KPMG

Ten ways to optimize your TPRM program

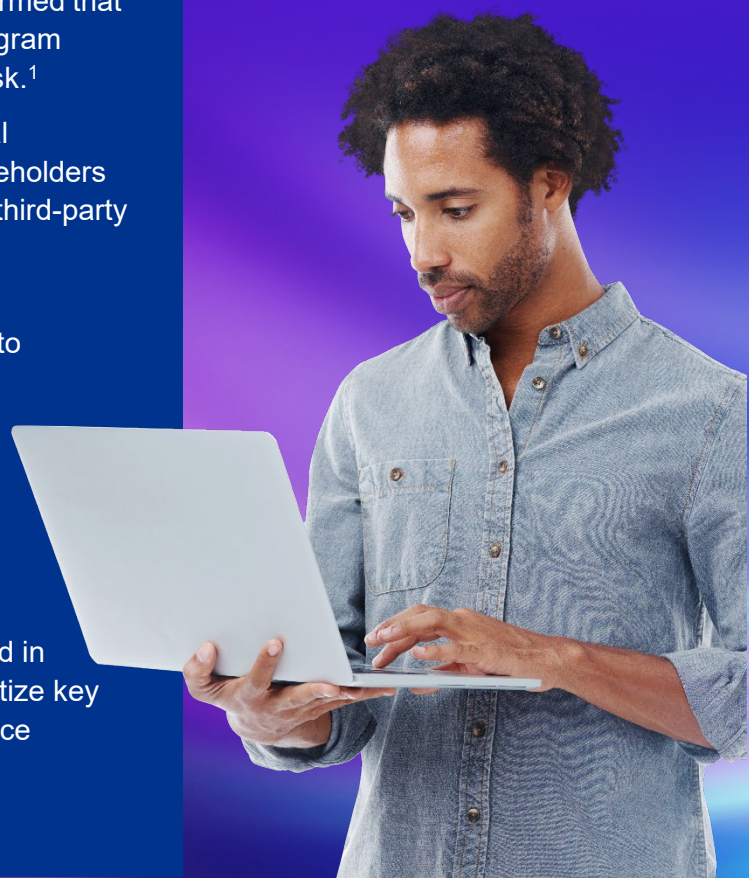
Foreword

In an increasingly interconnected global business environment, firms are becoming more reliant on third parties for critical operations, processes, and functions. Although these relationships can provide significant benefits, they also pose potential risks, ranging from ensuring compliance with regulations to addressing cybersecurity and data protection risks.

Management of risks associated with third-party relationships is a top priority for management and regulatory agendas. A survey conducted by KPMG found that 73 percent of respondents confirmed that inefficiencies in their TPRM program exposed them to reputational risk.[1]

The complexity of organizational structures and the multiple stakeholders involved in the management of third-party risk remains key challenges to management teams.

Based on our work as advisers to the financial services industry, we have seen large firms optimize their efforts around third-party risk management (TPRM) while improving their responses to emerging risks. This document aims to share best practices we have observed in adjusting firm programs to prioritize key risks and relationships to enhance operational resilience.



[1]KPMG International, “Third-Party Risk Management Outlook 2022” (January 2022).

01

Employ a risk-based approach

Adopting a risk-based approach is paramount to driving efficiency across the TPRM lifecycle. This approach involves focusing efforts on third parties that pose the highest risk to the firm, based on factors such as data access, service criticality, operational resiliency, and regulatory impact. For instance, third parties with access to sensitive customer data should be prioritized for more frequent and detailed reviews to mitigate risks.

Ask:

- Are we effectively prioritizing our third-party portfolio based on risk assessments?
- What processes do we have in place for conducting due diligence on third parties before engaging them, and how do we tailor these processes based on the risk profile of each third party?
- Is our population of services sufficiently stratified to allow us to focus on higher-risk services?
- Do we have consistent terminology used across our firm for third-party relationships?
- Do we utilize ongoing monitoring to create layers of oversight?
- Are our process and assessments up to date on our third-party risk assessments?

KPMG

02

Centralize oversight and governance

To respond to an increasingly complex risk environment, firms should utilize a multidisciplinary approach to TPRM by adopting a hub-and-spoke model. The TPRM function would function as a hub with a central leadership team responsible for setting policies, standards, reporting, and risk appetite of its operation. This central hub would be supported by subject matter experts (“spokes”) from relevant risk domains, such as privacy, cyber, business continuity, disaster recovery, etc., to provide insights and execution.

