Third Party Risk Management ("TPRM") Transformation

September 20, 2017

Internal use only
An introduction to TPRM

What is a Third Party relationship?
A Third Party relationship is any business arrangement between one organization and another, by contract or otherwise.

What is TPRM?
Although an organization may re-assign a service to a Third Party, it cannot outsource the associated responsibility for managing the risks and regulatory requirements. Additionally, the act of integrating a Third Party to your organization may create additional risks (e.g., country risk, concentration risk, etc.).

TPRM is the process of identifying, monitoring, and managing Third Party risks.
Use of a Third Party requires the following risks to be managed

Why is there an increased focus on TPRM?
Greater use of third parties by business and increased velocity of risk events due to use of the internet requires clarity of roles and responsibilities in the management of Third Party risks.

Isn’t TPRM Procurement’s job?
Procurement may be an integral stakeholder in TPRM but responsibility for initial and ongoing risk management must be shared throughout an organization. This way, risks are monitored by individuals with the proper expertise.

What are the challenges?
An effective and sustainable TPRM program requires a clear operating model and an integrated approach. This requires coordination across the three lines of defense and clear ownership and accountability at each step.
KPMG’s TPRM Framework to manage Third Party risk

To address risk management needs and regulatory requirements, institutions should develop a risk-based program and incorporate a complimentary suite of preventative and detective controls across the three lines of defense.

KPMG’s TPRM framework assists institutions with the design and implementation of such a program. KPMG customizes an institution’s TPRM program based on the institution’s portfolio of Third Parties and works across functions (e.g., Risk Management, Procurement, and Accounts Payable (“AP”)) to tailor the controls to the needs of a particular function and business.
Key Focus Areas for Internal Audit

- TPRM Governance and Program Design
- Operating effectiveness of TPRM Program including
  - Integration with Procurement
  - Exceptions, Escalations
- Information Security
Internal Audit Challenges

- IA Resources and Skills
- Issue Management of Third Party Related Issues
- Design vs. operating effectiveness
- TPRM Governance
- TPRM Audit Planning
- Internal Affiliates
- Vendor specific audits
- Risk Stratification
- Credible Challenge

Design vs. operating effectiveness
Stages of TPRM transformation

The path to an effective and sustainable TPRM operating model matures along a continuum of three stages:

**Comply**: The organization is reactionary, addressing risk management needs in response to regulatory changes, findings, and risk events.

**Integrate**: The TPRM framework matures and the organization develops disciplined, coordinated risk assessment and monitoring practices across the enterprise.

**Automate**: An optimal mode, in which the organization achieves greater sustainability by leveraging advanced technology and data science to enhance management of risk at a lower cost to the organization.
TPRM - Signs of a lagging program

Getting the grit out of the gears...

What are some signs of a lagging program?

- Lack of a strategy for the business use and risk management of Third Parties
- Incomplete inventory of Third Parties (e.g., only medium or higher risk services) or improper risk segmentation
- Decentralized and redundant risk assessment processes (Compliance Risk Assessments, Risk Control Self Assessments, New Initiatives Assessment etc.), resulting in increased burden for business personnel and increased cost for the organization
- Insufficient coordination, resulting in overlapping and inconsistent processes as well as unclear roles and responsibilities
- Lack of an integrated platform and data across risk management domains (e.g., Info. Sec., BCM etc.) to enable oversight and conduct analysis

...means solving for simultaneous problems
Sound third party risk management is good business

There are many drivers for a holistic TPRM program. What ‘good’ looks like is depicted below including KPMG’s TPRM framework that was used to conduct the assessment

1. Heightened standards (OCC) and enhanced prudential standards (Fed)
   - Board risk reporting and oversight
   - 1st Line ownership of risk
   - 2nd Line credible challenge
   - Data aggregation and reporting

2. Operational risk and compliance risk assessments
   - Enhanced RCSA, KRI’s and Testing

3. Cyber-security preparedness, incident management and resilience
   - 3rd Party Cyber incident scenarios must be incorporated into BCP and Disaster Recovery plans to enhance response capabilities
   - Supplier assurance (third parties), including clear contractual requirements

4. Balanced but effective affiliate risk management
   - Why? OCC Definition of a “Third-Party Relationship” includes Affiliates

5. Increased examiner focus on Regulation W (23a and 23b) compliance programs

6. IRS (foreign tax authority) focus on transfer pricing

---

**TPRM**

- **Regulatory compliance**
  - Global guidance around the management of third parties and the risks they manage on behalf of the organization
  - Increased information security and data privacy requirements
  - Risk and compliance requirements
  - Increased consumer protection and cost of remediation

- **Performance**
  - Growth of top line revenue through strategic joint ventures and alliances
  - Management of bottom line costs by outsourcing core and non-core activities
  - Driving greater return on investments through increased margin and operating resiliency

