Identifying and Mitigating Third Party Risk
Conducting Risk-Based Anti-Corruption, Anti-bribery Due Diligence

Jennafer B. Watson
Chief Compliance Officer
Layne Christensen

Diana M. Lutz, Chief Ethics and Compliance Officer, Steele
dlutz@wwsteele.com
+1 (415) 354-3851

Topics for Discussion

• Introductions and overview of third party risk
• Launching a risk review for third party risk
• Identifying and tracking third parties
• Analyzing data and setting risk mitigation strategy
• Risk rating examples
• Extending program initiatives and controls to third parties
• Setting priorities and taking steps
Who are Third Parties?

- Third Party Types:
  - Suppliers, Vendors
  - Distributors, resellers
  - Consultants - Expertise in: Legal, Accounting, Strategic Business, Local and Regional Issues, etc.
  - Industry Experts, Advisory Services
  - Contractors, Temporary Services
  - Agents, Sales Representative, Marketing Intermediaries
  - Companies who service your products
  - Joint Venture Partners

Reliance on Third Parties

- Companies doing international business engage suppliers, contract employees, distributors, consultants, agents, lobbyists, etc.
- Businesses are increasingly entering new and emerging markets and expanding the global reach of their products and services.
- “Outsourcing” work has increased in popularity, allowing companies to access and leverage the global workforce.
- Use of third parties includes relying on local companies to sell and service products, contracting for specialized and local products, services and expertise.
- Seeking faster growth and a greater impact in new and emerging markets.
Third Parties - What’s the risk?

From a practical perspective, the risk comes from:
- Doing business with people your employees don’t know (increasingly doing business strictly electronically).
- Working with geographically remote third parties with little management oversight or true accountability.
- Third party companies and individuals working in different cultures with varying rules and expectations.
- Unless you tell them... and can audit and enforce, third parties don’t know your company rules and don’t have to comply with them.
- Third parties under pressure to perform quickly and win deals for you.

Initial Considerations

- Vetting is essential part of an overall robust and “reasonable” anti-corruption, anti-bribery compliance program.
- Companies need a consistent, rational, implementable third-party due diligence program.
- Challenges in implementation can cause companies to get stuck before any decisions are made on implementation.
- When faced with implementation challenges, some companies may instead implement by settling for a haphazard approach to determining which intermediaries need to be vetted and what level of diligence will apply.
- Companies need to evolve a specific and systematic methodology to calculate risk among third-party intermediaries.
Initial Considerations

• Companies need to know the real-time status of their third party intermediaries.
• For a successful compliance project and process that will offer the desired level of risk mitigation...
  – who you investigate and how much due diligence you conduct is as important as how you conduct your due diligence.
• Disreputable entities are masters of reinvention. As with other compliance initiatives, quality counts. The quality of your process and each investigation is paramount.
• Ensuring that those conducting due diligence are familiar with local laws and practices allows you to reassure your third parties about participating in your due diligence process.

Due Diligence Program Challenges

• Companies face numerous challenges in executing a systemic approach to due diligence.
• Three Common Trouble Spots in Implementing Third Party Due Diligence Programs:
  1. Knowing which third parties to vet, with what priority and how to systemize the approach.
  2. Determining sufficient level of due diligence for each third party.
  3. Being overwhelmed with the volume of pre-existing third parties and potential new partners.
Identifying Your Third Parties

- Getting started with incomplete data?
  - Figure out what you do know about your third parties.
    - Conduct interviews / surveys with management to understand and map the types and locations of third parties, the nature of business interactions with and volume of business with third parties;
    - Gather contract types for review;
    - For additional narrowing of these initial efforts, focus on an already indentified high risk business unit or region;
  - Work on data and contract aggregation for existing third parties; and
  - Create a go-forward process to manage third party engagement, renewal and approvals.

