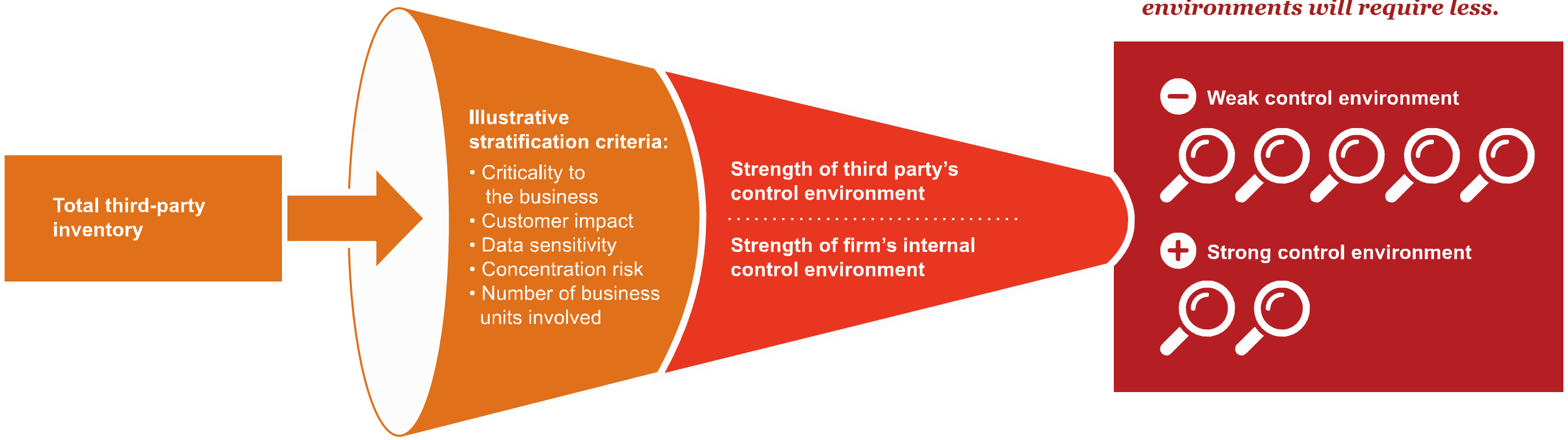
In addition, stratification analysis should consider concentration risk. For example, too many third parties clustered in one geographical area could intensify business continuity risk, or a firm might rely heavily on too few third parties.

Figure 7: Tailor due diligence and monitoring processes based on the levels of inherent and residual risk.

Use stratification criteria to prioritize higher-risk relationships based on inherent risk.

Tailor risk assessment and monitoring activities based on the control environment and residual risk.

Third parties with weak control environments will require more due diligence and monitoring, while those with stronger environments will require less.


Total third-party inventory
Illustrative stratification criteria:
• Criticality to the business
• Customer impact
• Data sensitivity
• Concentration risk
• Number of business units involved
Strength of third party's control environment
Strength of firm's internal control environment
Weak control environment
Strong control environment

Processes and tools

Examples of third party due diligence assessments:

- Reputational
- Operational competency
- Subcontractor
- Technology
- Financial
- Business continuity and resiliency
- Country risk
- Human resource risk
- Concentration risk
- Physical security
- Information security and privacy
- Compliance

Leading financial institutions are using social listening tools, offshore delivery models, and other methods to improve the accuracy and scope of their risk assessments.

Risk assessment execution

Once a firm has identified third parties performing high-risk services, the next step is to perform due diligence assessments for each of those third parties. The results of these assessments help establish the appropriate level and frequency for monitoring and oversight for each third party.

Firms should execute risk assessments at two stages during the third party's lifecycle:

- During the due diligence process.
- Periodically after on-boarding to verify that a third party continues to meet the firm's needs.

In both of these stages, avoid using a "one-size-fits-all" approach when performing the risk assessment. Only those controls that apply to the services a third party provides require assessment.

The depth and frequency of the follow-up assessments will depend on the results of the stratification analysis. You might decide that the most inherently risky third parties will require an on-site audit twice a year, for example. Use of offshore and onshore delivery models can also standardize assessments, extend geographical reach, and reduce assessment costs.

