NAVEX GLOBAL™
The Ethics and Compliance Experts

A PRESCRIPTIVE GUIDE TO

Third Party Risk Management

By Randy Stephens, Vice President, Ethical Leadership Group, NAVEX Global

The recent examples of compliance program credits for Morgan Stanley and Ralph Lauren have demonstrated that, more than ever, an effective compliance program can protect a company from criminal indictment and generate bottom line benefits by helping a company avoid or reduce fines and penalties. Much of the recent enforcement action has been focused on liability for bribery and corruption actions performed by third parties on behalf of another company. When it comes to third party corruption, many compliance program leaders worry that they don't know where to start on a third party compliance program and that they cannot afford the elaborate, richly funded programs that are so often profiled in the news.

Luckily, you don't have to have a legion of compliance personnel and an unlimited budget to meet standards recently outlined in A Resource Guide to the U.S Foreign Corrupt Practices Act (FCPA Guidance) provided by the United States Department of Justice (DOJ) and Securities and Exchange Commission (SEC).

The good news is that almost every company has some, many or all of the elements of an effective third party compliance program. The challenge is to identify what you have. Next, document your program elements and, finally, develop and implement a work plan for addressing gaps.

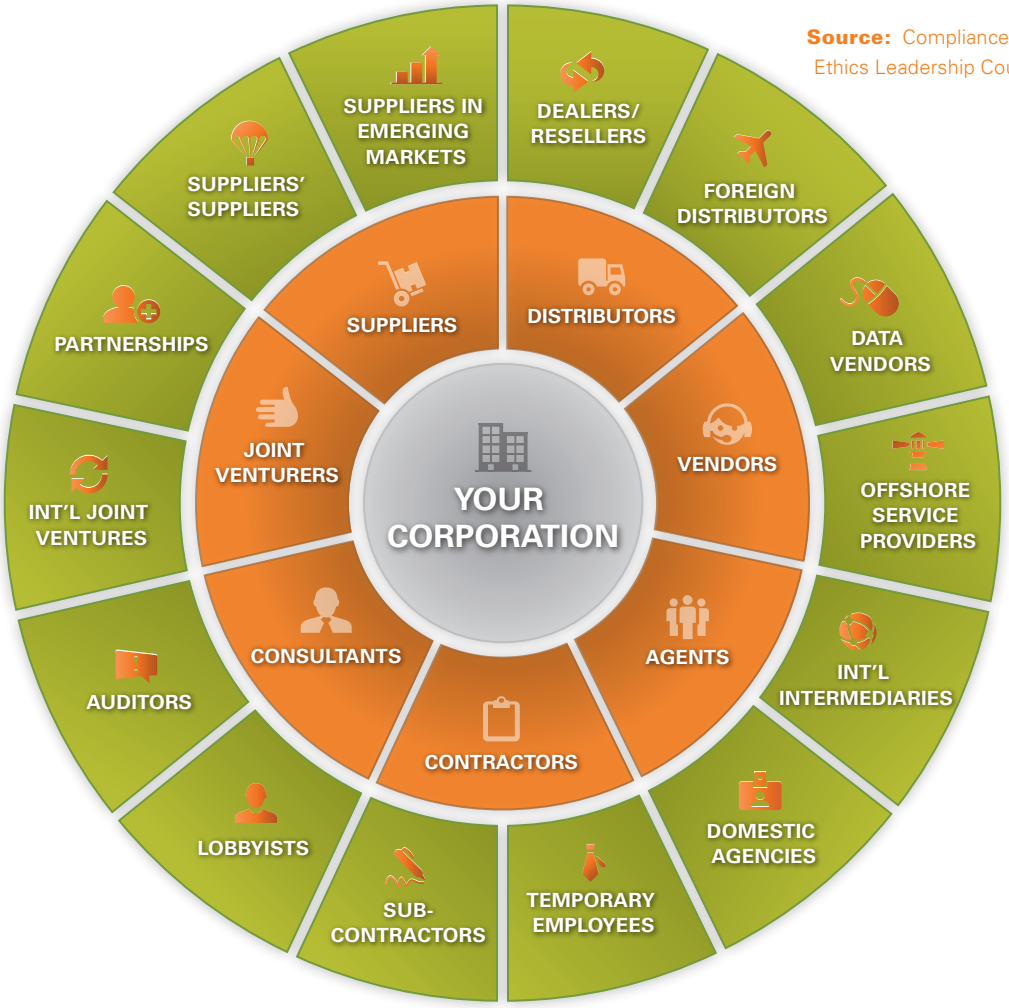
START WITH A STANDARD PROCESS

IDENTIFY/PRIORITIZE	ASSESS	MITIGATE	MONITOR
Identify your universe of relatonships and prioritize by risk.	Conduct due diligence on a risk-adjusted basis, Uncover and assess risks.	Take steps to mitigate risk that was uncovered.	Continuous monitoring and periodic re-screening to identify risk events, keep information current, and ensure policy compliance is in force.

As with all good compliance programs, the first step is always to identify and assess your company's risks. I liken the risk assessment to an excellent road map prepared for driving across country. While you could start driving without a map and eventually reach your destination, a well thought out road map helps you to get there faster and more efficiently. This risk assessment helps make sure that you properly focus your program and make the best use of your limited resources. **Don't fret over what you don't have**, focus on what you do have and fill any necessary gaps in a reasonable way. If you can't do it all at once, use your risk assessment to help you determine where to focus your energies and develop a work plan for the other items.

