Compliance perspectives on third-party risk

DRAFT – For Discussion Purposes Only

November 16, 2018

Agenda

I. Introductions

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

III. Third parties and risk

IV. TPRM and effective ethics and compliance programs

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

Basics of Third Party Risk Management ("TPRM")

Third Party Risk Management

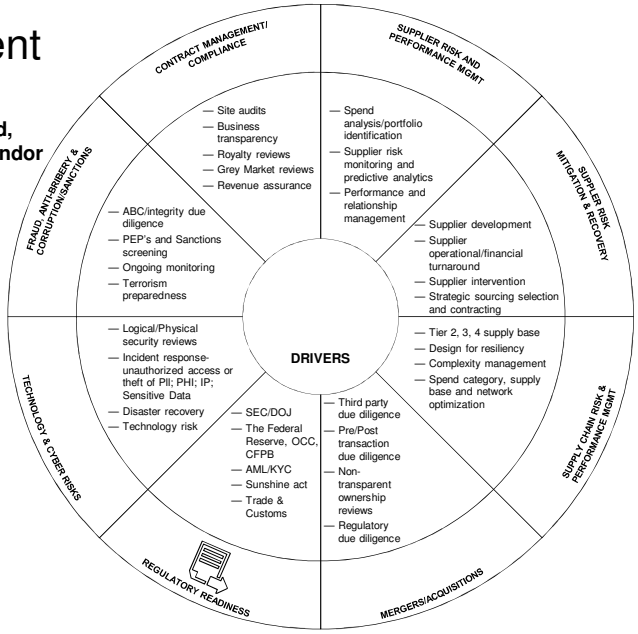
Effective Third Party Risk Management is a coordinated, cross-functional effort and requires integration with Vendor Management, Procurement, and other business units

Lifecycle Phases:

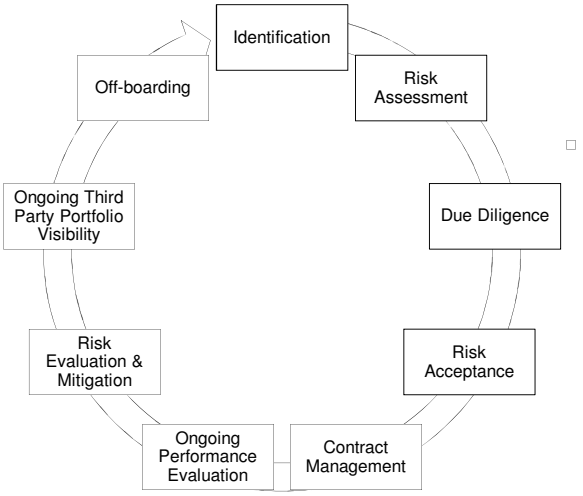
— Identification/Onboarding
— Ongoing Relationship Management
— Offboarding

Critical elements:

- Strategy
- Governance
- Policies and procedures
- TPRM Process
- Governance
- Information Reporting & Technology



Elements of a TPRM program



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

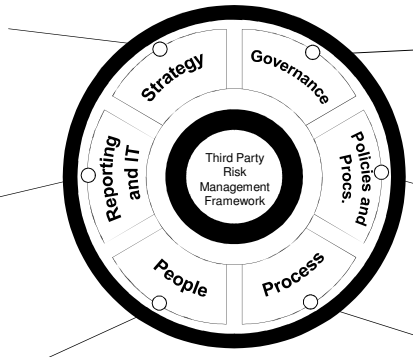
- Disentanglement
- Notification of other parties
- Financial obligations
- Possession of assets, IP, technology
- Access control
- Data destruction
- Replacement

Areas of a TPRM Program

Strategy
—Mission and objectives
—Align third party use to risk appetite
—Management of operating expenditures
—Where in life cycle is first contact

Information Reporting and Technology
—Dashboards/reports
—Key risk indicators (KRIs)
—Key performance indicators (KPIs)
—Process automation

People
—Roles and responsibilities
—Skills and training
—Performance management and Compensation



Governance
—Oversight committees (i.e., Board, Enterprise Risk Management, Operations Risk)
—Tone and culture
—Group involvement (Procurement, Compliance)

Policies and Procedures
—Standard setting
—Policy management

TPRM Process
—Planning
—Risk assessment, due diligence and selection
—Contracting
—Monitoring and Testing
—Renewals
—Off-boarding

Third parties and risk

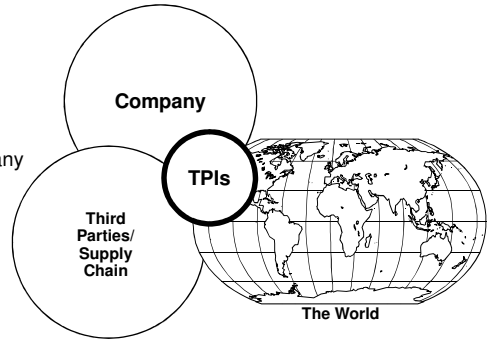
What are third parties?

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 – Suppliers, Vendors, Licensees, BPOs, Agents, etc.