Issues management

How an organization identifies, reports, and resolves issues is another critical component for a TPRM program. We suggest that you use a central third party issues repository with standardized processes for identifying, categorizing, remediating, and reporting issues. The repository should include issues identified not only through the TPRM program's risk assessments, but also through other sources such as internal audit and regulators.

For third parties that interact directly with customers, maintain consistent procedures for managing customer complaints. For example, third parties should have standardized protocols for identifying, classifying, escalating, and reporting customer complaints. Complaints that reach a certain severity should also be included in your customer complaint repository.

Third party relationship managers, risk managers, subject matter specialists (such as from legal or compliance), and third party representatives should collaborate to appropriately remediate all issues.

Processes and tools

Reporting, metrics, and scorecards

Reporting, scorecards and metrics—particularly key risk indicators and key performance indicators—are vital tools in managing both third party performance and the health of the TPRM program itself. Reporting should address the needs of your TPRM office, management, and business units (see Figure 8).

Third party metrics measure the performance of individual third parties in such areas as:

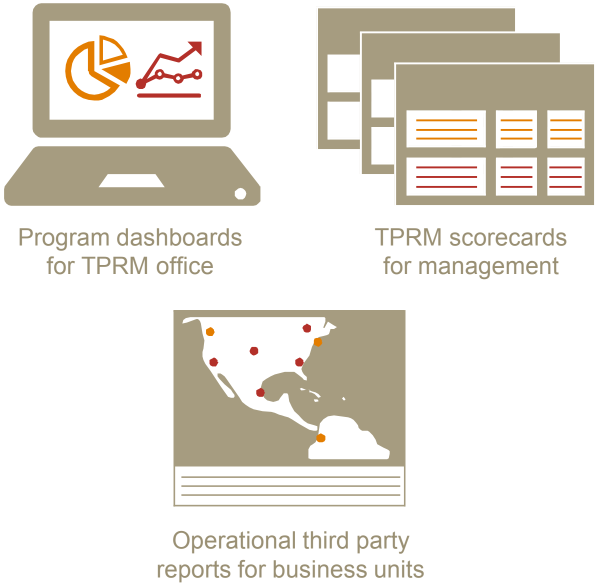
- Quality—low defects, compliance with standards.
- Customer support—effective communication, complaint management.
- Service and delivery—on-time delivery, flexibility.
- Human capital—competent staff, ongoing training.

Management-level reporting may also provide insight into how third parties are performing as a group. This aggregate reporting highlights exceptions (for example, service providers that provide similar services to others but are more costly) and trends over time (for example, whether customer complaints fall after implementation of new customer handling protocols).

TPRM program metrics measure such internal program-related progress and issues as:

- Number of third parties with access to sensitive information.
- Number of third parties supporting critical processes; percentage of critical activities performed by third parties.
- Number of issues by third party.
- Percentage of staff trained in third party risk management processes.
- Remediation plans by status.

Figure 8: Reporting should address the needs of the TPRM office, management, and business units.



