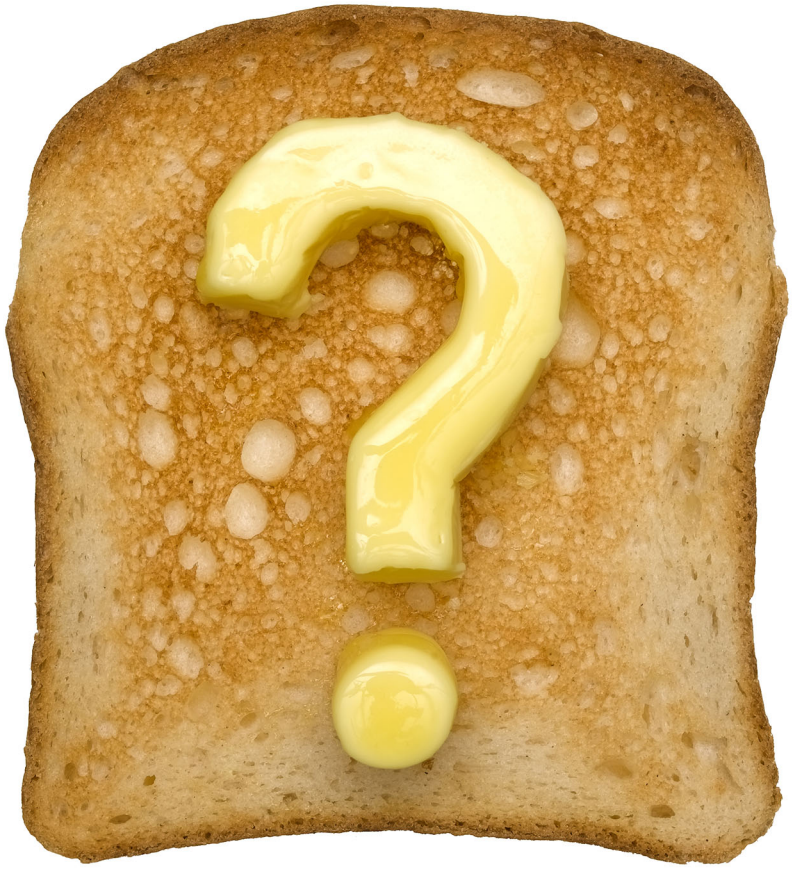
A Corporate Compliance Insights Publication

Question EVERYTHING

Effective Due Diligence and Third-Party Risk Management



By Michael Volkov

Question Everything:

Due Diligence and Third-Party Risk Management

Forward

I like to give practical advice – to my clients, my wife, my kids and my friends. And rest assured, I get a lot of practical advice from my wife, my kids and my friends.

I try not to repeat myself but would never claim to be perfect. As a strong proponent of robust ethics and compliance programs, I have noticed that I often remind my clients about the importance of due diligence.

As part of this effort, I am often explaining to clients and convincing them to devote ***more*** resources to due diligence of their third parties and their supply chain. Almost every FCPA enforcement action involves third party misconduct in one form or another. Given that fact, companies should attend to their due diligence and third-party risk management systems.

There is no magic bullet to implementing an effective due diligence system. Or, to put it another way, there is no magic formula to a due diligence system. It just takes two things: commitment and common sense. Every company knows how to do it; they just need to commit and make the effort.

This book is a compilation of advice I have given through the years. It sets out important principles and approaches to an effective due diligence system. My hope is that companies will embrace these principles as a foundation for an effective ethics and compliance program.

10 Basic Requirements for an Effective Due Diligence System

The purpose of a due diligence system is ***not*** to identify and avoid hiring a third party who will commit bribery. On the contrary, no one can predict with accuracy who will commit bribery, unless they truly have mind-reading capabilities.

Instead, the purpose of a due diligence program is to build a documentary record that can protect the company from an enforcement action under the FCPA statute when a third party engages in bribery. With this perspective in mind, there are 10 basic requirements for an effective due diligence system.

1. **Risk Ranking**: A due diligence program has to risk-rank third-party intermediaries so that the due diligence program does not treat all third parties equally. Some present a higher risk than others, and the system has to be designed to treat higher-risk candidates differently than lower-risk candidates. The risk-ranking factors are outlined in the FCPA Guidance, and they provide a comprehensive set of factors that can be used, coupled with any additional factors that are industry-specific.

