Third-party due diligence

Key components of an effective, risk-based compliance program
The economic crisis, vigorous governmental enforcement activity and the increased focus on enterprise risk are causing global corporations and their audit committees to take a closer look at how they manage and conduct their due diligence around vendor, distributor, joint-venture and customer organizations - defined broadly as third parties. Those with existing due diligence programs are finding they have not kept up with the increased global risks of third-party vendors - particularly in the areas of anti-bribery and corruption - leaving many companies to wonder what constitutes a reasonable due diligence program and how much research and documentation are enough.

We have helped many companies deal with this issue and have assisted in building compliance programs that address known vendor corruption risk. In this paper, we share some of the leading practices for building an effective vendor due diligence program and suggest steps that companies should consider to improve their current processes and technologies to address the global regulatory environment.

While the discipline around supply chain and vendor management is relatively mature, third-party risk, from a regulatory management perspective, is in its infancy with little guidance available and no standards established. Perhaps this is because most third-party management programs were developed decades ago when the focus of the due diligence tasks were around “operational” and “financial” criteria and were typically only done once during the on-boarding process. Operational and financial criteria often included verifying that the third-party was in good corporate standing; reviewing audited financial statements to ensure financial stability; and perhaps calling upon a few references. Documentation rarely included due diligence activities related to adverse media searches, criminal history, government sanctions or queries to identify politically exposed individuals.

From a regulatory perspective, neither the US Department of Justice (DOJ) nor the Security and Exchange Commission (SEC) provide specific guidance on the components of an effective third-party due diligence program. However, the US Sentencing Commission voted unanimously on April 7, 2010, to modify the Federal Sentencing Guidelines for organizations, including the provisions that set forth the attributes of an effective compliance and ethics program. The guidelines provide some high-level components that should be integrated into your third-party due diligence and compliance programs. These components, which took effect November 1, 2010, suggest that management should:

1) Establish standards and procedures to prevent and detect criminal conduct.

2) Be knowledgeable about the content and operation of the program and exercise reasonable oversight with respect to the implementation and effectiveness of the compliance program.

3) Make reasonable efforts not to include within the substantial authority personnel of the organization any individual whom the organization knew, or should have known through the exercise of due diligence, or has engaged in illegal activities or other conduct inconsistent with an effective compliance and ethics program.

4) Take steps to communicate the program’s standards and procedures throughout the organization and provide training tailored for various audiences.

5) Take reasonable steps to ensure that the program is followed, including monitoring and auditing to detect criminal conduct, periodically evaluating the program’s effectiveness and publicizing a system that allows reporting potential and actual criminal conduct without fear of retaliation.

6) Consistently promote and enforce the program with appropriate incentives for proper performance and appropriate disciplinary measures for those who engage in criminal conduct or fail to take reasonable steps to prevent or detect it.

7) Take reasonable steps to respond appropriately to criminal conduct when detected and prevent further similar criminal conduct, including making any necessary changes to the program.

“Third-party due diligence must be robust, thorough, impeccably documented and preserved.”

– Former DOJ Fraud Section Deputy Chief Mark Mendelsohn (2005 - 2010), FCPA Conference November 2009
One may also look to the Organisation for Economic Co-operation and Development (OECD) for its February 18, 2010, adoption of “Good Practice Guidance on Internal Controls, Ethics and Compliance.” This Good Practice Guidance was adopted by the OECD Council as an integral part of the “Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions,” dated November 26, 2009.

The guidance provides for the following leading practices for ensuring effective internal controls, ethics and compliance programs or measures for the purpose of preventing and detecting foreign bribery. As it relates to third-party due diligence, the guidance includes the following points:

