Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Getting a Grip on

Third-Party Entity Risk

An e-Book publication sponsored by NAVEX GLOBAL™ The Ethics and Compliance Experts

COMPLIANCE WEEK

Compliance Week, published by Wilmington Group plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resources for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

NAVEX GLOBAL™
The Ethics and Compliance Experts

NAVEX Global helps protect your people, reputation and bottom line through a comprehensive suite of ethics and compliance software, content and services. The trusted global expert for more than 8,000 clients in 200+ countries, our solutions are informed by the largest ethics and compliance community in the world. More information can be found at www.navexglobal.com.

Inside this e-Book:

Supply Chain Risk Assessments Require Digging Through Data

2014 compliance trends survey says 85 percent of respondents are re-assessing business links with third parties

By Joe Mont

Think you've got supply chain headaches? Consider the challenges facing George Henein, compliance officer for the United Nations' procurement division. The UN deals with more than 60,000 vendors across the world and strives to give them all some level of scrutiny.

The UN's mission of fostering economic development among member states also often leads to purchases of goods and services from far-flung locales in developing nations with, to put it politely, less-than-stellar devotion to compliance.

Then there is the intense scrutiny of critics and watchdogs. The UN is a media magnet and a political target that is under constant watch that makes taking a risk-based approach more difficult. "If we buy the wrong toilet paper, it will make Fox News within 30 seconds," Henein says. "Reputational risk is on everybody's radar, and we are the most audited and over-audited division."

Henein's core concerns are not unique. Even a small company can have a web of vendors and suppliers that spans the globe. So how can a chief compliance officer, rooted to headquarters, detect bad behavior at distant suppliers and reduce the company's exposure to supply-chain risk? Data that companies may already possess, or may easily obtain, can be a starting point for anticipating problems, not just reacting to them, supply-chain experts say.

> "There is more information nowadays, whether that is media or social media, that can be mined to effectively identify risks and isn't necessarily cost prohibitive."
>
> Tom Golding, Vice President, Thomson Reuters GRC

The 2014 Compliance Trends Report, a joint effort by Compliance Week and Deloitte, elaborates on third-party risk. According to the study, 85 percent of respondents said they are re-assessing their business links with joint-venture partners, suppliers, distributors, agents, and other third parties. Despite persistent concerns, however, the most common means of managing third-party risk is only to provide them with a copy of the code of conduct. More active forms of oversight are less common: Less than one-third of respondents said they perform extensive background checks on third parties, and another 17 percent said they hardly ever do.

Yet, third-party risks keep expanding. There is not only the persistent threat of bribery that can net an enforcement action under the Foreign Corrupt Practices Act; companies also face a growing number of causes championed by legislators, activists, and consumers, including the use of conflict minerals, environmental and sustainability issues, and human trafficking, to name a few.

Corruption Risks

For the UN, corruption risk is no academic debate, especially in countries where bribery is prevalent and accounting standards are minimal or ignored. "How can we expect even the smallest vendors to not only have financial records or statements, but to translate them from their language to ours?" Henein asks. "It makes it so hard to even do financial due diligence, let alone something extra."

In some countries, corruption is a fact of life. "We've had shipments stopped at the port for months at a time because the port officials are expecting a bribe. You are at a complete impasse," Henein explains. "What do you do? Do you pay the bribe, be completely non-compliant, and face the obvious risk of prosecution—and that same country can also prosecute you for accepting the bribe. Or, do you stick to your guns and say, 'No, we are going to do it by the book and by the rules,' but then you don't get your product."

It all takes on an added urgency when that shipment—often perishable food items—loses value each day it sits in limbo. "Where do you draw the line? Do you just do this one bribe under the table and let it go, or do you stick to the rules?" Henein asks.

The UN, he says, takes a zero-tolerance stance in such situations. It also conducts risk assessments prior to all new procurement deals, checking financial compliance with rules established by its General Assembly of member states. Every vendor is also asked to acknowledge the UN Global Compact—a "bill of rights" related to child labor, human trafficking, and other issues. Internal compliance reviews and specialized training is used to, as best possible, see that vendors are following the rules.

"Most of our due diligence with vendors, unfortunately, is financial in nature," Henein says. "We would actually like to get to the point where we are doing the full deep dive. We do compliance reviews, but in reality they are more reactive because we have to wait for the hotline call where somebody calls in and complains about a specific vendor."

Moving to a Proactive Approach

How should an organization identify such risks as conflict minerals, human trafficking, or environmental concerns and move from reactive to proactive? Risks vary by sector and need to be prioritized to best understand what training and enforcement should be ramped up, says Tom Golding, vice president of product and proposition for Thomson Reuters GRC. Due diligence can range from a rather simple scan of local media and social media mentions, looking for red flags, to conducting audits of those third parties. The real difficulty comes from the tangled web

of suppliers and sub-suppliers.

"People may agree that they don't want to do business with companies involved with human trafficking," Golding says. "But there are very real challenges. It is not just your first tier of supplier. It is their suppliers, and the suppliers behind that. You have this amplified effect of trying to manage data around a lot of entities."

Data, Data Everywhere

Parsing available data should be a hunt for both known and inferred risks. The former can rely on the aforementioned news reports and online posts, and it can encompass whistleblower complaints. "There is more information nowadays, whether that is media or social media, that can be mined to effectively identify risks and isn't necessarily cost prohibitive," Golding says. "If information is in the online domain, you want to know about it. You will be called to task if you haven't at least done those searches."