Program dashboards for TPRM office

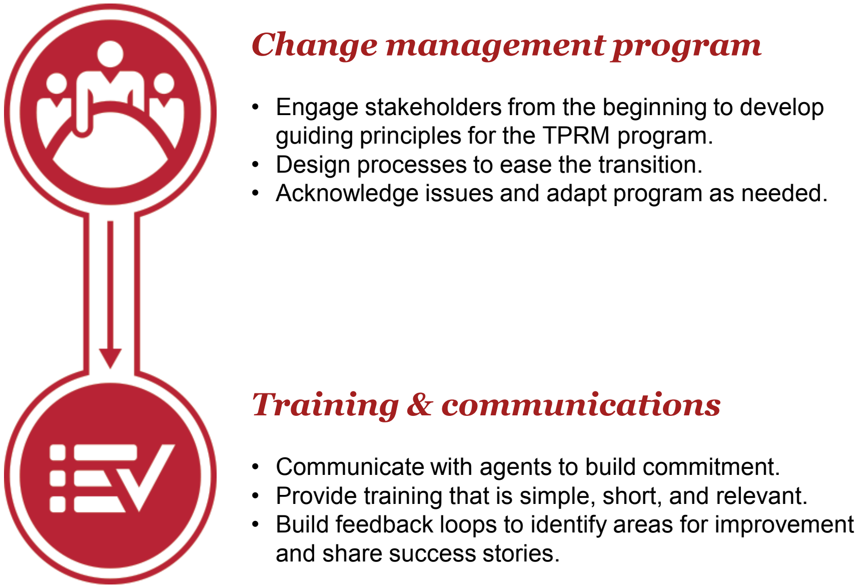
TPRM scorecards for management

Operational third party reports for business units

Enablers

As with any major undertaking, having the right support structures in place will help you implement the TPRM program and keep it current with business needs. In our view, all TPRM programs should provide for three enablers: change management, training and communications, and technology.

Figure 9: Training and communications should be linked to the broader change management program.



Change management program

- Engage stakeholders from the beginning to develop guiding principles for the TPRM program.
- Design processes to ease the transition.
- Acknowledge issues and adapt program as needed.

Training & communications

- Communicate with agents to build commitment.
- Provide training that is simple, short, and relevant.
- Build feedback loops to identify areas for improvement and share success stories.

Change management

A sound change management plan provides the right level of structure and discipline to manage the complex relationships and dependencies in a TPRM program (see Figure 9). It engages the right leaders and stakeholders from the start, soliciting their input to develop guiding principles for the TPRM program. It gives them a voice in planning the program rollout so that competing priorities can be reconciled and aligned. Lastly, it identifies the process changes and deliverables needed to foster accountability and deliver business benefits.

Training and communications

Start your TPRM training and communications program by evaluating who the stakeholders are, how they will be impacted by the TPRM program, and the level of support they will need to understand and implement new requirements. By tailoring the approach and scope of training (both materials and delivery) based on location, roles, and existing training strategy, you can improve adoption by integrating the program with day-to-day activities of employees.

Measuring training effectiveness also helps organizations find out if employees are adapting well to changes. If they're not, measurement data will give the firm valuable feedback in adapting the program.

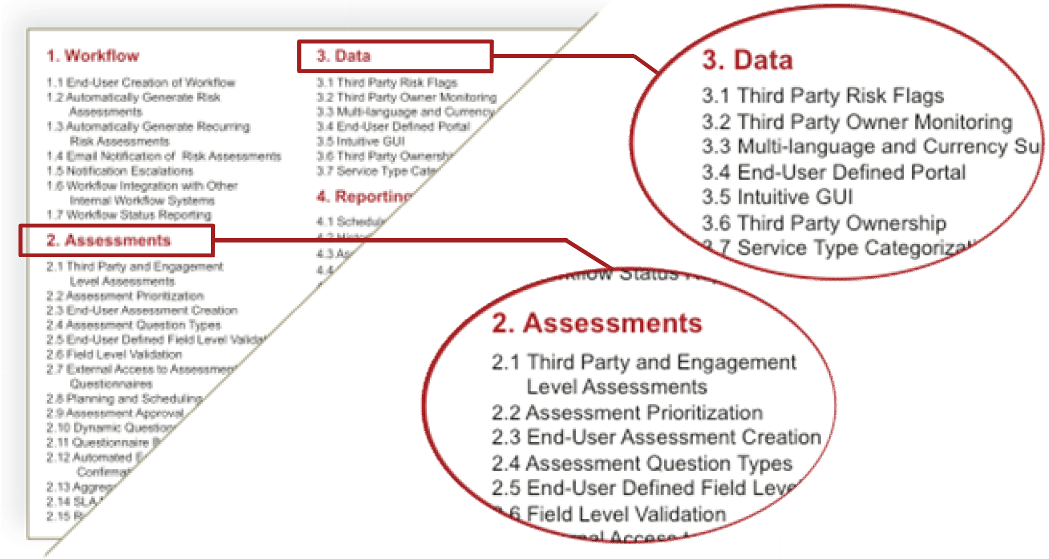
Enablers

Technology

Technology is a core enabler at every stage of a TPRM program. It is key to supporting and even completely automating workflows of all kinds, including third party risk assessments, analyzing and collating risk data, reporting, and issues management. Some programs adopt self-service portals that third parties can use for reporting, documentation, and completion of required surveys.