- Strong, explicit and visible support and commitment from senior management
- Ethics and compliance programs or measures designed to prevent and detect foreign bribery applicable, where appropriate and subject to contractual arrangements, to third parties such as agents and other intermediaries, consultants, representatives, distributors, contractors and suppliers, consortia and joint venture partners (hereinafter, “business partners”), including, among other things, the following essential elements:
  - Properly documented, risk-based due diligence pertaining to the hiring, as well as the appropriate and regular oversight of business partners
  - Informing business partners of the company’s commitment to abiding by laws on the prohibitions against foreign bribery, and of the company’s ethics and compliance program or measures for preventing and detecting such bribery
  - Seeking a reciprocal commitment from business partners
  - Effective measures for:
    - Providing guidance and advice to directors, officers, employees and, where appropriate, business partners on complying with the company’s ethics and compliance program or measures, including when they need urgent advice on difficult situations in foreign jurisdictions.
    - Internal and, where possible, confidential reporting by, and protection of, directors, officers, employees and, where appropriate, business partners not willing to violate professional standards or ethics under instructions or pressure from hierarchical superiors, as well as for directors, officers, employees and, where appropriate, business partners willing to report breaches of the law or professional standards or ethics occurring within the company, in good faith and on reasonable grounds.
    - Undertaking appropriate action in response to such reports.
    - Periodic reviews of the ethics and compliance programs or measures designed to evaluate and improve their effectiveness in preventing and detecting foreign bribery, taking into account relevant developments in the field, and evolving international and industry standards

Finally, the UK Bribery Act effective July 1, 2011, mentions due diligence as one of its six principles for anti-bribery compliance and stresses the importance that companies should focus their third-party due diligence resources using a “risk-based” approach. The Act creates four offenses, one of which is failing to prevent bribery, which covers the activities of any person or third-party acting on behalf of a business (for example, employees, agents or subsidiaries).

“... due diligence procedures should be proportionate to the identified risk. ‘Due diligence’ ... should be conducted using a risk-based approach”

– Bribery Act 2010 Guidance UK Ministry of Justice
Key components of an effective program

Taking the existing guidance into consideration, four key principles become apparent, which serve as a strong frame of reference for incorporating the multiple guidelines and legal rulings previously discussed into an effective global due diligence program. These guidelines are consistency, management oversight, objectivity and reasonableness.

Consistency — Automating the process and developing standard templates for vetting third parties, especially overseas, will help drive consistency across the company. A robust platform allows a company to effectively and efficiently manage a decentralized program. Your goal should be to have one system that everyone uses on a consistent basis.

Management oversight — It is important that management’s intent and actions provide for a robust third-party due diligence process. Is management doing the best they can based on their perceived risk and limited resources or are they choosing to look the other way?

Objectivity — Are the due diligence procedures objective and performed separately from the requestor, which could contain inherent conflicts of interest? Each due diligence investigation should be independently performed with its own case file, notifications, investigative findings, remediation actions, education and representations between the company and its agent, partner, distributor, third parties and others. Having a defined case management work flow integrating people, process and technology can be particularly useful to ensure an objective process.

Evaluating your program

Questions to ask

Consider your current anti-corruption vendor on-boarding process and ask tough questions about consistency, management oversight, objectivity and reasonableness.

Consistency. Is the process followed consistently? Can you audit or tie back vendor request forms to each vendor in the vendor master? Is there training around the process? Is it globally deployed? Is the process repeatable – i.e., would you arrive at the same conclusion if you were to run a selection of new vendor setup forms through the same process? Are the rules and contract language around FCPA and anti-corruption consistent from country to country?

Management oversight. When was the last global training program on anti-corruption, due diligence or compliance? When did you last update your new vendor setup form or procedures? Does your company use software tools for case management to manage and document the vendor setup process? What database and due diligence steps does accounts payable take to categorize new vendor submissions received from the requestor? Is the right person making the decision? Once accepted, is it rechecked annually or on an ongoing basis? During the escalation process, who is responsible for making the tough calls? How robust is the vendor “vetting report”? Does it incorporate public database checks, include the officers of a company and search for “politically exposed persons,” adverse media, country-specific sanctions and more? Who is made aware of a new vendor once approved – is it communicated to the corporate office and centrally managed, or is it handled and decided by the local office?

Objectivity. Given so many decision-makers at the country or subsidiary level, can the current process stand up to independence scrutiny from an outside (or DOJ) perspective? For example, can the accounts payable clerk processing the original new vendor setup form be forced to designate a form as “low risk” from the requestor in order to avoid additional scrutiny from upper management?

Reasonableness. Is the process reasonable? Does the process generate too much paperwork that may not get reviewed or too little paperwork where rogue third parties or necessary contract terms might be missed? Does the process incorporate leading practices, including the criteria set forth in the US Sentencing Guidelines and OECD?