STEP ONE: IDENTIFY AND PRIORITIZE

Identify and prioritize all of your third parties. This is not as easy as it sounds. Depending on your company's business, size and complexity, the number of third parties could range from the hundreds to the hundreds of thousands! Cast a broad net and include anyone who represents your company, especially with foreign government officials. Don't limit your search to suppliers, agents and distributors.



Source: Compliance and Ethics Leadership Council

STEP TWO: ASSESSMENT

Now that you have identified your universe of third parties, you have to develop a process for assessing and assigning risk to each third party. The FCPA Guidance offers the "guiding principles" the DOJ and SEC have outlined for an effective third party compliance program.

RISK-BASED DUE DILIGENCE

For myriad financial and flexibility reasons, companies are relying more and more on third parties. The recent waves of FCPA enforcement actions demonstrate that third parties are often the source of inappropriate payments under the FCPA. The FCPA Guidance makes it clear that a risk-based due diligence process will be considered when assessing the effectiveness of a company's compliance program. Luckily, "…the degree of appropriate due diligence may vary based on industry, country, size and nature of the [third party] transaction, and the historical relationship with the third-party…" So one size doesn't have to fit all, but you need to have some level of documented risk-based due diligence commensurate with your risk.

WHAT DOES RISK-BASED DUE DILIGENCE LOOK LIKE?

Qualified Third Parties

The obligation is on the company to make sure that it understands the qualifications and responsibilities of third parties it engages. FCPA Guidance states that "the degree of scrutiny should increase as red flags surface."

What are some issues which might be considered "red flags?"

- Industry
- Corruption Index for the country in which the third party is operating
- Large size or sensitive nature of the transaction
- No history of past relationship with the third party
- Abnormally high commission or compensation
- Lavish gifts and entertainment expenses
- Third parties making unexpected, unreasonable or illogical decisions
- Unusually smooth processing of matters where the individual does not have the expected level of knowledge or expertise

Business rationale for using the third party

The company should understand why a third party is needed for the engagement and ensure that the third party has reasonable expertise and compensation for the engagement. A best practice utilized by many companies is to have a business sponsor assigned to each third party.

STEP THREE: RISK MITIGATION AND ACTION STEPS

Once you have identified all of your third parties, you need to ensure that you are managing your program and mitigating your risks. This is going to require some level of due diligence for each third party and watching for red flags or risks which need to be mitigated. This means checking multiple sanction or watch lists, adverse publicity, knowing the principals of the third party and the possibility that they may be or have relationships with foreign officials, etc. This may be done in-house if you have a limited number of third parties, but a preferable approach in cases where you engage either a large number of third parties or third parties who are spread globally is to use an automated provider who can swiftly and completely conduct the appropriate level of due diligence on all of your third parties.

What event might trigger a risk which needs to be mitigated or addressed?

- On-boarding new relationships
- Screening existing relationships
- Alerts:
  - Change of control
  - New adverse media
  - Change in sanctions list presence

STEP FOUR: ONGOING MONITORING AND AUDITING

The FCPA Guidance explicitly states that one guiding principle of third party due diligence is that "companies should undertake some form of ongoing monitoring of third party relationships."

So even if you have a third party program it can't be a one and done process. Even if your due diligence did not turn up any red flags or issues with your existing or newly on-boarded third parties, you can't close the book. Things change. With any effective compliance program, one of the critical factors is regular monitoring and auditing to ensure that nothing new has arisen which might change the risk profile.

Consider:

- Regular updating of previous due diligence
- Ensuring that the contract provides for audit rights, and exercising audit rights when appropriate
- Providing or ensuring that the third party is receiving periodic training on anti-bribery and your company's policies on anti-bribery and corruption, gifts and entertainment and accurate record keeping

CONCLUSION

An effective third party compliance program for every company does not require a huge budget or a large staff and a sophisticated, mature program. You do, however, need to have a program in place which is reasonable for the level and types of risks your company faces in its dealings with third parties. You have to start with identifying the size and scope of your third party universe. Then conduct a risk assessment and a risk-based due diligence process. Regularly follow up and monitor your third parties and your third party compliance program to ensure that you are catching and addressing any new risks.

Above all, seek third party expertise when you can, document your process and have a compliance work plan to address any gaps you may currently have. Having a third party compliance program in place, however basic and recently-implemented it might be, can still offer some element of defense in the event that of compliance failure by one of your third parties; having no program at all, however, will offer no protection. The sooner you start and the more closely you follow the guiding principles of the FCPA Guidance, the stronger and more legitimate your defense.

RANDY STEPHENS, J.D., C.C.E.P.

Vice President, Ethical Leadership Group, the Advisory Services division of NAVEX Global

Randy Stephens is vice president with NAVEX Global's Ethical Leadership Group. He has served as an attorney and head of compliance at a number of large national and multi-national corporations including US Foods, Inc., Dollar Stores, Inc. and The Home Depot.

Randy has spoken at national and regional conferences sponsored by organizations like the Society of Corporate Compliance and Ethics (SCCE), Compliance Week, Corporate Executive Board (CEB) and Ethics and Compliance Officers Association (ECOA) on topics like developing effective compliance programs, building values-driven workplaces and effective third-party risk management initiatives. He has also been featured in publications including the Wall Street Journal and Corporate Secretary Magazine on issues related to third party risk.

ABOUT NAVEX GLOBAL

NAVEX Global is the trusted global ethics and compliance expert for more than 8,000 clients in over 200 countries – the largest ethics and compliance community in the world. We provide a comprehensive suite of solutions to manage governance, risk and compliance (GRC), providing critical cross-program insights thorough unmatched expertise and actionable data.