This approach not only facilitates comprehensive identification and mitigation of risks but also provides opportunity to set up a lines of defense model within the hubs and spokes and enable independent oversight of the function, thus ensuring consistency in risk management and compliance practices while enabling flexibility to address specific business needs.

Ask:

- Have we established a clear governance structure that balances centralized policy oversight with the agility of decentralized risk management execution?
- Do we have clear roles and responsibilities across the firm?
- Do we report third-party risks to appropriate forums?
- Are individuals reviewing third-party risks knowledgeable or require training?
- Do we include all stakeholders in the centralized TPRM function?
- Does our TPRM function benefit from multidisciplinary subject matter expertise across different functional areas?

KPMG

03

Leverage technology and automation

Adopting specialized TPRM software can profoundly enhance the efficiency of routine operations, such as risk assessments and due diligence, and streamline monitoring activities. This strategic move allows for the smarter allocation of precious human resources toward more-critical functions such as analysis and decision-making. For example, leveraging AI-driven analytics enables the real-time and continuous evaluation of a third party's financial health and cybersecurity practices, thereby elevating the effectiveness of risk management.

Moreover, by utilizing advanced monitoring technologies that integrate artificial intelligence, firms can detect patterns indicative of potential noncompliance with US financial regulations more proactively. This enhances the capability to address concerns before they escalate. A practical application includes employing voice-to-text technology for the automated analysis of communication, ensuring adherence to compliance standards. Additionally, the use of AI for the review or summarization of control reports, or policy examination for crucial components, further optimizes resource utilization, making the TPRM process more efficient and proactive.

Ask:

- How effectively does our technology enhance and optimize TPRM processes?
- Do we possess a coherent technology strategy that aligns with both the overarching TPRM program and the specific needs of individual risks and business units?
- What processes do we have in place for the continuous monitoring and auditing of third-party compliance, and how can we leverage automation to improve resource efficiency for routine tasks?

KPMG

04

Leverage adaptive contractual requirements

Embed compliance obligations within contracts and ensure they are adaptive compliance clauses that automatically update to reflect changes in US financial regulation, ensuring continuous compliance without manual contract revisions. For example, a financial services firm could include a clause in its third-party contracts stating that the vendor must comply with all current and future regulations related to data protection and privacy, as applicable under federal and state laws.

This clause could specify that in the event of new regulations or amendments to existing laws (such as updates to the California Consumer Privacy Act, CCPA, or introduction of new federal data protection laws), the contract obligates the third party to adjust its operations and data handling procedures accordingly, without the need for contract renegotiation. This approach ensures that third-party services remain in compliance with the evolving regulatory landscape, reducing the administrative burden on the financial firm and maintaining a focus on compliance agility and resilience.

Ask:

- Are compliance obligations and expectations clearly defined and embedded within our contracts with third parties?
- Do these contracts include clauses for adaptive requirements, audit rights, incident reporting, and compliance breach consequences?

05

Develop strong ongoing monitoring

To ensure that third-party risk is accurately measured and mitigated, firms need to perform ongoing monitoring of third-party risk profiles and contract performance. Risks assessments should be conducted during the contracting phase and refreshed on a regular basis according to the third-party risk score. As the business environment changes, the third party's management structure and internal controls could expose firms to increased risk and liability. To integrate third-party compliance into their own compliance programs, firms should request third-party compliance reports such as SOC 1 and SOC 2 reports. Utilizing automated external data feeds for third-party financials and negative news can also assist with this process by driving efficiency and assessing the risk associated with a third party beyond the services they are providing.

Failure to deliver services by the third party could also have a massive negative impact on a firm, particularly if the third party is supporting a critical business function, so monitoring vendor performance of the contract is also required. The overarching goal of ongoing risk and performance monitoring is to create a view of key metrics across all third-party relationships to effectively enable TPRM framework assessment and reporting to leadership and regulators.