“Put simply, the prospect of significant prison sentences for individuals should make clear to every corporate executive, every board member and every sales agent that we will hold you personally accountable for FCPA violations”

— Assistant Attorney General for Criminal Division Lanny Breuer, Feb. 2010
The supplier vetting activities

Filtering criteria example:

<table>
<thead>
<tr>
<th>Third Parties</th>
<th>Total Supplier Universe</th>
</tr>
</thead>
<tbody>
<tr>
<td>80,000</td>
<td></td>
</tr>
<tr>
<td>10,000</td>
<td>Develop Supplier Category and Geographic Filtering Criteria*</td>
</tr>
<tr>
<td>1,000</td>
<td>Develop Detailed Filtering Criteria on Supplier Relationship and Nature of Contract</td>
</tr>
<tr>
<td>250</td>
<td>Develop Supplier Vetting Protocols to Effectively Document Legal, Regulatory and Reputational Risks</td>
</tr>
<tr>
<td>150</td>
<td>Develop Decision Criteria for Acceptance, Denial or Specific Contract Modifications, Based on Risk Profile</td>
</tr>
</tbody>
</table>

*Geographic filtering will include Transparency International’s Global Corruption Perception’s Index, among other criteria.

Reasonableness – Given limited company resources, taking a risk-based, tiered approach to third-party due diligence helps management to allocate resources accordingly. Reasonableness addresses the question, “How much is enough?” In your efforts to avoid doing business with the wrong people, a prudent and well thought-out process is important. A thoughtful and reasonable compliance program that is risk based is the best preventive strategy for making sure that compliance is both practical and defensible.

Taking a risk-based approach

The four components described above are predicated on a critical first step: a credible, risk-based assessment of a company’s third parties. Many corporate compliance departments we observe conduct their due diligence programs based on deploying multiple levels of investigation based on the perceived or known risks. Many global corporations have vendor masters and third-party databases spanning in the tens of thousands, even the hundreds of thousands. Filtering them down to a management population is a critical first step before deciding which due diligence procedures to conduct as demonstrated by the diagram above.

As it relates to actually conducting regulatory related due diligence activities for those higher risk third parties, we see the process broken down into three general levels of investigation:

Level I: open source background checks

Level I analysis includes a comprehensive check of available sanctions and embargo and watch lists. It also includes internet and media search inquiries. These searches use open source databases and public information to search a wide range of business journals, websites, industry publications and mainstream media. When these processes are streamlined through the use of case management software, online databases and internet searching, a Level I analysis can be accomplished by an investigator in three to five hours; and given its streamlined, repeatable nature, it is ideal for centralization and perhaps even outsourcing.

Level II: enhanced due diligence

Based on the Level I analysis, Level II analysis involves additional public database searches with a specific focus on localized public records databases, such as court filings. A Level II analysis may also incorporate phone interviews, reference checks and research into potentially vulnerable corporate relationships with a deeper dive into public records and media searches. A Level II analysis often requires local country presence to gain access to local records and contacts and typically requires significantly more hours (between 20 to 40 hours) of local, in-country investigator time to research and report.

Level III: deep dive

As the risk level dictates, a Level III analysis may be further warranted. This may include on-site inspections; interviewing associates in political, business and social circles to uncover reputation; reviewing corporate, civil and criminal documents; and validating financial records.

Reasonableness — Given limited company resources, taking a risk-based, tiered approach to third-party due diligence helps management to allocate resources accordingly. Reasonableness addresses the question, “How much is enough?” In your efforts to avoid doing business with the wrong people, a prudent and well thought-out process is important. A thoughtful and reasonable compliance program that is risk based is the best preventive strategy for making sure that compliance is both practical and defensible.

Taking a risk-based approach

The four components described above are predicated on a critical first step: a credible, risk-based assessment of a company’s third parties. Many corporate compliance departments we observe conduct their due diligence programs based on deploying multiple levels of investigation based on the perceived or known risks. Many global corporations have vendor masters and third-party databases spanning in the tens of thousands, even the hundreds of thousands. Filtering them down to a management population is a critical first step before deciding which due diligence procedures to conduct as demonstrated by the diagram above.