Relatively straightforward media mining often reveals neglected problems, says Michael Grady, an associate with the law firm Willkie Farr & Gallagher and a former assistant U.S. attorney. "To the extent you find out about a problem in the *Wall Street Journal*, you usually could have identified that issue through a hotline tip or audit result that wasn't followed up on, or an employee bringing up a question during training."

Inferred risk, predicting problem areas, will vary by sector and country. A venture in Malaysia may have a higher risk of human trafficking because the textile industry there is seasonal and needs to build a temporary workforce by any means necessary, Golding offers as an example.

"Usually there is some hint of a problem before it blows up," Grady says. "You want to consider a whole host of factors including the countries that you are doing business in and the particular risks in those countries. If everybody has a customs problem in Nigeria, that is easy to see coming around the bend. It is easy to predict if you are shipping containers from China into Nigeria that you are probably going to have a problem getting the documentation correct to get those through customs."

Close attention needs to be paid to permits and licenses, as they are often a source of corruption, Grady cautions. He also recommends using media reviews to flag potential issues. "If your competitor is brought up on charges of criminal activity in a certain country, chances are that you have that same problem, especially if you are using the same vendor and supplier," he says.

"If one of your vendors makes the news, you are probably going to make the news," Henein warns. Research by the UN makes it clear that any company can find itself under scrutiny for an issue like human trafficking. Human trafficking is relevant to 50 percent of companies globally, with 8 percent of company employees indicating they have dealt with human trafficking on a daily basis. Only 60 percent of surveyed companies, however, have policies to address the risk.

Information, mined and inferred, should be used to focus resources on the 5 to 10 percent of vendors where resources are warranted, rather than trying to tackle thousands of suppliers all at once, Golding says. He compares this process to the way an emergency room may triage patients.

Grady stresses the importance of viewing this data through the prism of FCPA guidance issued by the Department of Justice and the SEC. "We are supposed to be continuously re-evaluating, reassessing, and tailoring our compliance programs—not just to emerging risks, but to changes in business models and changes in our personnel," he says. ■

PRIORITIZING RISK

The following guidance on third-party risk assessment comes from a Resource Guide to the U.S. Foreign Corrupt Practices Act guidance issued by the Securities and Exchange Commission and Department of Justice.

Devoting a disproportionate amount of time policing modest entertainment and gift-giving instead of focusing on large government bids, questionable payments to third-party consultants, or excessive discounts to resellers and distributors may indicate that a company's compliance program is ineffective. A $50 million contract with a government agency in a high-risk country warrants greater scrutiny than modest and routine gifts and entertainment.

Similarly, performing identical due diligence on all third party agents, irrespective of risk factors, is often counterproductive, diverting attention and resources away from those third parties that pose the most significant risks. The DoJ and SEC will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program, even if that program does not prevent an infraction in a low risk area because greater attention and resources had been devoted to a higher risk area.

Conversely, a company that fails to prevent an FCPA violation on an economically significant, high-risk transaction because it failed to perform a level of due diligence commensurate with the size and risk of the transaction is likely to receive reduced credit based on the quality and effectiveness of its compliance program.

As a company's risk for FCPA violations increases, that business should consider increasing its compliance procedures, including due diligence and periodic internal audits. The degree of appropriate due diligence is fact-specific and should vary based on industry, country, size, and nature of the transaction, and the method and amount of third-party compensation. Factors to consider, for instance, include risks presented by: the country and industry sector, the business opportunity, potential business partners, level of involvement with governments, amount of government regulation and oversight, and exposure to customs and immigration in conducting business affairs. When assessing a company's compliance program, the DoJ and SEC take into account whether and to what degree a company analyzes and addresses the particular risks it faces.

Source: SEC.

Managing Third-Party Risk in Decentralized Companies

By Karen Kroll

In April, tech giant Hewlett-Packard announced a $108 million agreement with the Department of Justice to settle charges that it violated the Foreign Corrupt Practices Act.

The charges centered on the conduct of H-P affiliates in Russia, Poland, and Mexico, and they highlight a trend at the center of many recent FCPA cases: The bribes are often orchestrated by third-party organizations, including vendors, suppliers, and even shadow companies created to keep the bribes off the books of foreign subsidiaries.

H-P's Russian subsidiary, for example, admitted to bribing government officials to secure a large technology contract, and it used intermediaries to pay the bribes. H-P Russia executives created a slush fund, from which the bribes would come, via a "buy-back deal structure," the Justice Department said. The scheme worked like this: H-P sold computer and technology products to a Russian channel partner, then bought the same products back from an intermediary company at a markup, while also paying the intermediary additional money for purported services. H-P then sold the same products to an agency of the Russian government at the increased price. The payments that had been made to the intermediary then were transferred to government officials via a number of shell companies.

The H-P judgment is just the latest of many FCPA enforcement actions that involve companies' subsidiaries and use of third parties. According to EY's recent 12th Global Fraud Survey, some 90 percent of reported FCPA cases have involved third-party intermediaries.

> "Companies in general tend to underestimate the risk that third parties present."
>
> Kelvin Dickenson, Managing Director, D&B Global Compliance Services

Companies often rely on third parties to expand into new markets, says Traci Coughlan, principal of advisory services at compliance consulting firm the Red Flag Group. Indeed, more than three quarters of the companies participating in the 2012 FCPA Benchmarking Report by Kroll Advisory Services indicated that they partner with foreign entities to conduct business abroad.

