Third Party Risk

DRAFT – For Discussion Purposes Only

March 27, 2019
Agenda

I. Introductions

II. Third parties and risk

III. Basics of Third Party Risk Management (“TPRM”)

IV. Frameworks to look at a TPRM program

V. Select third-party risks

VI. Summary
Introductions
Matthew Hansen
Director

— Director in the Seattle office of KPMG LLP’s U.S. Forensic Advisory Services practice
— 14 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
Third parties and risk
What are third parties?

Third Parties
— Broadest, most inclusive term
— Parties not controlled by either the company (First Party) or its customers (Second Party)
— Third parties are effectively the external parties with which a company interacts

Third-party Outside Service Provider (“OSP”)
— Definition generally derived from COSO 2013
— Performs functions not central to the company’s core operational purpose

Third party intermediaries (“TPIs”)
— Third Party Intermediaries are described by the OECD as “a conduit for goods or services offered by a supplier to a consumer”
— TPIs include business partners, distributors, agents, consultants, vendors, dealers, customers, logistics providers, and others
Examples of Third Party Intermediaries

— Regulatory consultants
— Product registration agents
— Health and safety consultants
— Purchasing agents
— Lobbyists
— Promotional

— Travel and events vendors
— Customs agents
— Freight forwarders
— Shippers
— Wholesalers

— Joint venture partners
— Acquisitions targets
— Sales agents
— Brokers
— Distributors
— Resellers
A view of the risk universe

- Financial
- Reputational
- Compliance
- Regulatory
- Operational
Potential Risk Drivers

- Contract Management and Compliance
- Supplier Risk and Supply Chain Risk
- Anti-bribery and Corruption
- Anti-money Laundering and Sanctions
- Regulatory Risks
- Financial/operational risks
- Trade compliance
- Mergers and Acquisitions
- Technology and Cyber Risks
Some big picture questions

Data and privacy
— Who has our employees’ data?
— Our customers’ data?
— Who has our IP and trade secrets?
— What are they doing with it?
— How are they securing it?

Geographical / geopolitical
— Who is doing business where?
— Who is doing business with whom?
— Are they obeying local and US laws?
— Are they complying with international requirements?

Brand / reputation / labor laws
— Who is using our logo and/or represents us?
— Who could be considered our employees?
— Slave labor, forced labor, human rights abuses, etc.
— Labor or environmental practices that, while legal, are undesirable for US companies

Financial risks
— What happens if they fail to deliver or go out of business?
— Are they overcharging us?
— Are they defrauding us?
— Are they honoring obligations to pay for work/products we receive?
— Are they creating liability or fines we may have to deal with?
— Financial statement accuracy
You can outsource the process, not the responsibility
Basics of Third Party Risk Management ("TPRM")
Elements of a TPRM program

Identification/On-boarding

— Should we start doing business with these Third Parties?
— What types of risks might this Third Party present?

Ongoing Relationship Management

— Are we getting what was agreed upon?
— How are we managing risk?
— Should we continue the relationship?

Offboarding

— How do we extricate ourselves from the relationship?

Whether your third parties are customers, vendors, or other service providers, they all have the same life cycle as they work through your organization.
Elements of a TPRM program (continued)

1. Identification
2. Risk Assessment
3. Due Diligence
4. Risk Acceptance
5. Contract Management
6. Risk Evaluation & Mitigation
7. Ongoing Performance Evaluation
8. Off-boarding
9. Ongoing Third Party Portfolio Visibility
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

Risk Acceptance
- 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
Frameworks to look at a TPRM program
Frameworks and lenses

Committee of Sponsoring Organizations (“COSO”) - 2013 Integrated Internal Control Framework

United States Sentencing Commission - Federal Sentencing Guidelines

COSO
Five components of the COSO framework
Major Themes

Role of Third Parties – Who and Why
— Cannot be risk free and isolated - third parties are a necessity and risk management is an expectation
— Companies need controls around the TPRM cycle
— Extension of control environment and expectations to third parties and beyond

Connectivity to the business
— Opportunity to re-evaluate third party relationships as the business evolves
— Synergies with proactive procurement and vendor management
— No employee, group, or third party, should be seen as “untouchable”

Program elements
— Right to audit clauses and compliance mechanisms must not be purely ceremonial
— Anonymous complaint hotlines are essentially mandatory
— Communication of “Tone at the Top” and company expectations
— Third Parties are a common attack vector for Cyber Security and Data Access/Privacy
— Design of a program and controls is not enough
Federal corporate sentencing guidelines
Section §8B2.1. of the Federal Sentencing Guidelines Manual lays out seven considerations for sentencing of individuals and organizations, by which the effectiveness of an Ethics & Compliance program can be judged.