2. **Written Policies and Procedures**: It is important to establish a written set of policies and procedures that are followed with respect to the initial hiring, renewal, monitoring and auditing process for third parties. The document should be comprehensive, but not too detailed since several issues will be decided on a case-by-case basis.

3. **Business Justification**: A company has to require a businessperson to "sponsor" a proposed third party. This information is critical for answering the questions of how the company learned of the third party, what services the third party will provide and the reason for hiring the third party rather than providing the services itself through internal expansion.

4. **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. There are many alternatives, but the system has to be efficient, minimize false positives and be easily accessible for company staff.

5. **Questionnaires and Reference Checks**: Everyone has their favorite draft questionnaire; they always claim theirs is the best. Some questionnaires are too complicated and unworkable. It is important to maintain focus. Why is the information needed? What will the information tell you? The questionnaire should be provided electronically to minimize the burden. Technology has made it easier and companies have to take advantage of technology. The questionnaire should include references.

6. **Due Diligence Investigative Services**: Websites are filled with advertisements and claims by third-party due diligence services. There is no question that due diligence services are needed to provide adverse media searches, local investigations and reputational evidence. The difficult questions are when to use such services and which ones to hire. The industry is moving fast in this area; information is becoming critical to corporate decisions on due diligence candidates. Some companies are stronger in certain regions, and others pride themselves on customer responsiveness. It is an important decision and one that requires careful soul-searching and ultimately, comfort with the company.

7. **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 difficult and often present serious risks. They should be reserved for the critical third-party reviews.

8. **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 the most effective way to reduce risk and demonstrate a company's good faith attempt to ensure compliance with the FCPA. Specific contractual provisions should be drafted to respond to specific risks or concerns.

9. **Documentation and Advice of Counsel**: A due diligence program should be fully documented. Tom Fox has emphasized this point repeatedly, and rightfully so. If it is not documented, it did not happen. Similarly, due diligence requires advice of counsel, an extra layer of protection for every company so that they can argue to the DOJ and/or the SEC that they sought advice of counsel on a due diligence issue and relied on that advice when making its good faith decision.

10. **Monitoring and Auditing**: The DOJ and 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 the company used its audit rights to ensure compliance. This is the new cutting-edge issue and one that demands careful thought and design.

The Missing Link in Every Third-Party Risk Management System

As the old saying goes, "don't break your arm patting yourself on the back." Everyone is pretty happy about their due diligence systems for screening third parties. I understand how they feel, but there is still a long way to go.

It is one thing to screen a third party at the on-boarding process; it is quite another to build out an entire due diligence system that screens at renewal of a third-party relationship, monitors third-party activity and conducts a range of audits to ensure compliance by third parties. Even if you have implemented all of this listed above (which is more than a mouthful), there is one important link missing in the chain of compliance.

When it comes to third parties, the focus of due diligence is prescriptive and requires responding to red flags. As monitoring and auditing practices become more sophisticated and entrenched, we will see the focus become clear: follow the money.

We can read settlement action after settlement action and we know the fact pattern: a company makes payments to a third party with the understanding that the money will be used for bribery purposes. In most cases, the third party does not have the capability or the

resources to provide the necessary services. In other cases, the payment scheme is intended to move money out of the company to the third party for improper purposes.

In the end, someone at the company is authorizing that the money be paid to the third party with questions and red flags draped all over the transaction. This is where the rubber meets the road, as we say, and this is where compliance needs to dedicate resources.

If anyone is really serious about preventing bribery, then resources and efforts need to be allocated to the movement of money. There are a number of critical questions that have to be answered:

- What is the purpose of the payment?
- What legitimate service did the third party provide?
- How did we verify that the third party provided the service?
- Is the payment amount commensurate with the market rate for the service?
- What documentation has been provided to verify all of the above questions?

I have argued for years that the best way to ensure that money does not go out the door for bribery purposes is to put an ex-pat in control of finances in a high-risk country. If your company operates in China, an ex-pat controller should manage and make all payments to third parties. In China, for example, there usually is an improper relationship between a third party and someone with access to company money that is then used to fund a bribery scheme.

If a company wants to make sure that its due diligence investment is successful, the company has to focus on payment authorizations and processes. It is a basic internal control that has to be designed and enforced.

Due diligence is designed to mitigate risk. Basic financial controls surrounding high-risk activities are critical for protecting the company from illegal bribery schemes involving a company insider and a third party.