In general, it's important to consider your third party risk management objectives and adopt the right technology to support those objectives. When designing TPRM processes, make sure they are flexible enough to work with whatever technology platform you ultimately select.

Figure 10: Business, functional, and technical requirements should be adequately considered.



1. Workflow

1.1 End-User Creation of Workflow
1.2 Automatically Generate Risk Assessments
1.3 Automatically Generate Recurring Risk Assessments
1.4 Email Notification of Risk Assessments
1.5 Notification Escalations
1.6 Workflow Integration with Other Internal Workflow Systems
1.7 Workflow Status Reporting

2. Assessments

2.1 Third Party and Engagement Level Assessments
2.2 Assessment Prioritization
2.3 End-User Assessment Creation
2.4 Assessment Question Types
2.5 End-User Defined Field Level Validat
2.6 Field Level Validation
2.7 External Access to Assessment Questionnaires
2.8 Planning and Scheduling
2.9 Assessment Approval
2.10 Dynamic Question
2.11 Questionnaire
2.12 Automated E Confirmat
2.13 Aggreg
2.14 SLA
2.15 R

3. Data

3.1 Third Party Risk Flags
3.2 Third Party Owner Monitoring
3.3 Multi-language and Currency
3.4 End-User Defined Portal
3.5 Intuitive GUI
3.6 Third Party Ownersh
3.7 Service Type Cate

4. Reporting

4.1 Schedul
4.2 Histo
4.3 As
4.4

3. Data

3.1 Third Party Risk Flags
3.2 Third Party Owner Monitoring
3.3 Multi-language and Currency Su
3.4 End-User Defined Portal
3.5 Intuitive GUI
3.6 Third Party Ownership
3.7 Service Type Categoriza

2. Assessments

2.1 Third Party and Engagement Level Assessments
2.2 Assessment Prioritization
2.3 End-User Assessment Creation
2.4 Assessment Question Types
2.5 End-User Defined Field Leve
2.6 Field Level Validation

TPRM technology leading practices

- Appropriate consideration and prioritization of business, functional, and technical requirements (see Figure 10).
- Accurate and complete organizational record of third party relationships across the organization, including the employees responsible for managing them. This helps facilitate transitions as employees change roles or leave the company.
- Comprehensive contracts management system and third party master data repository.
- Consistent taxonomies for service categories and entity naming conventions between TPRM, contracting, and accounts payable systems. Interfaces between these systems help ensure that the inventory of third parties is comprehensive and up-to-date.
- Issues, complaints, and incidents repositories to track third party related items.

Appendix

Select qualifications.

PwC offers a range of services across the third party risk management life cycle tailored to clients' needs.

Sample services

Program diagnostic	We perform a high-level assessment of your firm's current TPRM function against leading practices, identifying gaps and potential needs.
Transformational roadmap	We perform an in-depth analysis, collaborating with key stakeholders to develop a new TPRM program design that fits your business and risk management goals. We also build a roadmap that identifies the key steps, anticipated level of effort, costs, and timing for getting there.
TPRM office implementation	We assist in both building and implementing a new TPRM office, including the operating model, governance and structure, policies and procedures, processes and controls, and reporting framework.
Technology enablement	We help firms assess their TPRM technology needs and identify business and technical requirements. We also support firms during the vendor selection and implementation phases, and help integrate processes into new or existing technology platforms.
Third party stratification	We help firms build a thorough inventory of their third parties and the services they provide. This includes assessing risk, determining a risk score for outsourced third parties and services, and developing a strategy to respond to that risk.
Third party assessments	Using our global network of firms and service delivery centers, we assist with on-site or remote assessment of third parties and their risk and control environments. We also help develop self-assessments for use by third parties.
Third party monitoring	Using our global network of firms and service delivery centers, we assist with on-site and remote monitoring activities (for example, data mining and analytics, monitoring external sources, and performing data aggregation and exception reporting) to support each of the three lines of defense within an organization.
Program management office (PMO)	We provide TPRM program support to firms interested in outsourcing or co-sourcing their programs. This includes, but is not limited to, project planning, execution, and reporting.