Ask:

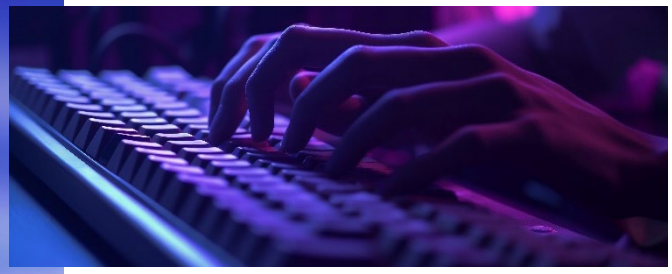
- What processes do we have in place for the continuous monitoring and auditing of third-party compliance, and how can we leverage automation to improve resource efficiency for routine tasks?
- Are we leveraging real-time data to its fullest potential to monitor third parties?
- Do our contracts define audit rights to allow us to assess third parties?
- What safeguards are in place in the contract to ensure third parties meet their obligations?

KPMG

06

Create an incident management framework

Establish clear protocols for incident reporting, ensuring third parties know how and when to report security breaches or compliance lapses. The protocols should tie incidents based on their impact on the firm, and the risk rating of the third party. Additionally, roles and responsibilities should be outlined regarding remediation and escalations using a RACI model (responsible, accountable, consulted, informed). Within the TPRM framework, firms should outline drivers of additional actions by the third parties. Incidents and the remediation that occurred should also be well documented to ensure resolution. Incident management and proper documentation are especially impactful for compliance breaches affecting financial and data privacy regulations to ensure swift and coordinated remediation efforts.



Ask:

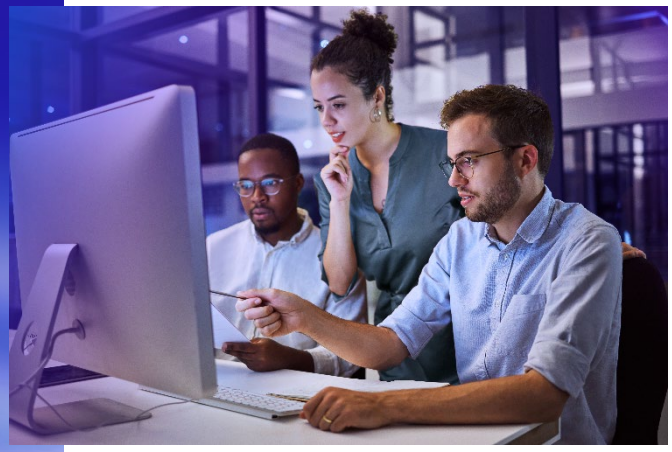
- Do relationship owners appropriately escalate issues with third-party performance?
- Do we have an appropriate plan in place for key third parties and/or services that have high-priority regulatory requirements associated with them?
- Do we have a system in place to swiftly direct and manage reports of incidents/breaches?
- How do we report on risk-related events connected to services delivered by third parties?

KPMG

07

Create a reporting framework

Through establishing ongoing monitoring and incident reporting within the TPRM framework, firms can easily outline a clear reporting framework for third-party relationships. Creating this framework also enables analysis of the effectiveness of the overall TPRM framework through the metrics measured during ongoing monitoring. For example, reporting on the number of incidents associated with a particular third party or step in a firm's TPRM lifecycle can illustrate the effectiveness of current practices or outline areas for improvement, either to the process or the mitigating controls.



Ask:

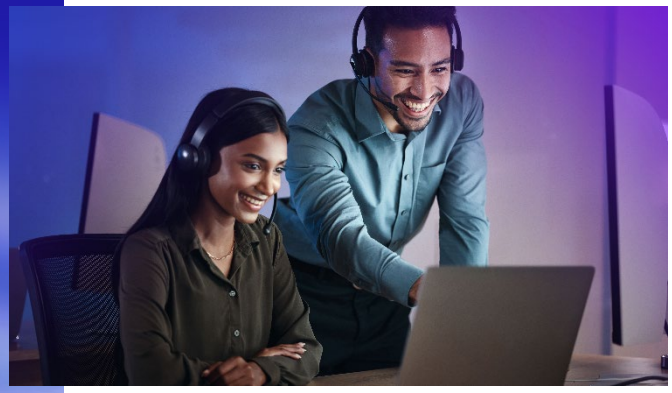
- What metrics and key performance indicators (KPIs) do we use to measure the effectiveness of third-party compliance management?
- What contractual notification requirements do we have (e.g., all breaches must be reported within 24 hours)?
- How do these metrics inform our continuous improvement efforts?
- Are our reporting channels clearly communicated to third parties?