The "I didn't know" defense is a tough one to sustain. Maybe you didn't "know," but ***should*** you have known? Were all the signs there, but you looked the other way? Should you have asked more questions? Is it fair to infer by *your failure to act or ask questions* that you **"knew"** you were violating a law or regulation?

Due Diligence and the "Knowing" Standard

The FCPA's "knowing" standard is well-defined. The DOJ's FCPA Guidance states that "Under the FCPA, a person's state of mind is 'knowing' with respect to conduct, a circumstance or a result if the person: (i) is aware that [he] is engaging in such conduct, that such circumstance exists or that such result is substantially certain to occur; or (ii) has a firm belief that such circumstance exists or that such result is substantially certain to occur. Thus, a person has the requisite knowledge when he is aware of a high probability of the existence of such circumstance, unless the person actually believes that such circumstance does not exist."

To put it simply, you cannot look the other way. If something seems off or wrong, you have to investigate. If your third-party agent promises huge returns but requires you to wire his payment to a bank account in his mother's name in Malta, you have to ask questions. If your third party asks for commission that is double what the market price is, you have to ask why. If your third party refuses to show you his business license or answer your questionnaire at all, you should considering ending any potential relationship.

Not All Red Flags Are Equal

Compliance professionals love to bandy about the term "red flag." It is a term with infinite meanings depending on the context. A red flag in a money-laundering context is different than a red flag in a corruption context.

I like to say, *not all red flags are created equal*. Some red flags are more red than others – or in extreme cases, I use the term "bloody red flag." (And I am not using the British version of bloody).

In the anti-corruption world, a red flag has a vey specific meaning because the FCPA is crafted in a way to target situations where a company or individuals act or fail to act with "willful blindness."

As a result, the existence of red flags takes on much greater significance than in other contexts, including money laundering. In the anti-bribery world, a red flag in conducting due diligence (of a third party, acquisition candidate or potential joint venture partner) translates to a circumstance that indicates an increased risk of corruption.

In the FCPA context, the danger of red flags is the risk that a failure to identify, respond and resolve a red flag can lead to a government enforcement action. DOJ and SEC prosecutors have a unique advantage when enforcing the FCPA – the term "knowing" applies to a situation where a person is aware of the high probability of a circumstance and acts or fails to act in response to the existence of the situation where there is a high probability of an FCPA violation.

To meet its burden of proof, DOJ and SEC prosecutors can cite (and have cited) the presence of multiple red flags and the actor's decision to move forward without addressing these risks. The Bourke case is a perfect example of how the statute works; Bourke moved forward in a transaction despite his knowledge of four separate circumstances (or red flags) indicating a high probability of an FCPA violation.

As a result, a Chief Compliance Officer's challenge, in the presence of a red flag, is to respond to and resolve the red flag. That can be done in a variety of ways depending on the red flag.

For example, in response to adverse media suggesting that a third party has engaged in corruption, an appropriate response may be to interview the third party about the corruption allegations, request documents that corroborate the third party's explanation, and carefully weigh the evidence and credibility of the third party. If documented, this process can create a perfect record of the company's appropriate response to a red flag.

If the record of the company's response to the red flag of adverse media is maintained, the government will be hard pressed to cite this red flag as evidence that the company chose to move ahead with the transaction despite the allegations of corruption against the third party. On the contrary, the evidence will show that the company identified, investigated and resolved the red flag, which in the end will negate any inference that the company acted with corrupt intent.

Some red flags are easier to deal with in the due diligence process. For example, if a third party requests that payment for its services be made to a bank account in Malta, an area known for bank secrecy and money laundering activities, the company can respond to the red flag by rejecting the payment request and requiring payment to the third party through more acceptable systems. Of course, the fact that the third party asked for unusual payment arrangements is still a minor red flag. The third party's agreement to a more traditional means of payment is probably an acceptable resolution of the red flag.

Some red flags can derail a due diligence process. In those circumstances, the company has to realize that doing business with the third party may not be worth the trouble.

For example, if a third party does not want to disclose its ownership information, its non-cooperation is a bloody red flag that cannot be addressed. If the third party is uncooperative in the due diligence process, how can a company expect to conduct business with the third party? These situations cry out for pulling the plug or trying alternative techniques and patience to gain the third party's trust and confidence.