At the same time, many companies appear unprepared to handle the risk posed by using third parties. Just 40 percent of respondents to a recent survey by Deloitte say they have a program to prevent and detect supply chain waste, fraud, or abuse. More than one-third of respondents say they monitor their third parties once a year, or less.

"Companies in general tend to underestimate the risk that third parties present," says Kelvin Dickenson, managing director at D&B Global Compliance Services.

The use of third parties creates a dilemma for many compliance professionals. "Compliance officers juggle two realities," says Donna Boehme, principal at compliance advisory firm Compliance Strategists. On the one hand, the business units create the risks need to own them, she says, as they are in the best position to understand and mitigate them. "The business is responsible for making the case to engage a third-party intermediary and perform necessary due diligence and ongoing monitoring of the agent relationship," Boehme says.

On the other, compliance has the expertise and the tools to conduct the necessary monitoring and may come with a more independent view. At the same time, compliance needs to create the framework and tools the business units use to manage third-party risk. It then needs to be able to guide the business units and monitor just how they're managing their risks.

As Boehme notes, balancing these goals can be difficult. Time and resources are always limited. It's often difficult for corporate executives to grasp fully the culture and business norms of all the countries in which their organizations are operating. And their efforts to work with the local business units may not always be warmly received.

In many organizations, "the local country manager or regional vice president is the most powerful face of the company," Coughlan says. Their backing is critical to gaining support from employees and third parties.

Overcoming these challenges often requires a "bifocal approach," Coughlan says. That is, compliance needs resources in place within the operating companies in various locations, as well as visibility into activities across the enterprise. "It's think globally, act locally," she explains.

Bunge, a $61 billion food and agriculture company operating in 40 countries, is implementing a third-party risk management system that will "bring further standardization to the way it manages third-party risk," says Paul Zikmund, director of global ethics and compliance. He adds that the system will formalize many of the processes already in place.

The operating companies, for example, will follow a standard process for conducting due diligence and requesting background information on specified types of third parties. In addition, a database of third-party representatives' names, as well as third-party due diligence materials, will be centralized, Zikmund says.

Gaining Buy-In

Communication, say third-party risk-management advisers, is the critical factor to securing support from operating companies for third-party compliance initiatives. Corporate compliance can help the local operating units understand the risks of non-compliance, as well as the benefits of undertaking initiatives that might initially appear to be simply more bureaucratic processes. Compliance can help local management appreciate the ways in which visibility into the supply chain can help not only compliance, but also lead to efficiencies, Coughlan says.

Compliance also can work with the operating units to meld compliance actions within the procedures already in place, Dickenson says. The local finance group, for example, probably has an on-boarding process for new suppliers that could be modified—perhaps rather easily—to incorporate the questions that compliance also needs answered. "You want to weave in compliance requirements to become part of the process," he says.

Weeding out shell companies, which often are used in bribery schemes, requires compliance to obtain the entities' true legal names, principals, headquarters, and other information, Dickenson says. The processes for obtaining this can be similar to that used by banks to comply with "know your customer" requirements.

Ongoing Risk Management

Managing third-party risk on an ongoing basis is just as important as the initial due diligence—even though that's where the communication with third parties tends to be concentrated, Coughlan notes. While no magic formula exists, organizations should make multiple attempts to reach out to third parties and ensure that employees there are trained on anti-bribery and anti-corruption practices.

Some companies use electronic training modules. While these can help, compliance still needs some way to ensure that it's not just a small segment of third parties that are working with them, Coughlan says. Another tactic: dedicating a session at annual gatherings of third parties to compliance topics.

Healthy skepticism can also help. If a reseller's recent sales figures are well above historical numbers, it may mean the company is doing a better job, but it might indicate that the company's policies or rules are being bent or broken. "It may be cause for celebration, but you also want to look at sales practices," Dickenson says.

Technology's Role

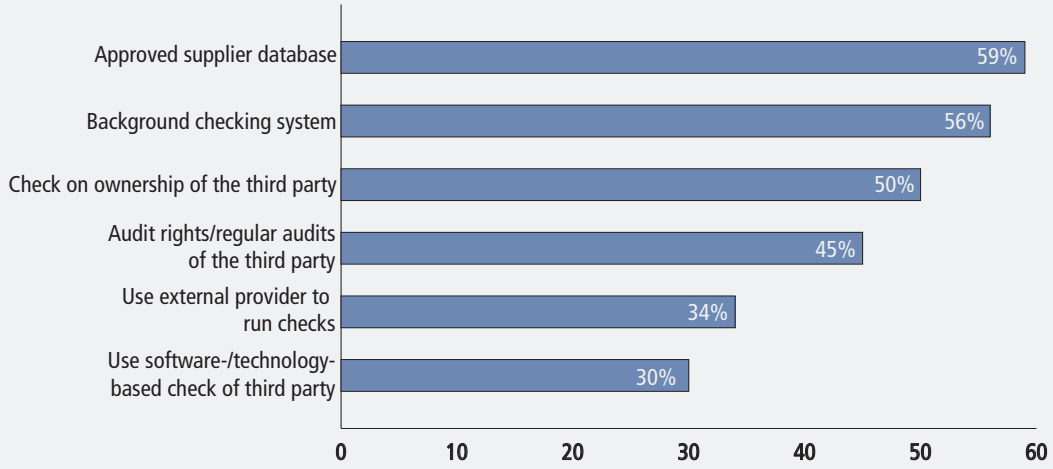
Of course, automating many of the internal and external monitoring needed for an effective third-party risk management program can save valuable time for operating units and corporate compliance professionals. "At Bunge, for instance, the compliance area is developing a portal through which the on-boarding process and forms will be automated," Zikmund says.