Third-party Outside Service Provider ("OSP")

— Definition generally derived from COSO 2013

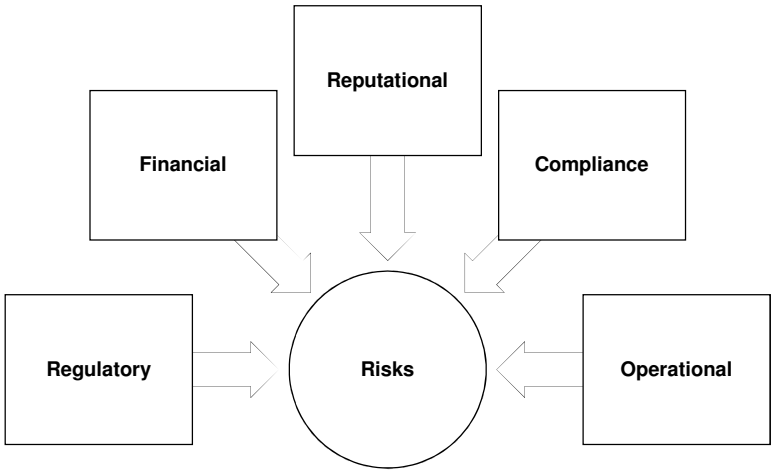
— Performs functions not central to the company's core operational purpose

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

A view of the risk universe



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

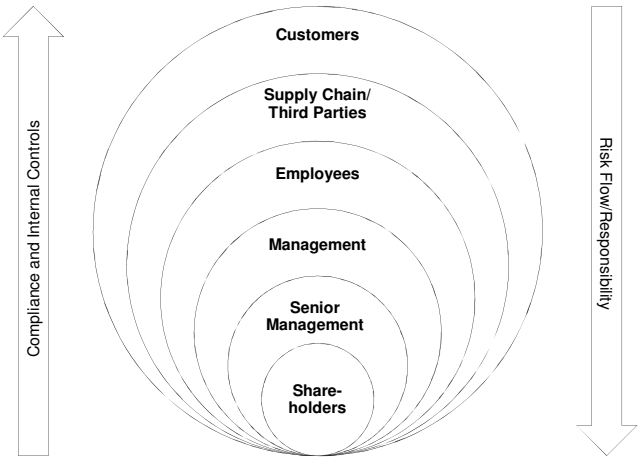
Brand / reputation / labor laws

— 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



Compliance and Third Party Risk

Goal of Third Party Risk Management ("TPRM"): Protect the company from risk exposure, harm, loss, damage, etc. by managing third party relationships more effectively

How can Compliance help?

Help identify, mitigate, and avoid risk by:				
Providing checks and balances against the business	Auditing and monitoring of the process	Auditing and monitoring of the suppliers	Providing a regulatory perspective	Providing a risk and risk mitigation perspective

TPRM and effective compliance programs

Frameworks and lenses

Committee of Sponsoring Organizations ("COSO")	2013 Integrated Internal Control Framework
United States Sentencing Commission	Federal Sentencing Guidelines
US SEC/DOJ	Foreign Corrupt Practices Act FCPA Resource Guide Evaluation of Corporate Compliance Programs (Evaluation Guide)

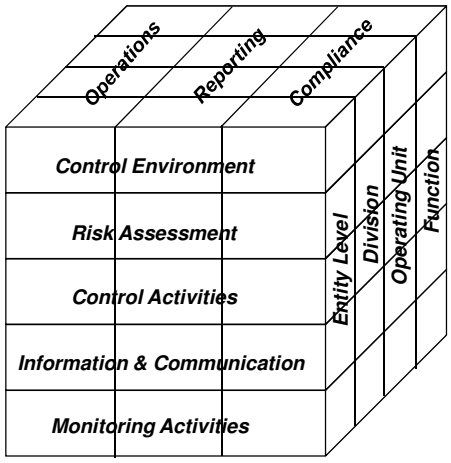
Effective compliance program strategies

Effective compliance program strategies can help companies and personnel tasked with managing risks of fraud, waste, and abuse by focusing efforts on:

- **Identifying and understanding potential risk areas**
- **Evaluating design and operational effectiveness of compliance controls**
- **Leveraging insights and awareness to increase effectiveness of existing compliance activities**
- **Applying risk focused approaches to maximize value of investments**
- **Setting tone for ethical behavior and achieving high levels of integrity**

COSO

Five components of the COSO framework



Control environment

Control Environment

— Commitment to integrity and ethical values
— Independent board with oversight of internal controls
— Established structures, reporting lines, and authority/responsibility
— Commitment to attract, develop, and retain talent
— Accountability for internal control responsibilities

Risk Assessment

— Identification and assessment of risks relating to business's objectives
— Identify risks to the achievement of objectives and analyze risks to determine how to manage
— Consider the potential for fraud in assessing risks
— Identify and assess changes that could significantly impact internal controls

Control Activities

— Control activities that contribute to the mitigation of risks
— General control activities over technology
— Deploy controls through policies that establish what is expected and procedures that put policies into action