Questioning Third Party Questionnaires

Third party questionnaires are a standard part of any due diligence process. They are emailed to the potential third-party business partner, filled out and sent back or the third party enters the information through an Internet portal. Compliance officers and outside counsel review the answers and squeeze as much information out as possible. The questionnaire process depends on the honesty and integrity of the third party filling out the form.

So why do we make them so difficult to answer completely and truthfully?

Many people use questionnaires that are so wordy or legally crafted that the point of each question is lost in commas, phrases and run on sentences. Even more disturbing is that the questionnaires are frequently limited to English and the prospective third party may speak English as a second, third or fourth language.

The compliance profession needs to focus on the KISS principle: Keep It Simple, Stupid.

Two basic requirements have to be met: questionnaires need to be accessible in foreign languages and they need to be designed using straightforward and concise questions.

The instinct to make third-party questionnaires complex is understandable; they are intended to gather specific information. But there is a careful balancing that must be done between making questionnaires understandable and user-friendly vs. specific and thorough. Thus far, the compliance function has tipped the scales – too far in my opinion – toward the latter.

For example, it is standard to ask about a third party's connections to the government. This is a relatively typical question:

"Are any of the Company's principals, shareholders, directors, officers, employees or related parties currently or formerly (within the last 10 years) an official, employee, agent or representative of a foreign government, state-owned enterprise or other instrumentality or political party official, political candidate for office or an official of a public international organization?"

Say that again? How long will it take a third party, for whom English is a second language, to understand this question? If they ever do?

To be fair, there is a lot of nuance in the question and it is difficult to communicate the entire concept of government connection. But if the third party cannot even understand the question, how can we expect accurate answers? Instead, what about asking:

"Has anyone at the Company worked (or do they currently work) for a government branch, a political party or the military in the last 10 years?

Does anyone at the Company currently (or in the last 10 years) work for the government, including any division, the military or a political party?"

Sure, we can include a footnote that explains: *"This includes the Company's principals, shareholders, directors, officers, employees or related parties (including close family members). The 'Government' includes any part of any government, any department, agency, state-owned enterprise (such as a state-owned oil company or airport), a political party official, a political candidate or an official of a public international organization."* Just keep it out of the main question.

A similar issue exists with contracts. We frequently use legalese and extremely complex language to address very specific topics – but contracts are designed to be examined in a courtroom. They have to define rights and responsibilities of parties very precisely and therefore need to be complex by nature. There is not a second chance to get it right once a dispute arises.

Not so for questionnaires. If you did not get the answer you want, follow up and ask another question. If you discover something later in the due diligence process that you want to follow up about, ask more questions.

An effective third-party due diligence program will often require circling back with a third party to discuss concerns that have come up. In-depth due diligence is a dynamic process; the more interactive the better. Start simple and head toward complex and specific when and if you need to do so.

Third-party questionnaires should not require days and days to decipher and complete. Simple and direct questionnaires will begin a process that leads to more complete questions and answers. Take a few minutes to review your own third-party

questionnaire, and ask yourself whether you have fallen into the complexity trap. If so, go back and revise the questionnaire to make it simple.

Basic Due Diligence Reviews – The First Step

[T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – there are things we do not know we don't know.

— former Secretary of Defense, Donald Rumsfeld

It is getting pretty crowded these days out in the anti-corruption compliance space. There are more and more companies, consultants, software providers and other entities offering to provide the right mix of information and data needed to support a due diligence review of a third party, joint venture partner or acquisition target. These companies, consultants and investigators are at the infancy of this new and sophisticated industry. Just look on the Internet for information and you will be overwhelmed.

How does a Compliance Officer shop intelligently for the right mix of information? Hopefully, the CCO will not just rely on word-of-mouth recommendations. What are the right questions to ask?

Of course, it depends on the 4 W's: who, what, when and where. The due diligence process has to be documented at every step of the process. When I say documented, I do not mean reams and reams of paper, but a good accurate summary of what was done and why certain decisions were made. So long as these are completed in good faith and with reasonable explanations, a company will be fine.

Let's be clear: we are not talking about conducting a financial audit or due diligence review, but we are talking about a due diligence investigation for potential corruption risks. The first and most important question is, who are the parties to the project? How does a company find out about all of the related and affiliated parties, along with the complicated

issue of personal relationships among family members and even political connections and relationships?

Companies have been conducting due diligence reviews for financial and legal issues for years. Anti-corruption due diligence is another matter, which frequently requires a greater in-depth analysis and fact checking. A known relationship with a government official could take on monumental significance in an anti-corruption assessment and is usually of much smaller significance in a financial or legal due diligence process.