Another example: A company bringing on a low-risk supplier may determine that confining its due diligence to a database search of the company will suffice, Dickenson says. With a higher-risk third party—perhaps one that will be working in a riskier region or that accounts for a greater portion of business—it may make sense to supplement the electronic research with more extensive investigation, such as a site visit.

Technology can also help companies systematically monitor news reports and sanction lists for mention of their third parties, such as a report by a local publication in the supplier's home country that a supplier's CFO was arrested on bribery charges. Using technology to uncover such reports can accelerate the process, provide an audit trail, and allow those within the company who should have the information an easy way to access it, Dickenson says. ■

MANAGING THIRD PARTIES

The graph below from EY's *12th Global Fraud Survey* shows what approaches survey respondents use in managing third-party relationships.



Source: EY.

10 Components NO DUE DILIGENCE PROGRAM Can Go Without

By Michael Volkov

Unless you are a mind reader, you will never be able to predict whether any particular third party you work with will commit bribery. Instead, a systematic, holistic, and rigorous approach to due diligence must be in place to ensure that your company is asking the right questions about whom to work with based on the right information delivered at the right time.

There are some components that all programs should have. Below are the ten components all due diligence programs need:

1. Support and Buy-In of Senior Executives and the Board

Before, during, and after a due diligence program is implemented, it is critical to have the full support of senior executives and the board. Your program needs to be structured to work with your managers and executives to help them build the business by partnering with responsible, professional companies. A due diligence program that is seen only as an annoyance, e.g. "a bunch of forms that don't matter anyway," is ineffective and a waste of time for everyone involved.

As a compliance officer, your job is to make the case for why a due diligence program is necessary and how it can be a valuable company asset. An effective ethics and compliance program:

a. Helps prevent: enforcement actions, collateral civil litigation, and the associated loss of confidence by shareholders, stakeholders, and the public at large.

b. Will improve: employee morale and productivity, financial performance, decision-making quality, and employee stability.

If company leaders do not see the value in a due diligence program, it will not be allocated adequate resources. Take time to gain buy-in from top executives and the board up front.

2. Internal Due Diligence Policies and Procedures

This is the most basic requirement. Written policies and procedures are the starting point for most compliance programs. The following are common policies that benefit most companies in supporting and maintaining an effective due diligence program:

» Due Diligence Procedure: This policy should lay out each step in the due diligence process and require certification that each step was completed. It should be comprehensive but not too detailed since some issues will be decided on a case-by-case basis.

» Due Diligence Forms for Internal Use: A company has to require a businessperson to "sponsor" a proposed third party. These forms should ask for basic information about the selection process for the third party, the anticipated scope of the relationship, and the business justification for hiring a third party. These forms should be viewed as flexible—altered and added to when needed to reflect unique circumstances or risks.

At a minimum, internal due diligence forms should ask for:

- ✓ Business Justification
- ✓ Statement of Work
- ✓ Proposed Relationship
- ✓ Proposed Compensation Structure

3. Due Diligence Questionnaires for Third Parties

The questionnaire that you provide to potential third party business partners is one of the most important tools in your due diligence toolbox. You should view this as a direct line of communication to the potential third party. In addition to asking for basic background information, use this form as an opportunity to ask pointed questions about specific concerns. These forms should be flexible—altered and added to when needed to reflect unique circumstances or risks. To minimize the burden on compliance teams, the process of distributing and collecting responses to the questionnaire can be automated using an online due diligence application.

At a minimum, the questionnaire should ask for the following in-

Before, during, and after a due diligence program is implemented, it is critical to have the full support of senior executives and the board. Your program needs to be structured to work with your managers and executives to help them build the business by partnering with responsible, professional companies.

formation:

- ✓ **Ownership:** Who owns the potential third-party business partner?
- ✓ **Relationships With Foreign Officials:** Is there any direct or indirect foreign official ownership?
- ✓ **Type of Services Provided:** What services will be provided in the proposed relationship?
- ✓ **Business Background:** What prior experience does the potential third-party business party have?
- ✓ **Business References:** Request professional and financial references attesting to the proposed third-party business partner's solid standing.

4. Risk Ranking Based on Red Flags

An effective due diligence program allocates resources by ranking risks. Higher risk candidates should be treated differently than lower risk candidates. You should risk rank third parties annually and assign monitoring tools based on relative risk ranking (e.g. audits, unannounced visits or meetings, annual training, more frequent certifications).

A good due diligence investigative service will provide risk ranking information in a due diligence report. The best services have developed their own risk ranking formulas based on sophisticated algorithms that take into account the type, frequency and relationships between identified red flags. Sophisticated risk-ranking systems are "locked-down" so they cannot be manipulated by users to reach desired results. Objectivity is key to the Justice Department and Securities and Exchange Commission when evaluating whether a compliance program is effective.

Key risk-ranking factors include:

- ✓ **Geographic:** Countries are ranked by Transparency International, a ranking can be found here: http://www.transparency.org/research/cpi/overview
- ✓ **Industry:** Some industries are historically more dependent upon bribery such as the medical device industry and the oil industry.
- ✓ **Adverse Media Reports:** If any negative media reports were discovered you must investigate further. Was there any basis to any corruption allegations? How did the potential third-party business partner explain the adverse information? This may require an enhanced due diligence service investigation.
- ✓ **Government Relationships:** Involvement of foreign official, foreign government referral
- ✓ **Services or Compensation Irregularities:** Are the proposed services typically provided by third parties in that region in that industry? Is the proposed compensation structure typical of third parties in the region in the industry?