As it relates to actually conducting regulatory related due diligence activities for those higher risk third parties, we see the process broken down into three general levels of investigation:

Level I: open source background checks

Level I analysis includes a comprehensive check of available sanctions and embargo and watch lists. It also includes internet and media search inquiries. These searches use open source databases and public information to search a wide range of business journals, websites, industry publications and mainstream media. When these processes are streamlined through the use of case management software, online databases and internet searching, a Level I analysis can be accomplished by an investigator in three to five hours; and given its streamlined, repeatable nature, it is ideal for centralization and perhaps even outsourcing.

Level II: enhanced due diligence

Based on the Level I analysis, Level II analysis involves additional public database searches with a specific focus on localized public records databases, such as court filings. A Level II analysis may also incorporate phone interviews, reference checks and research into potentially vulnerable corporate relationships with a deeper dive into public records and media searches. A Level II analysis often requires local country presence to gain access to local records and contacts and typically requires significantly more hours (between 20 to 40 hours) of local, in-country investigator time to research and report.

Level III: deep dive

As the risk level dictates, a Level III analysis may be further warranted. This may include on-site inspections; interviewing associates in political, business and social circles to uncover reputation; reviewing corporate, civil and criminal documents; and validating financial records.
Consistency — Management oversight — Objectivity — Reasonableness

**Process examples**

By incorporating the attributes of consistency, management oversight, objectivity and reasonableness, we have developed a third-party due diligence framework that seeks to provide adequate risk-based categorization, appropriate levels of data analysis, ongoing monitoring and effective communication.

The framework starts with the business unit, where adequate training and communication are essential. Business units interact with multiple parties, so the framework must be flexible to accommodate vendors, resellers, customers and acquisition targets. Through standardization and a risk-based set of questions, we have worked with companies to develop a standardized business risk assessment that categorizes each third-party into categories such as low, moderate, high or extreme risk groups.

Based on the risk assessment categorization, the analysis phase is represented by the integrated due diligence program as set forth in the next phase. Typically, the majority of third parties, regardless of the categorization, are run through a battery of Level I public database checks, as previously defined. This starts the case management file for each third-party where all decisions, tests and outputs are centralized and documented. While the rules to getting to an “approval” are always unique to the business, the key point of the analysis phase is to centralize and document the process. Depending on the business rules set, a third-party may be approved with “unrestricted business” (e.g., no issues), semi-approved with either specific contract language or other limiting conditions or denied entirely.

Company management plays a key role in decision-making; however, its burden is reduced as its decisions follow a predictable rules-based methodology in a documented, consistent format that reduces ambiguity and helps provide for more “fact-based” decision-making.

**Recommended next steps**

Here’s how you can get started on your own assessment.

- Develop categorization and decision rules as part of the data-gathering process
- Seek assistance from outside advisors and legal resources who are specialists in the areas of third-party due diligence and FCPA

**Conclusion**

Today’s global companies should evaluate their current third-party, anti-corruption due diligence programs in the context of a risk-based framework that incorporates attributes of consistency, management oversight, objectivity and reasonableness. The economic crisis, recent governmental enforcements and the increased focus on enterprise risk are causing global corporations and their audit committees to take a closer look at how they manage their vendor and customer compliance relations. While several corporations are still grappling with what processes represent an effective due diligence program, incorporating the attributes above can go a long way in demonstrating an effective, risk-based vetting program.
“We recognize the issues of costs to companies to implement robust compliance programs, to hire outside counsel to conduct in-depth internal investigations and to forego certain business opportunities that are tainted with corruption. Those costs are significant, and we are very aware of that fact. The cost of not being FCPA compliant, however, can be far higher.”

— Lanny Breuer, Assistant Attorney General, Nov. 17, 2009
About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global and of Ernst & Young Americas operating in the US.

About Ernst & Young’s Fraud Investigation & Dispute Services

Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to achieve your company’s potential. Better management of fraud risk and compliance exposure is a critical business priority — no matter the industry sector. With our more than 1,000 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It’s how Ernst & Young makes a difference.

© 2011 Ernst & Young LLP.
All Rights Reserved.

SCORE No. BB0000

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.