KPMG

08

Provide continuous education and training

Provide ongoing education and training for TPRM staff and stakeholders across the firm on emerging risks, regulatory changes, and best practices in TPRM. However, as firms have increasingly relied on third parties for key business functions, it is prudent to extend that training to them as well. For example, we have seen several clients set up regular key supplier days where topics such as new cybersecurity threats and regulatory compliance updates are discussed. A mortgage servicing firm, for instance, might provide training on the Fair Credit Reporting Act (FCRA) and the Real Estate Settlement Procedures Act (RESPA) to its service providers.



Ask:

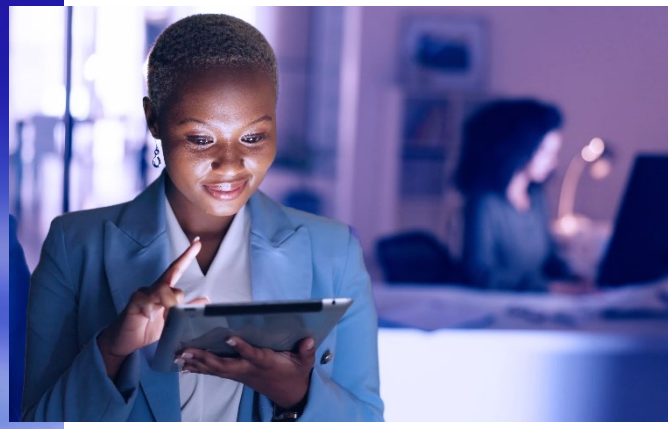
- Are we keeping our team and relevant stakeholders informed and equipped to manage third-party risks effectively?
- What ongoing support and resources do we provide to facilitate third party's compliance?

KPMG

09

Dynamic framework

Firms should map the types of data accessed by third party based on applicable regulations and establish horizon scanning to quickly identify and mitigate emerging risks and changes to the regulatory environment. By developing risk assessments with horizon scanning in mind, firms can quickly incorporate these new rules and risks into their existing frameworks without upending their entire TPRM function. Given the rapidly changing threat landscape, it is more critical than ever to recognize and focus on the ever-evolving risks from AI and potential cybersecurity threats, including data breaches, particularly for cloud service providers.



Ask:

- How do we ensure that the services provided by third parties align with our compliance requirements, including adherence to specific regulatory standards relevant to our industry (e.g., PCI DSS, GDPR, and CCPA)?
- How do we determine applicability of laws, rules, and regulations to a particular service to allow us to tailor due diligence?
- As a global organization with multiple regulators and requirements, are we considering how to most efficiently comply with these rules and regulations?

10

Be proactive

Develop a strategic approach to managing key vendor relationships, including regular performance reviews, alignment of business objectives, and collaborative risk management efforts. For example, through regular touchpoints with strategic third parties, we have seen the enhanced practices they are putting in place as a result of servicing their customers being shared with the firm to drive better outcomes.

Ask:

- Are we actively engaging with our key vendors to manage risks and drive performance improvements collaboratively?
- Do we have a clear point of contact over the entire relationship with strategic/critical third parties?

KPMG

Final thoughts from a KPMG leader

Greg Matthews, Partner, Financial Services Compliance says:

We have seen many clients refine their TPRM program since the updated OCC guidance in 2013. One critical lesson has stood out for me: the importance of proactive communication and collaboration with your third-party vendors.

Initially, the industry focused heavily on compliance monitoring and audits to verify that the service provided was done in accordance with the contract and relevant laws, which are undoubtedly crucial. However, I have seen that building strong relationships based on transparency and mutual understanding between firms and their third parties significantly enhances compliance outcomes.

By engaging your third parties in regular discussions about regulatory changes and compliance expectations, our clients not only improved their compliance results but also fostered a culture of shared responsibility for risk management. This approach has led to more effective identification of potential compliance issues before they escalate, saving them significant resources and reinforcing their commitment to maintaining the highest standards of compliance.

Greg Matthews
FS Risk, Regulatory and Compliance
KPMG US

Contact

Greg Matthews

Partner
FS Risk, Regulatory and Compliance Services
KPMG US

T: +1 212 954 7784
E: gmatthews1@kpmg.com

Special thanks to Daniel McManus, Grace Bowden, Jamie Lau, and Jack Shickell for their supporting contributions to this article.

Discover more KPMG risk insights:
visit.kpmg.us/RiskInsights

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.