— **Standards and Procedures** to prevent and detect criminal activity. Typically accomplished through an organization’s Code of Conduct.

— **Oversight** from high levels within an organization including company leaders.

— **Education and Training** to facilitate understanding of the company’s Code of Conduct and expectations.

— **Auditing and Monitoring** of Ethics and Compliance program systems.

— **Reporting** mechanisms to allow employees and/or other stakeholders to make the organization aware of issues

— **Enforcement and Discipline** for individuals or groups who do not abide by the organization’s expectations, enforced consistently.

— **Response and Prevention** related to offenses.
Foreign Corrupt Practices Act and SEC/DOJ guidance
High-level overview of the FCPA and other laws

— A company and those acting on a company’s behalf may not offer, pay, promise to pay, or authorize the payment of, any money, gift, promise, or anything else of value to a foreign official in order to obtain or retain business, to direct business to a person, or to otherwise secure an improper advantage.

FCPA Accounting Provisions [15 U.S.C. § 78m(b)]
— “Books and Records” Provision
  - Companies must maintain books and records in reasonable detail and accurately reflect all transactions.
— “Internal Controls” Provision
  - Companies must devise and maintain a system of internal accounting controls.
— Applies to Public Issuers only, however the requirements are leading practices.

Other Anti-Bribery and Corruption Statutes
— Many countries, including the UK, Canada, and Brazil, have anti-corruption laws.

Third Party Relationships and Activities constitute the majority of US enforcement actions!
2012 and 2017 US SEC/DOJ Guidance

2012 Guidance reiterates the express prohibition on corrupt payments through third parties or intermediaries, recommends an *effective compliance program, including due diligence* of any prospective foreign agents.

**Covers common red flags associated with third parties**
- Excessive commissions or discounts to third-party agents, consultants, or distributors
- Third parties in a different line of business than the intended services, or with vague/unspecific agreements
- Related or closely associated with, or included at the request of, a foreign official
- Third parties are offshore/shell companies, or request payment to offshore accounts

**Risk-Based Due Diligence: business rationale and identity of the third party, and relation to monitoring**

**The 2017 DOJ Evaluation Guidance section on Third Party Management contains four areas:**
- Risk-Based and Integrated Processes
- Appropriate Controls
- Management of Relationships
- Real Actions and Consequences
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 you choose not to monitor risk, your only strategy is to react when risks arise – this is neither Compliance nor a Program, and you lose the ability to take control of dangerous situations and/or minimize damage
— Initial diligence and onboarding alone provide a false sense of security as relationships and risk factors change
— Cyber and FCPA issues are well publicized, but less egregious 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 prove inadequate for managing third party risk – today’s marketplace is digitized, and 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

— A well-designed, well-documented program may not be enough without an adequate system of execution
— A TPRM solution might have all the right features and still be a “paper program” – program elements not effective
— Accessing “below the surface” data and evaluating execution can be challenging in initial diligence, but will yield better returns in the long run
In summary
In summary…

— A risk-based TPRM program protects the organization, and helps ensure that the third party network stands as an ongoing benefit to the organization, not an imminent danger

— Third party risk management is a critical part of an effective ethics and compliance program, which many standards (DOJ, Federal Sentencing Guidelines, COSO, etc.) describe as having key elements in common

— A TPRM solution can change the game for your organization, but must be accompanied by integration, design, execution, and investment in changing the way a company does business – no silver bullets

— A TPRM program, and the necessary Compliance and operational discipline that go into making the program effective, can likely save a company money, and avoid downstream difficulties and damage

— You can always “start by starting” - if your universe is huge and has grown with no governance, do vendor segmentation and do SOMETHING for the highest risk groups - risk may be a driver of vendor rationalization

— You can outsource a process but you cannot outsource responsibility
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.