Working with a High Volume of Individual Third Parties

- Using a risk based approach to assign due diligence by category of third parties, can help manage high volume issues.
  - Each third party is assigned to a category (third party type) and systematically assigned a level of due diligence based on that category and the completed risk inventory.
  - Risk scores for individual within a category can be raised or lowered depending on additional risk factors.
  - Highest risks receive deepest due diligence.
  - Prioritize resources to align with highest risks.
  - Additional prioritization possible using broad risk assessment approach based on profile of business unit, products, geography, etc.
  - Can also be implemented using a risk based pilot approach.
Additional Factors Affecting Third Party Risk

When reviewing third parties and their relationship and business interactions with your company cover the following areas of interest.

High Risk
- Sales to foreign governments or State Owned Enterprises (SOEs)
- Makes contacts with government / foreign officials or SOEs
- Authorized to act on behalf of COMPANY Close ties to COMPANY (for ex. use of logo, shared marketing)
- High level of mutual dependency(success or results depending on relationship)
- May receive cash incentives from COMPANY
- Refuses to agree to or include any compliance or anti-corruption language in contract
- Not a public company listed on a recognized exchange
- Operates in countries having a reputation for high risk of corruption (CPI)

Medium Risk
- Potential sales to foreign governments or SOEs
- Potential for other contacts with government / foreign officials or SOEs
- Close ties to COMPANY but no authorization to act on behalf of COMPANY
- High level of mutual dependency
- May receive cash incentives from COMPANY
- Public company listed on a recognized exchange
- May not agree to COMPANY’s standard form contracts containing anti-corruption language
- Operates in countries having a reputation for low or moderate risk of corruption

Low Risk
- Major, public, multinationals expected to have robust ethics and compliance programs
- Low sales, no cash incentives from COMPANY,
- Low likelihood of sales to foreign govts or SOEs
- Sells other products lower mutual dependency
- Incorporates COMPANY’s products into other products or uses COMPANY brand name
- Operates in countries having a reputation for little to no risk of corruption
After inventorying and categorizing your third parties, use existing data to define risk classification buckets or tiers and sort the third parties using identifiable characteristics (sample attributes below).

**HIGH**
- High Risk Country
- Big $ Contract
- Key Supplier
- Unusual Terms
- Govt Contact

**MED**
- Med Risk Country
- Low-Med $ Contract
- Closely Connected to Company

**LOW**
- Low Risk Country
- Publicly Traded
- No Govt Contact
- Low $ Contract

**Example Classification Using Risk Attributes**

**High**
- CPI ≤ 3.9
- GOVT CONTACT
- SALES > $1M
- SPEND > $100k

**Med**
- 4.0 ≤ CPI ≤ 5.9
- GOVT CONTACT
- $1M ≥ SALES ≥ $250K
- $25K ≤ SPEND < $100K

**Low**
- CPI ≥ 6.0
- NO GOVT CONTACT
- SALES < $250K
- SPEND < $25K
Sample Assignment of Risk Points in a Risk Rating System

### CPI Index

<table>
<thead>
<tr>
<th>CPI Index</th>
<th>CPI Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0-3.3</td>
<td>6 High</td>
</tr>
<tr>
<td>3.4-3.9</td>
<td>5 High</td>
</tr>
<tr>
<td>4.0-4.9</td>
<td>4 Med</td>
</tr>
<tr>
<td>5.0-5.9</td>
<td>3 Med</td>
</tr>
<tr>
<td>6.0-6.9</td>
<td>2 Low</td>
</tr>
<tr>
<td>7.0-10.0</td>
<td>1 Low</td>
</tr>
</tbody>
</table>

#### 2010 Sales (000) Risk Rating

<table>
<thead>
<tr>
<th>Sales / (000)</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>3 High</td>
</tr>
<tr>
<td>250-999</td>
<td>2 Med</td>
</tr>
<tr>
<td>1-249</td>
<td>1 Low</td>
</tr>
<tr>
<td>0</td>
<td>0 Low</td>
</tr>
</tbody>
</table>