Sophisticated risk-ranking systems are "locked-down" so they cannot be manipulated by users to reach desired results. Objectivity is key to the Justice Department and Securities and Exchange Commission when evaluating whether a compliance program is effective.

- ✓ **Prior History:** Has this potential third-party business partner ever been involved in a corruption scandal in the past? Have other major companies worked with them? Have other major companies performed due diligence on them and ultimately rejected them?

5. Due Diligence Investigative Services

This is perhaps one of the most essential components of a compliance program. Your company should form a relationship with a due diligence provider—there are a number of excellent options available today. These services are vital—they are your "boots on the ground," providing adverse media searches, local record checks, and pictures of local facility and local investigative and reputational evidence. These services empower you to double-check your inter-

nal knowledge of a potential third party and the information a third party provides in their questionnaire.

Even more importantly, due diligence reports from investigative services provide a source for customizing your third party due diligence questionnaire. For example, if a due diligence investigative service report finds an article making corruption allegations against a board member of a potential third-party business partner, you can include specific questions about the allegations and that individual's involvement in a potential joint venture.

Open Source Intelligence Screening: A company has to use an open source intelligence screening service to check the third party and its owners against databases that collect adverse information, prior corruption allegations, civil and criminal prosecutions, and other important relationship information.

Risk Ranking Formula: The best due diligence investigative services include a risk analysis in their due diligence reports. Some of the most sophisticated due diligence investigative services have developed their own risk ranking formulas that assist you in identifying potential third-party business partners who may need more in-depth due diligence based on discovered red flags.

For important relationships that require in-depth due diligence, outside counsel should be used for investigation and resolution. These due diligence reviews are aimed at "problem situations," address serious risks, and require more resources.

In selecting a due diligence investigative service, you should look for:

- ✓ **Adequate Due Diligence Report Scope:** Does the service perform a risk assessment to rank identified issues? Are due diligence reports provided timely and with appropriate information (e.g. watch or sanctions list screening, adverse media report screening, Politically Exposed Persons (PEP) screening, financial background checks)? Are multiple levels of due diligence reports offered for when red flags necessitate a more in-depth review?

- ✓ **Online Access:** Can you easily administer through an online portal? Is there a quick glance dashboard to alert you of any newly discovered red flags? Can you designate others to assist you in carrying out due diligence tasks? Does the system allow for global collaboration with other business units? Can third parties upload documents to your portal?

- ✓ **Automation of Routine Tasks:** Does the system automate ongoing review? Are notifications automatically sent upon initiation or completion of a task? Can you "batch screen" existing third parties?

- ✓ **Third-Party Relationship Management:** Some systems will facilitate your interaction with potential third-party business partners. Is there a third-party "onboarding" process to integrate direct feedback from the third party?

6. Enhanced Due Diligence

For important relationships that require in-depth due diligence, outside counsel should be used for investigation and resolution. These due diligence reviews are aimed at "problem situations," address serious risks, and require more resources. They should be reserved for critical potential third-party partners that present an abnormally high degree of risk or where a number of red flags are found.

7. Comprehensive and Creative Written Contract Procedures

Too often companies do not approach the issue of drafting a contract as an important step in the due diligence process. It is an extremely effective way to reduce risk and demonstrate a company's good-faith attempt to ensure compliance with the Foreign Corrupt Practices Act and U.K. Bribery Act. Targeted contractual provisions should be drafted to respond to specific risks or concerns.

You should never use a "standard" contract; rather each contract should specifically address any red flags or unusual circumstances with a potential third-party business partner.

- ✓ **Control Parties:** Are there any individuals identified with red

The DoJ and the SEC have seen improvements in every company's due diligence programs. The next issue they are certain to emphasize is how the company monitored its third parties and how it used its audit rights to ensure compliance.

flags that need to be screened from operation and management of business?

- ✓ **Disclosure of Relationships:** Do any relationships need to be disclosed to prevent conflicts of interest (e.g. a manager of the potential third party is also a government official, or related to one, and must make public any conflicts of interest that may arise)?

- ✓ **Limitation of Scope:** Should the scope of the venture be limited to mitigate risks that arise from certain activities such as limiting a sales rep to commercial (not governmental) sales?

- ✓ **Anti-Corruption Training Needed:** Does the potential third-party business partner require additional anti-corruption training due to any identified red flags? Are there any specific areas of higher concern where targeted training is necessary?

8. Audit Trail

A due diligence program should be fully documented. FCPA expert Tom Fox has emphasized this point repeatedly: If it is not documented, it did not happen.

- ✓ **Research Records:** Due diligence investigative service reports provide clear proof that research was conducted to identify red flags. You need to retain all records for 5 years.

- ✓ **Advice of Counsel:** Due diligence requires advice of counsel—an extra layer of protection for every company so that they can argue to government that they sought advice of counsel on a due diligence issue and relied on that advice when making its good-faith decision. Advice of counsel completes the documentation process, providing a clear record of the due diligence process undertaken and resulting actions or decisions based on any identified red flags.

9. Ongoing Third Party Monitoring and Auditing

The DoJ and the SEC have seen improvements in every company's due diligence programs. The next issue they are certain to emphasize is how the company monitored its third parties and how it used its audit rights to ensure compliance. This is the new cutting-edge issue and one that demands careful thought and design.

