Agenda

I. Introductions

II. Third Party Risk Management (TPRM) Fundamentals

III. Basics of Third Party Risk Management Program

IV. Ways to look at a TPRM program

V. Top third-party risks
Introductions
Matthew Hansen
Director

— Director in the Seattle office of KPMG LLP’s U.S. Forensic Advisory Services practice
— 16 years of experience at KPMG in the Minneapolis, São Paulo, and Seattle offices
— Focus on fraud, investigations, compliance, third party risk management, and related issues for companies in the PNW and elsewhere

Contact Information
Tel 206-913-4961
Cell 952-334-0784
mfhansen@kpmg.com
What is third-party risk management?

1. **A program to...**
   identify, assess and manage the various risks associated with the use of the organizations' third parties

2. **A third-party relationship can be defined as...**
   any business arrangement between one organization and another, by contract or otherwise. Includes use of material fourth party or subcontractors.

3. **TPRM involves...**
   assessing third-parties ability to manage risk throughout the lifecycle of the relationship, from initiation to termination, including reporting to management

4. **Risk based program requirements...**
   so that time and effort is focused on managing third parties that pose the greatest risks to the organization

5. **Clear roles and responsibilities across a three lines of defense model...**
   that help each component part of the organization understand their role in managing third parties so nothing slips through the cracks.
### Defining third parties

<table>
<thead>
<tr>
<th>Who? Internal</th>
<th>Examples of Third Parties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Affiliates</td>
<td>— Cloud Providers</td>
</tr>
<tr>
<td>— Shared services</td>
<td>— Payment processors</td>
</tr>
<tr>
<td>— Legal entities</td>
<td>— Document Storage</td>
</tr>
<tr>
<td></td>
<td>— Professional Services</td>
</tr>
<tr>
<td></td>
<td>— Agents of your business</td>
</tr>
<tr>
<td></td>
<td>— Fintechs</td>
</tr>
<tr>
<td></td>
<td>— Data and System Providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who? Internal</th>
<th>Examples of Third Parties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Affiliates</td>
<td>— Cloud Providers</td>
</tr>
<tr>
<td>— Shared services</td>
<td>— Payment processors</td>
</tr>
<tr>
<td>— Legal entities</td>
<td>— Document Storage</td>
</tr>
<tr>
<td></td>
<td>— Professional Services</td>
</tr>
<tr>
<td></td>
<td>— Agents of your business</td>
</tr>
<tr>
<td></td>
<td>— Fintechs</td>
</tr>
<tr>
<td></td>
<td>— Data and System Providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What?</th>
<th>Examples of Third Parties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Trade reporting</td>
<td>— Cloud Providers</td>
</tr>
<tr>
<td>— Call centers</td>
<td>— Payment processors</td>
</tr>
<tr>
<td>— Advertising</td>
<td>— Document Storage</td>
</tr>
<tr>
<td>— Printing statements</td>
<td>— Professional Services</td>
</tr>
<tr>
<td></td>
<td>— Agents of your business</td>
</tr>
<tr>
<td></td>
<td>— Fintechs</td>
</tr>
<tr>
<td></td>
<td>— Data and System Providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How?</th>
<th>Examples of Third Parties:</th>
</tr>
</thead>
<tbody>
<tr>
<td>— On-shore</td>
<td>— Cloud Providers</td>
</tr>
<tr>
<td>— Off-shore</td>
<td>— Payment processors</td>
</tr>
<tr>
<td>— Outsource</td>
<td>— Document Storage</td>
</tr>
<tr>
<td>— On-site</td>
<td>— Professional Services</td>
</tr>
<tr>
<td></td>
<td>— Agents of your business</td>
</tr>
<tr>
<td></td>
<td>— Fintechs</td>
</tr>
<tr>
<td></td>
<td>— Data and System Providers</td>
</tr>
</tbody>
</table>

### Third Parties vs. Outside Service Provider (OSPs) vs. Third Party Intermediaries (TPIs)

- **Third Parties** include:
  - Customers
  - Regulators

- **Outside Service Providers (OSPs)** include:
  - On-shore
  - Off-shore
  - Outsource
  - On-site