#### Total Risk Risk Rating

- 9-12 High
- 5-8 Medium
- 1-4 Low

Government Contact Y = +3
Government Contact N = +0

---

Sample Risk Rating

<table>
<thead>
<tr>
<th>Company</th>
<th>Country</th>
<th>Pts</th>
<th>Sales / (000)</th>
<th>Pts</th>
<th>Gov’t Contact</th>
<th>Pts</th>
<th>Total Risk</th>
<th>DD (H,M,L)</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>Russia 2.1</td>
<td>6</td>
<td>3422</td>
<td>3</td>
<td>Y</td>
<td>3</td>
<td>12</td>
<td>H</td>
</tr>
<tr>
<td>Y</td>
<td>China 3.5</td>
<td></td>
<td>218</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Z</td>
<td>Azerbaijan 2.4</td>
<td></td>
<td>33</td>
<td></td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A</td>
<td>United States 7.1</td>
<td></td>
<td>16371</td>
<td></td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>India 3.3</td>
<td></td>
<td>5096</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>Uzbekistan 1.6</td>
<td></td>
<td>298</td>
<td></td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>Brazil 3.7</td>
<td></td>
<td>3121</td>
<td></td>
<td>Y</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consider: How many 3Ps get deepest level of due diligence? Who is doing the investigations? Who reviews the reports? Who “clears” the red flags? Are all those steps documented?
Why Not Conduct the Same Diligence on All?

- Why not just run all your third party types through the same level of due diligence?
- From a risk perspective, not all third parties are the same nor do they require the same level of scrutiny.
  - Each category of third party exposes their partners to varying types and levels of compliance risks.
- Obtaining detailed due diligence on an overly broad group will consume more resources than you likely have, and can cause delay or failure of your program.
- Doing point in time checks or relying on minimal, publicly available information means some risky third parties are not getting the level of scrutiny that is justified by the risk.

Quick Benchmarking

- Among the attendees how many prefer a risk based approach to due diligence?
- How is third party risk calculated?
  - By general attributes / bucket approach?
  - Should there be a specific risk calculation for each third party or can all similar third parties be treated the same?
- How often is risk recalculated?
- How often is due diligence conducted, one time, annually, biannually?

DISCUSSION AND COMMENTS
Risk-based Due Diligence: a Critical Component

- Sufficient, clear policies addressing company's high-risk areas for bribery.
- Clear position statement from management regarding bribery.
- Effective culture and reporting system for violations (hotline, who to go to).
- Strong policy against retaliation for reporting violations.
- Required swift investigation of reported or suspected violations.
- Effective training on bribery policies including web and live training.
- Employee certification of understanding and compliance.
- Education of board and top management on oversight responsibilities.
- Clear detailed gifts, entertainment, expense, contribution policies/processes.
- Regular audits of policies/processes for high risk groups & high risk location.
- Third-party risk assessment and programmatic due diligence effort.
- Strong policies and implementation of due diligence on third parties.
- Ongoing risk assessment, monitoring, adjustments.

Recap: Four Steps to Tailor the Level of Diligence to the Risk

1. Identify and classify third parties by categories.
2. Use data on services, revenue, contract, location, gov't contacts, etc.) to assess and create risk scores or other attribute based risk profile for each category.
3. Assign each third party category to a risk tier.
4. Assign an initial level of due diligence to each risk tier.
   - Consistent and systematic approach, well documented.
   - Especially helpful where your backlog or unchecked third parties may be in the hundreds or even thousands of entities.
   - Individual third parties can be afforded increased scrutiny as circumstances dictate and when red flags occur.
Indicators of Success

- Creating risk based approach – testing and receiving logical results (ie. looking at certain parties to ensure they fall into the tier where you’d expect to see them).
- Clearing your backlog in a reasonable amount of time.
- Designing a manageable, integrated go-forward process.
- Quickly executing on the process.
- Creating appropriate documentation.
- Analyzing red flags and eliminating or mitigating risky third parties.
- Business value imparted from process and from due diligence reports received.