Many due diligence investigative services include this service for a designated amount of time with their initial due diligence report. NAVEX Global's system includes ongoing, continuous monitoring of initial screening targets for two years. If an alert appears, the system automatically generates a new report and e-mails compliance personnel. For your organization, this translates into peace of mind knowing your third parties are continuously screened. Furthermore, costs become more predictable since you don't have to pay for additional screening every quarter/six-months/year—depending on your existing protocol.

10. Ongoing Evaluation and Improvement Procedure

No due diligence program is perfect. Each due diligence process undertaken for a potential third-party business partner will reveal strengths and weaknesses of a due diligence program. Make sure that there is a regular, scheduled method to utilize experience to improve your program. This can take the form of a "summary of due diligence procedure" write-up after each potential third-party business partner is evaluated or a quarterly evaluation of the process as a whole. Survey executives and managers who initiate the due diligence process about how it could be improved on a yearly basis.

Use the information you glean to reallocate resources, identify unnecessary or burdensome procedures, and look for technological solutions to resource issues. ■

Mapping and Monitoring Third-Party Risk

In order to center on the greatest third-party risks, companies must first know who those partners are

By Jaclyn Jaeger

Many third-party risk-management efforts start with the goal of providing full visibility over a company's universe of third-party relationships.

The trouble is that many companies still don't have a firm grasp on how to achieve that transparency, or even where to begin, exposing themselves to significant legal and compliance risks. "Companies often underestimate their universe of third parties," Randy Stephens, vice president of advisory services for NAVEX Global, says. Most tend to focus on traditional third-party relationships—such as suppliers, distributors, agents, and joint ventures, for example.


Stephens

Stephens advises, instead, that they cast a broader net to include anyone who represents the company. These third parties might include suppliers' suppliers, resellers, sub-contractors, and more.

Most global companies, however, have thousands—if not tens of thousands of third parties—and all of them must be monitored to ensure they adhere to the company's business practices. To efficiently and effectively get better control over a company's full universe of third-party relationships, the real difficultly is to "take that population of third parties and get it down to a manageable number," Graham Murphy, a principal in KPMG's U.S. forensic advisory services practice, says.

Stephens advises starting with a plan. Pull together an inter-departmental project team that includes regional and business leaders, as well as any country representatives, he says.

Next, identify the size and scope of your third-party universe—a task much easier said than done. "Most businesses procure services in a decentralized way," Walter Hoogmoed, a principal with Deloitte, says. Without any sort of master list, assembling an initial inventory of third parties involves leveraging multiple databases from multiple business units.

Develop a Matrix

Once you've gathered that master list, you'll want to separate high-risk third parties from low-risk third parties in order to more easily manage the third-party risk-management process, depending on which risk the company wants to focus on most. "If you want to concentrate on the FCPA, for example, you may want to eliminate domestic suppliers," Murphy says. "You should look at your third-party risk mitigation program as a part of your anti-bribery and anti-corruption program."

Criteria used to assess and rank the risks associated with each third party will vary by organization and may include:

- Country of operation where service will be provided;
- Nature of third-party relationship and services provided;
- Type of industry;
- Length of the third-party relationship; and
- Degree of involvement with foreign government officials.

Third parties that pose the greatest risk from an anti-bribery and corruption standpoint are those that have regular interaction with foreign government officials. "Because a company has political connections, it doesn't mean you don't do business with them; it may just mean you want to put processes and controls around that so you don't run afoul of anti-corruption laws," Murphy adds.

Another consideration when vetting third-party risk is to consider how frequently you use that particular third party. "You may want to eliminate those entities that you haven't done any business with over the last few years," Murphy says.

Triaging third parties helps set the wheels in motion for how much due diligence to perform on each third-party relationship moving forward. "Based on the inherent risk of that relationship, you might do more rigorous control testing," Hoogmoed says. For some third parties, a due diligence questionnaire might suffice, whereas others might require on-site audits, he says.

> "The business manager that runs the business process should own the risk and be accountable for the exposure associated with that third party."
>
> Walter Hoogmoed, Principal, Deloitte

Then determine who actually owns the risk. Who is purchasing from that third party? Who is approving payment to that third party?

"Every line of business has some sort of procurement, operation, or relationship manager that deals with third parties on a day-to-day basis," Hoogmoed says. "The business manager that runs the business process should own the risk and be accountable for the exposure associated with that

> "Companies can outsource the function, but they cannot absolve themselves of any responsibility ... So you want to make sure agents and those acting on your behalf have a good reputation and prior experience."
>
> Graham Murphy, Principal, KPMG's U.S. Forensic Advisory Services Practice

third party."

Remediation Measures

Once a company has mapped out its total universe of third-party relationships, the next step is to continuously monitor third parties to ensure that you are catching and addressing any new risks.

Many companies still perform this task on an ad hoc basis. "They don't have a process in place to address third-party risk from a holistic standpoint," Murphy says. "A lot of companies, for example, are managing the process on Excel spreadsheets, and it becomes very difficult to manage from that perspective."

Conducting risk management from a manual process standpoint makes it difficult to capture all third parties and the level of risk that each one poses. As a result, Murphy says, "a lot of companies right now are looking to technology-enabled solutions and putting systems in place to really help take them from a manual process to an automated process."

Some third-party risk-management solutions automate the assessment and monitoring of a company's third parties, screening for issues related to sanction and watch lists, politically exposed persons lists, and adverse media, for example.