- **Third Party Intermediaries (TPIs)** include:
  - Cloud Providers
  - Payment processors
  - Document Storage
  - Professional Services
  - Agents of your business
  - Fintechs
  - Data and System Providers
Potential areas of third-party risks

### Regulatory/Compliance Risk
- Regulatory requirements
- Theft/Crime/Dispute Risk
- Fraud, Anti-bribery and Corruption/Sanctions
- Compliance with internal procedures and standards
- ESG requirements

### Strategic Risk
- Service delivery risk
- Expansion/roll-out risk
- Mergers and acquisitions
- Alignment to outsourcing strategy
- Intellectual property risk

### Subcontractor Risk
- Applicable across all risk areas

### Concentration Risk
- Supplier concentration across critical services
- Industry concentration (incl. subcontractor)
- Concentration of critical skills (i.e., tech support)
- Geographic concentration
- Reverse concentration

### Technology/Cyber Risk
- Information security
- Cyber security
- Data privacy/data protection

### Financial Viability
- Financial risk from lending to a third party
- Liquidity risk

### Operational/Supply Chain Risk
- Business continuity
- Disaster recovery
- Physical security
- Operational Resilience
- Performance management (incl. SLA’s)
- Model risk
- Human resources risks (conduct risk, etc.)

### Country Risk
- Geopolitical risk
- Climate sustainability

### Reputational Risk
- Negative news
- Lawsuits (past and pending)
- Brand of the third party
- Key principals/owners of the third party
- Workplace safety

### Legal Risk
- Jurisdiction of law
- Terms and conditions of the contract
You can outsource the process, not the responsibility
Basics of Third Party Risk Management ("TPRM")
# TPRM building blocks

## Business drivers
- Regulatory Compliance
- Manage Risks
- Global Operations
- Operational Efficiencies
- Innovation

## Risk domains
- Regulatory/Compliance Risk
- Subcontractor Risk
- Technology/Cyber Risk
- Financial Viability
- Reputational Risk
- Strategic Risk
- Concentration Risk
- Country Risk
- Operational/Supply Chain Risk
- Legal Risk

## Lifecycle phases
- Planning and third party identification
- Risk assessment and due diligence
- Contract management
- Ongoing monitoring
- Off-boarding

## Foundations of a TPRM program
- Policies and procedures
- Organization, people, skills, and training
- Governance and program effectiveness
- Data and reporting processes
- Enabling technology
Elements of a TPRM program (continued)

1. Identification
2. Risk Assessment
3. Due Diligence
4. Risk Acceptance
5. Contract Management
6. Ongoing Performance Evaluation
7. Ongoing Third Party Portfolio Visibility
8. Risk Evaluation & Mitigation
9. Off-boarding
Elements of a TPRM program (continued)

**Identification**
- Data & Analytics
- POs, Invoices, Payments, etc.
- Business systems
- Intake channels (e.g., business request)

**Risk Assessment**
- Onboarding:
  - Collecting baseline data & documents
  - Assessing services
- Risk Assessment:
  - Weighted per risk tolerance
  - Attribute screening
  - Risk Ranking

**Due Diligence**
- Depth based on Risk
- Low end: Desktop review
- High end: Boots on the ground
  - Enhanced Due Diligence
- Reconsider Risk Rating
- Accept and on-board
- Request further due diligence
- Remediation, monitoring, enhanced controls
- Terminate/decline
- Escalated approval
Elements of a TPRM program (continued)

**Contract Management**
- Mandatory conditions (e.g., training, certifications)
- Contract conditions (e.g., audit clause, ethics language)
- Escalated contract approval
- Length of agreement and renewal terms

**Ongoing Performance Evaluation**
- Risk-based periodic review
- Performance review
- Event-driven review
- Third Party profile changes
- Adverse reputational events

**Risk Evaluation & Mitigation**
- Refreshed diligence and profiling
- Macroeconomic and geopolitical triggers
- Results of compliance review/audit
- Legal/sanctions flags
- Risk limitations