Appendix—selected qualifications

Project and client	Issues	Approach	Benefits
Integration of a new TPRM approach— Global financial services provider	This global financial services firm needed to upgrade its third party risk management program after a regulatory review identified numerous areas requiring attention. The firm also needed to better integrate its standalone TPRM program with the rest of its operational risk management infrastructure, including the information security, business continuity, legal, and contracting functions.	PwC helped the client assess its existing TPRM program and identify and design several enhancements, including: • Third party service stratification and risk ranking. • Questionnaires, standards, and training. • Issues capture, monitoring, escalation, and exception tracking tools and processes. • Service level agreements for third parties working with particular business lines. • Reporting metrics and key risk indicators, management, and oversight processes. PwC helped the client to better link the TPRM program with other operational risk assessment functions, including business continuity, information security, legal, and contracting.	The client benefited from the engagement in several respects. These benefits included: • A substantial reduction in the time and effort needed to manage a much smaller number of significant third party relationships, which decreased from more than 35,000 to less than 500. • A more thorough understanding of its third parties. • An improved methodology for identifying and monitoring high-risk third parties and services.
Creation of a third party compliance program to augment existing TPRM programs— Global financial services firm	In response to increased regulatory requirements, the client, a global financial services firm, established new standards for compliance management of third party service providers. The client needed help with: • Comparing the program with those of other large, complex banking organizations. • Implementing the newly developed process and procedures. • Developing a staffing model for managing the program. • Estimating costs for supplemental staff to perform the compliance function's third party, on-site visits.	PwC worked with the client to meet the newly established compliance standards. We helped develop appropriate guidance and procedures, and enhance existing tools to: • Identify relevant regulations based on the products or services provided by third parties. • Assess and document the third party's control environment. • Determine the appropriate nature and frequency of ongoing monitoring activities. In addition, PwC helped the client develop a staffing model by reviewing roles and responsibilities and helping to align them with standard industry practices. Finally, PwC collaborated with the client to develop a model for estimating costs for third party, on-site visits.	The client benefited from the engagement in several respects: These benefits included: • A more thorough understanding of the compliance and control environment at third party service providers. • More efficient and thorough compliance monitoring of third parties with potential cost reduction. • Improved compliance staffing model consistent with industry leading practices.

www.pwc.com/fsi

To have a deeper conversation, please contact:

Richard Altham	richard.d.altham@us.pwc.com +1 617 530 7188
TR Kane	t.kane@us.pwc.com +1 216 875 3038
Jeff Trent	jeff.s.trent@us.pwc.com + 1 646 471 7343
Darin Wettengel	darin.wettengel@us.pwc.com +1 704 350 7923
Andy Toner	andrew.toner@us.pwc.com +1 646 471 8327
Jason Chan	jason.chan@us.pwc.com +1 214 754 5142
Garit Gemeinhardt	garit.gemeinhardt.@us.pwc.com +1 704 344 7757
Dean Spitzer	dean.v.spitzer@us.pwc.com +1 646 313 3606

About our Financial Services practice

PwC's people come together with one purpose: to build trust in society and solve important problems.

PwC serves multinational financial institutions across banking and capital markets, insurance, asset management, hedge funds, private equity, payments, and financial technology. As a result, PwC has the extensive experience needed to advise on the portfolio of business issues that affect the industry, and we apply that knowledge to our clients' individual circumstances. We help address business issues from client impact to product design, and from go-to-market strategy to human capital, across all dimensions of the organization.

PwC US helps organizations and individuals create the value they're looking for. We're a member of the PwC network of firms in 157 countries with more than 184,000 people. We're committed to delivering quality in assurance, tax, and advisory services.

Gain customized access to our insights by downloading our thought leadership app: PwC's 365™ Advancing business thinking every day.

Follow us on Twitter @PwC_US_FinSrvcs

A publication of PwC's Financial Services Institute

Marie Carr
Principal

Cathryn Marsh
Director

Emily Dunn
Senior Manager

Kristen Grigorescu
Senior Manager

"Significant others: How financial firms can manage third party risks," PwC FS Viewpoint, May 2015. www.pwc.com/fsi.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.