Other avenues of continuous risk mitigation may include performing additional due diligence, exercising audit rights, providing third-party training on topics such as anti-bribery and conflicts of interest, and requesting annual compliance certifications. "You may decide to, in the worst case scenario, terminate the relationship," Murphy says.

In addition, companies should conduct a thorough onboarding process when going through a shift in business operations, or a merger or acquisition. A company that is expanding into an emerging market, for example, will want to ensure that it understands all the permits and licenses needed to build new facilities in that region. "Where you can run afoul of the law is by having an agent or third party do a lot of the gathering of that information for you," Murphy says.

"Companies can outsource the function, but they cannot absolve themselves of any responsibility," Murphy adds. "So you want to make sure agents and those acting on your behalf have a good reputation and prior experience."

The risks associated with third parties will continue to grow more prevalent as more multinational companies turn to third parties. According to a third-party risk report conducted by NAVEX Global, 92 percent of more than 300 respondents indicated that they would either increase the use of third parties over the next year, or weren't sure. Only 8 percent expected to reduce their reliance on third parties.

An effective third-party risk-management program doesn't require an unlimited budget or sophisticated tools, but it does need to be reasonably tailored to the company's level and type of third-party risk. By not monitoring third parties, and failing to document due diligence processes, companies expose themselves to significant legal, financial, and reputational risk. ■

RELATED CONTENT

Elements of a Third-Party Risk Management Program

Randy Stephens, vice president of advisory services for NAVEX Global, recommends a few basic steps toward developing an effective third-party risk management program:

Identify/Prioritize: Identify your universe of third-party relationships and prioritize by risk. Cast a broad net and include anyone who represents your company, especially those who have regular interaction with foreign government officials. Don't limit your search to suppliers, agents, and distributors.

Assess: Conduct due diligence on a risk-adjusted basis; uncover and assess risks. The FCPA Resource Guide states that the degree of appropriate third-party due diligence "may vary based on industry, country, size, and nature of the transaction, and the historical relationship with the third party."

Mitigate: Take steps to mitigate risk that was uncovered. This means checking multiple sanction lists, adverse publicity, the extent to which the third party might have relationships with foreign officials, and more.

Monitor: Even if your due diligence process did not turn up any red flags or issues with your existing or newly on-boarded third parties, resist the desire to close the book. Continuous monitoring and periodic re-screening is necessary to identify risk events, keep information current, and ensure policy compliance remains in force.

Source: NAVEX Global.

Have Great Anti-Bribery Measures? Prove It

Companies can't know if they have a great anti-corruption program without measuring effectiveness

By Jaclyn Jaeger

The list of companies facing charges from the Securities and Exchange Commission and the Department of Justice over violations of the Foreign Corrupt Practices Act continues to grow. Many of the more recent additions to that list, however, thought they had rock solid anti-bribery compliance programs in place.

So why are so many companies still getting hit with charges even though they are putting measures and programs in place to combat bribery and corruption? The answer, say anti-bribery advisers, is that there is a big difference between adopting a program and ensuring that it is effective.

"Just adopting a compliance program is not enough," says Shruti Shah, senior policy director at Transparency International USA, which issued a new report in August that looks at how companies can verify the effectiveness of their anti-corruption compliance programs. "You need to verify that the program is actually working effectively. Without verification, you don't know whether you have an effective program, or whether you have a program that's designed to be a paper tiger."

Proving the effectiveness of anti-bribery compliance programs, however, continues to elude many companies. "Few organizations have a really solid handle on this," says Ingrid Fredeen, vice president of advisory services for Navex Global. It's one area that continues to evolve, she says.

Conducting a thorough risk assessment is a good place to start. "It's a foundational element for any compliance initiative," Fredeen adds.

Another solution is to connect the dots on different elements of anti-bribery compliance. Tim Mazur, chief operating officer for the Ethics and Compliance Officer Association, says enforcement authorities "have the utmost respect" for companies that can show a clear connection between the risk assessment and the training and audits they conduct based on the findings of that assessment. "A lot of organizations don't do that," he says. Many companies perform risk assessments, audits, and training, but typically don't link the results of each one together.

"A targeted, risk-based approach is what enforcement agencies are looking for," Fredeen says. They're looking to see that compliance departments are being smart about the decisions they're making, and where they can make the biggest impact in their companies, she says.

According to Transparency International, it's more important to focus on effectiveness and risk than on thoroughness. "It's not possible to visit every location, interview every person, or test every transaction," Shah says. Taking a risk-based approach helps put focus to compliance anti-corruption efforts, she says.

A truly effective risk assessment will identify not only a company's high-risk areas, but also specific issues that may exist in those areas, or within certain business units. "What are the company's most pressing risks?" Fredeen says. "That's where you can take that risk assessment and figure out what group needs what kind of help to manage that risk better."

Compliance departments can then use the findings of the risk assessment in the company's annual planning process to effectively allocate resources. "You can't just have this great risk assessment, and not budget the initiatives that need to follow," Fredeen says.

Sight Testing

Risk assessments also serve as an important tool to determine where to allocate resources to perform sight testing and visits. "Nothing beats being able to get out and speak with people," Fredeen says.

While that's not always possible, many multinational companies have established effective compliance programs by embedding compliance heads into the business units to be the eyes and ears in various locations. "That can be very effective," Fredeen says.

The importance of performing on-site testing and visits can best be summed up by the experience of an investigator in an accounting firm, hired by a company to test its anti-corruption controls throughout various locations. "So one of my colleagues went to Brazil and checked the hotline," Shah explains. "There was only one place in the entire location where he could call the hotline from—and that was the CFO's office."