**Ongoing Third Party Portfolio Visibility**
- Portfolio analytics
- Geopolitical risk
- Act. vs planned spend
- Competitive bidding
- Balancing
- Vendor rationalization & consolidation
Elements of a TPRM program (continued)

**Off-boarding**

- Disentanglement
- Notification of other parties
- Financial obligations
- Possession of assets, IP, technology
- Access control
- Data destruction
- Replacement
Ways to look at a TPRM Program
## Frameworks and lenses

<table>
<thead>
<tr>
<th>Committee of Sponsoring Organizations (“COSO”)</th>
<th>2013 Integrated Internal Control Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Risk Management</td>
<td>Enterprise Risk Management Frameworks + Programs</td>
</tr>
<tr>
<td>Industry/Trade Standards and Frameworks</td>
<td>Industry standards (i.e., NIST, COBIT, SIG, etc.) and leading practices Consortia to build industry consensus to streamline/standardize TPRM</td>
</tr>
</tbody>
</table>
The value of TPRM for organizations

**Reputation Protection**
- Protect the organization’s reputation through identifying reputational risks, potential for cyber breaches, or other risk events

**Transparency**
- Provide insight and transparency to risks that individual business lines may not have access to (including concentration risk)

**Customer Trust**
- Preserve customer trust through safeguarding data and minimizing service disruptions

**Product Development and Innovation**
- Enable product development and business model innovation, without sacrificing intellectual property or exposing the organization to unidentified risks

**Coordination**
- Coordinate between the business, risk groups, Compliance, Procurement, and Internal Audit for risk assessment, due diligence, onsite visits, and right to audit

**Cost Identification**
- Identify the total cost of outsourcing functions to ensure the business understands compliance or oversight costs that may be required

**Business Partnership**
- Partner with business across the TPRM lifecycle, from third party identification through termination of the relationship

**Maintenance of TP Inventory**
- Own and maintain the comprehensive TP inventory
Key messages from 2020 KPMG Global TPRM Survey

1. TPRM is a strategic priority
2. Companies are inconsistent in their approach to TPRM
3. A risk-based approach is the number 1 ‘get right’ for TPRM programs
4. Data and technology are improving TPRM teams’ performance
5. It’s time to sustainably scale the program
6. An effective TPRM framework is built on 4 pillars: governance, process, infrastructure and data
Top Third Party Risks
Top third-party risks

Insufficient diligence in new relationships
— Multiple frameworks, and the US Department of Justice, stipulate that companies should perform due diligence on third parties, and that diligence must be risk based
— Companies manage risk and reduce likelihood of regulatory action by making third party due diligence insightful, procedural, thorough, and predictable

Viewing risk in silos vs. integrating risks
— Integrating, standardizing, and centralizing third party risk management is hard
  — Companies often grow through acquisition - incompatible systems
  — Integration and tools can be potentially expensive
  — Geographical dispersion and diversity of operating units/businesses
— Separating functions results in a decentralized, siloed approach seldom improves risk mitigation
— Governing and defining third party risk is most efficient and effective when risk management functions are integrated for a more robust impact
Top third-party risks (continued)

Absence of ongoing risk monitoring

— If don’t’ monitor risk, you must react – neither **Compliance** nor a **Program**, and you lose the ability to take control of dangerous situations and/or minimize damage
— Initial diligence & onboarding provide false security as relationships and risks change
— Everyday non-compliance by well-intentioned and qualified third parties should also be monitored, can arise after onboarding, and are usually invisible from 30k feet

Insufficient safeguards for third parties

— Effective internal information security practices may be inadequate for managing third party risk – their security issues are your security issues
— Lax posture towards third party data security, making blanket decisions rather than thoughtful determinations

A “paper program” may not keep you safe

— Well-designed and documented program is not enough without adequate execution
— A TPRM solution might have the right features but still be ineffective
— Accessing “below the surface” data and evaluating execution can be challenging in initial diligence, but will yield better returns in the long run
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.