- **Risk management**
  - Managing reputational impacts from failures by third parties to manage risk in accordance with client’s practices
  - Increasing the quantity and quality of risk management activities by leveraging third parties for skills and resources
  - Greater coordination amongst internal risk management parties
TPRM Transformation benefits

The following benefits may be achieved as a result of TPRM Transformation

**Benefits of a mature TPRM program**

- Clear understanding of which third parties you do business with.
- Services are ranked according to risk with critical services identified.
- Risk based approach to ongoing monitoring post contract.
- Clear roles and responsibilities across lines of defense and risk oversight functions.
- Alignment of TPRM policy and practices to procurement activities.
- Reduced redundancy of activities to assess third parties.
- Enhanced alignment of mitigation tactics with contractual language.
- Greater use of technology and automation to manage third parties.
- Greater consistency of practices across the organization with regards to treatment of third parties.
- Increased understanding of third party risk management activities and policy requirements across the relationship owners.
- Clearer understanding of the cost benefits analysis factoring in the true cost of oversight for services.
- Greater understanding of the dependencies your organization has on third parties and their subcontractors.
- Sustainable approach to Board reporting with comprehensive view of critical third parties, strategy, trends, and issues.
How KPMG can help clients along the TPRM Transformation path

<table>
<thead>
<tr>
<th>Key Attributes</th>
<th>Comply</th>
<th>Integrate</th>
<th>Automate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum requirements have been established for:</td>
<td>TPRM activities are incorporated into enterprise risk governance practices (e.g., RCSA and Compliance Risk Assessment)</td>
<td>Technology is leveraged to extract and catalogue SLAs and key contractual elements</td>
<td>Technology is leveraged to extract and catalogue SLAs and key contractual elements</td>
</tr>
<tr>
<td>- On-boarding and contracting</td>
<td>- Roles and responsibilities are clearly delineated across the lines of defense (including roles for Procurement and AP)</td>
<td>- Digital labor is integrated into Third Party oversight (e.g., monitoring and testing)</td>
<td>- Digital labor is integrated into Third Party oversight (e.g., monitoring and testing)</td>
</tr>
<tr>
<td>- Ongoing monitoring</td>
<td>- Technology is leveraged to improve cross-functional workflow (e.g., centralized issue and action items, test reporting)</td>
<td>- Reporting (e.g., KPIs, KRIs, and executive reporting) is automated</td>
<td>- Reporting (e.g., KPIs, KRIs, and executive reporting) is automated</td>
</tr>
<tr>
<td>- Off-boarding</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Roles and responsibilities are established across the lines of defense with some misalignment (e.g., 2nd line taking on 1st line duties)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use of Excel and SharePoint-based technology with manual processes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Benefits | | | |
| — Compliance with regulatory requirements | — Greater visibility into processes and non-compliance with the program | — Progress toward optimal resource usage, improving both effectiveness and sustainability while reducing program costs | |
| — Develop basic understanding of risk portfolio | — Increased sustainability and cost reduction | — | |
| — Focus shifts from “doing” to “analyzing” | | | |

| Key KPMG Services | | | |
| — Maturity assessment | — Target operating model enhancement and implementation | — Technology enablement | |
| — Regulatory enforcement action remediation | — Cost optimization (e.g., COE, leveraging Third Party tools and services) | — Contract compliance | |
| — Independent assurance (due diligence, testing) | — Third Party rationalization | — KPMG Spectrum - Contract Performance Manager | |
The KPMG advantage in TPRM Transformation

KPMG has an extensive network of client contacts, diverse network of subject matter professionals, and solutions to help clients mature their TPRM programs.

<table>
<thead>
<tr>
<th>Client network</th>
<th>Subject matter professionals</th>
<th>Execution enablers and technology solutions</th>
<th>Full service firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPMG has performed TPRM work for many Fortune 500 companies across industries such as financial services, telecommunications, consumer products, energy, and healthcare and life sciences. Through ongoing dialogue with our clients, KPMG has a current, multifaceted view of leading industry practices.</td>
<td>KPMG has leveraged past engagements to build a team of TPRM subject matter professionals that covers a variety of industries and risk domains. These professionals have extensive knowledge and expertise to help clients comply with regulations, innovate, and tailor TPRM solutions to their organizational needs.</td>
<td>KPMG has a portfolio of engagement enablers and technology solutions that can be deployed to help clients transform their programs in a manner that is both effective and sustainable.</td>
<td>KPMG offers cross-functional support to address needs that extend beyond TPRM. - GRC - Alliance Partners - Forensics - Contract Compliance - Spectrum - Procurement</td>
</tr>
</tbody>
</table>
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. NDPPS 654498

The KPMG name and logo are registered trademarks or trademarks of KPMG International.