> "Without verification, you don't know whether you have an effective program, or whether you have a program that's designed to be a paper tiger."
>
> Shruti Shah, Senior Policy Director, Transparency International-USA

But that wasn't the worst part. Language can also trip up companies on anti-bribery compliance. "When he called the hotline—keep in mind, this is Brazil, where Portuguese is the primary language—the recording said, 'Press 1 for English. Press 2 for Spanish.'"

Measuring Training Results

Verifying the effectiveness of training is another emerging area that compliance departments are now paying closer attention. Historically, compliance departments have spent a significant amount of time and resources training

employees, but they haven't really stopped to assess whether it's been effective.

"One of the major trends we're seeing is that compliance professionals want to measure effectiveness," Fredeen says. According to a recent ethics and compliance training benchmark report conducted by Navex, 46 percent of more than 750 compliance professionals polled cited "measuring training effectiveness" as one of their top priorities in the next year.

They'll have their work cut out for them. When it comes to measuring training effectiveness, 72 percent of respondents to the Navex benchmark report said they rely on completion rates. Completion rates, however, are "not a measure of effectiveness," Fredeen says.

"To test whether training is effective, you need to assess whether your employees understand the training," Shah says. Interviews or employee surveys are examples of how companies can achieve that, she says.

Employee surveys, however, are only as effective as the questions that are asked. "What behaviors do you want to know about? Make those surveys meaningful," Fredeen says.

"Training is meant to be skill-building," Mazur says. One way for companies to prove to enforcement authorities the effectiveness of its compliance and ethics program is to test employees on ethics- and compliance-related skills, the most obvious being decision making, he says.

One innovative and measurable metric that more companies are beginning to use, for example, is pre-testing and post-testing. Employees go through a training program to learn skills, or enhance existing skills, and then they're tested again to gauge how their knowledge has progressed, Mazur says.

"Pre-testing and post-testing really works," Mazur says. It sends a message to enforcement authorities that the company isn't just going through the motions by simply having employees complete the training, he says.

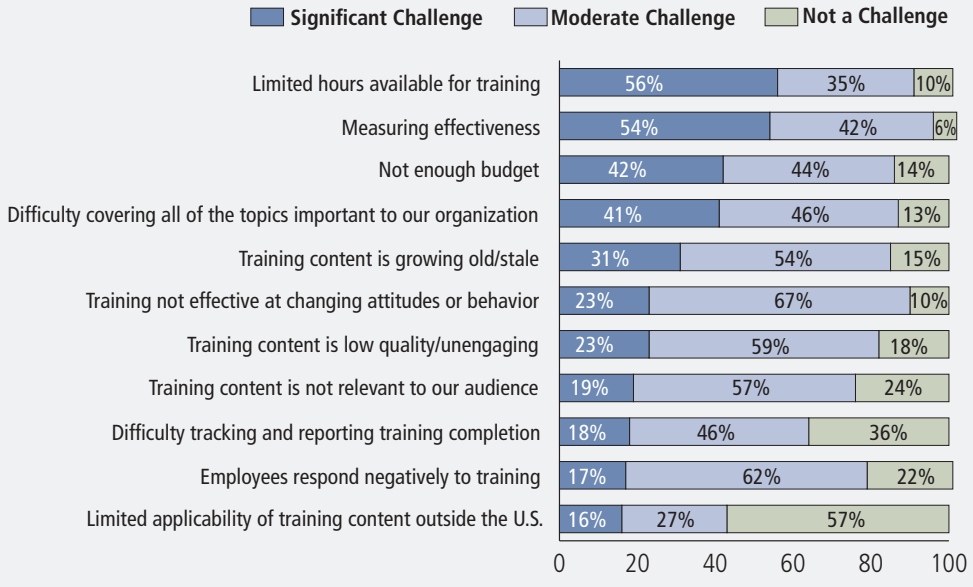
According to the Navex report, companies also have significant progress to make in the area of third-party training. Most companies do some form of initial due diligence, but don't have much interaction with third parties beyond that, Fredeen says. According to the report, for example, 57 percent of respondents said they don't perform any third-party training, while another 36 percent said they do only one to five hours of training per year.

"Do not take the approach that every third party needs the exact same level of attention," Fredeen says. "This is where the risk assessment can help to some degree." When it comes to training, target your resources to your highest risk third parties, she says.

"If you want to make sure your efforts are really effective, get critical about your program," Fredeen says. "Identify those gaps, and then train to those gaps." ■

TOP TRAINING CHALLENGES

NAVEX Global asked respondents to its 2014 training benchmark report to rank their top ethics and compliance training concerns and challenges as significant, moderate, or not a challenge. See their responses below. (Rounding may cause some totals to exceed 100 percent.)



Source: NAVEX Global.

ONLY 1 IN 3

legal and compliance executives believe they have the right tools in place to reduce third party compliance risks.*

ARE YOU ONE OF THEM?

Continuously identify, assess, mitigate and monitor risks presented by your relationships with third party business partners.

Eliminate the need for manual due diligence processing through continuous monitoring, centralized data and automated research and analysis.

Contact Us to Learn How

NAVEX GLOBAL™
The Ethics and Compliance Experts

+1 866 297 0224
info@navexglobal.com
www.navexglobal.com

*According NAVEX Global's Third Party Risk in a Global Environment: Key Survey Findings.