Information and Communication

— Obtain and generate relevant information to support the functioning of internal controls
— Internally communicates information, including objectives and responsibilities
— Externally communicates regarding matters affecting the functioning of internal control

Monitoring Activities

— Evaluate if internal controls are present and functioning
— Evaluate and communicate internal control deficiencies
— Take corrective action, including senior management and the board of directors

Major Themes

Role of Third Parties – Who and Why

— Most companies cannot have a perfect, isolated business – third parties are a necessity
— Risk management is an expectation – you must know who they're doing business with and how they're doing it
— Companies need controls around the TPRM cycle: identification, selection, engagement, and monitoring
— Extension of control environment and expectations to third parties and beyond - Contractually, Operationally, from a Compliance perspective, and otherwise

Connectivity to the business

— A TPRM program can also provide the opportunity to re-evaluate third party relationships in the face of changing risk levels with the third party, or changing risk tolerance or business objectives with the company
— Effective TPRM has synergies with proactive procurement and vendor management – many similar monitoring mechanisms and data efforts
— No employee or group within an organization, or third party, should be seen as "untouchable" – when a company is too beholden to a third party, its ability to execute its control mandates and manage risk is lost

Major Themes (continued)

Program elements

— Right to audit clauses and compliance mechanisms are nice to have, but if never utilized they do not mean much

— Anonymous complaint hotlines, accessible to employees, vendors, and customers, are essentially a mandatory compliance and internal control mechanism – and must be taken seriously

— Communication of “Tone at the Top” and company expectations starts internally - often times the business is charged with executing control elements which is not normally their mandate

— Communicating expectations and providing accessible documentation to third parties is necessary

— Third Parties present tremendous Cyber Security and Data Access/Privacy risk and are a common attack vector – strong technology controls are a fact of life

— Design of a program and controls is not enough - companies must evaluate and test controls, including monitoring, post-mortems and feedback loops when issues are identified

Federal corporate sentencing guidelines

Federal 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

FCPA Anti-Bribery Provision [15 U.S.C. § 78dd-1 et seq.]

— 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)]

— Relevant to Public Issuers only, however the requirements are leading practices

— *"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***

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 US SEC/DOJ FCPA guide

Reiterates that the FCPA expressly prohibits corrupt payments made through third parties or intermediaries

Guidance recommends that companies reduce FCPA risk with 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

— Vague or unspecific third party agreements

— Third parties seemingly in a different line of business than the intended services

— 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

Specifies that third party Due Diligence should be risk-based

— Qualifications, reputation, and business rationale for using a third party

— Relationships with government officials

— Third party relationships should be monitored on an ongoing basis

Point of view on compliance programs

The 2012 Guidance asks three basic questions

— "Is the company's compliance program well designed?"
— "Is it being applied in good faith?"
— "Does it work?"

The 2012 Guidance provides the "Hallmarks of Effective Compliance Programs"

— Commitment from Senior Management and a Clearly Policy Against Corruption
— Code of Conduct and Compliance Policies and Procedures
— Oversight, Autonomy, and Resources
— Risk Assessment
— Training and Continuing Advice
— Incentives and Disciplinary Measures
— ***Third-Party Due Diligence and Payments***
— Confidential Reporting and Internal Investigation
— Continuous Improvement: Periodic Testing and Review
— Mergers and Acquisitions: Pre-Acquisition Due Diligence and Post-Acquisition Integration

Point of view on compliance programs (continued)

In 2017, the Fraud Section of the US Department of Justice published its Evaluation of Corporate Compliance Programs ("Evaluation Guidance")

— Analysis and Remediation of Underlying Misconduct
— Senior and Middle Management
— Autonomy and Resources
— Policies and Procedures (Design and Accessibility; Operational Integration)
— Risk Assessment
— Training and Communications
— Confidential Reporting and Investigation
— Incentives and Disciplinary Measures
— Continuous Improvement, Periodic Testing and Review
— ***Third Party Management***
— Mergers and Acquisitions

Point of view on compliance programs (continued)

The Evaluation Guidance section on Third Party Management contains four areas

— Risk-Based and Integrated Processes
  - Whether the TPRM process corresponds to the company's risk levels
  - How the company has integrated TPRM into procurement and vendor management

— Appropriate Controls
  - Business rationale for using the third parties
  - Mechanisms for ensuring the contract terms are accurate, services provided, and payment terms and compensation are reasonable and appropriate

— Management of Relationships
  - How the company considered the third party's "incentive model" compared to compliance risks, and whether compliance and ethical behavior was incentivized
  - How the third party was monitored
  - Did the relationship managers understood the compliance risks and how to manage

— Real Actions and Consequences
  - Were red flags identified in Due Diligence? How were they resolved
  - Have other similar third parties been suspended, terminated, or audited
  - How has the company monitored termination and blacklisting

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 compliance program, which many standards (DOJ, Federal Sentencing Guidelines, COSO, etc.) describe as having key elements in common

A TPRM platform/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

If your third party universe is huge and has grown with no governance, you can still start by starting – do some vendor segmentation and get started on the highest risk groups - risk may be a driver a 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.

kpmg.com/socialmedia