The best source of information is usually local in nature – and it is hard to get boots-on-the-ground investigations in some of the developing countries. With time, this market will – and should – develop with new entrants or expansion of existing companies into this lucrative area.

Basic reviews should include collection and review of:

1. Publicly-available information about criminal and civil litigation, including government enforcement and private litigation, relating to all parties (owners, investors and associated financial institutions).
2. Federal sanctions lists, including Office of Foreign Assets Control (OFAC) , global watchlists and Politically Exposed Persons (PEP).
3. Newspapers, magazines, journals, NGO reports. Rumors or unsubstantiated reports need to be gathered, only to be assessed and resolved in a due diligence review.
4. Company records, ownership reports, court records, business references, real estate records and any other available information on assets or other related items.
5. The physical facilities maintained by the company, especially those smaller businesses in high-risk countries and industries.

A run-of-the-mill background check does not satisfy the due diligence requirement. The real work is in following up on the information gathered to determine what issues require further inquiry and the undisclosed gaps in intelligence. The trick is to assess the

implications of the information, what you need to know, what you do not know, what you will never know and how to weigh all of this information.

This is your basic first step. Before you unleash your questionnaires, before you interview any business references, before you interview any parties and before you do anything – you need an initial complement of information to determine what your next steps need to be.

Due Diligence – Enough is Enough

Due diligence of third parties can drive you crazy. You know you are in trouble when you start babbling to yourself and others about red flags, more red flags and even more red flags. You can start thinking that the movie "The Shining" was a documentary depicting your third-party due diligence process.

When this happens, you need an intervention. Someone has to say, "enough is enough." It is hard to do, because you always fear that under this last rock is going to be something so significant that it would change your overall assessment.

Due diligence is not an inquiry tied to findings beyond a reasonable doubt. It is guided by the principles of "reasonable inquiries." In other words, it does not mean a complete investigation of every known fact about a company or its owners. Instead, it means reasonable inquiries guided by risks, surrounding circumstances and red flags.

Two important points have to be remembered:

First, the importance of a due diligence inquiry is to document a careful review of the potential third party and to address any specific red flags that may come up. It is impossible to define every red flag that may come up; the common ones all make sense, but others can come up.

Each red flag has to be addressed and resolved one way or another. There are many ways to resolve red flags, and that can be the subject of another posting. In the absence of some effort to address a red flag, the company's risk increases. Why? Government prosecutors can cite each unaddressed red flag as evidence of willful blindness. If they find enough of them, they will prosecute the company and possibly individuals, claiming that the company possessed the requisite "corrupt intent."

Second, it is critical to consider the context in which this inquiry is conducted. It is impossible to predict in advance who among your third parties will engage in bribery. No one can read minds and no one can predict future behavior with any degree of certainty. The context for due diligence has to be remembered.

It is possible to become paranoid when conducting due diligence, especially when reviewing a third party in a high-risk country such as China, Russia or India. It becomes difficult when you cannot find any real red flags and you think to yourself, *there has to be a red flag somewhere or else I am not doing my job*.

You can only do what you can do. So long as you document the process, engage in risk ranking and allocate your time and resources based on the potential risks, you will be fine.

It is important, however, to know when enough is enough. Remote allegations in a local newspaper about potential misconduct do not by themselves require that you launch a full-scale investigation. Many times these allegations are politically motivated or made with little corroboration.

Like I said, the context and the surrounding circumstances in a due diligence inquiry are key. As long as you keep that in mind, everything will be all right.

Warning, Warning: The Danger of Third-Party Certifications

As companies wrestle with designing and implementing due diligence screening and monitoring programs, several organizations have been pushing the value of certifications.

The certification services come in different forms and with different levels of review. Plus, they come with a range of legal caveats.

For now, these programs are valuable, but only for a limited purpose. Companies that solely rely on certification services are definitely asking for trouble.

There are two problems with the certification programs:

First, and most importantly, the certification programs only collect information and ask follow-up questions, but do nothing or very little to test the accuracy or the veracity of such information. That is a big red flag unto itself and can cause serious problems.

It is easy to imagine the Justice Department and the SEC attorneys reviewing a certification file and then asking company officials why they did not follow up on information that was provided to them. It could be an easy and quick way for prosecutors to demonstrate the willful blindness of the company actors.

The certification process, however, is helpful as an initial information-gathering tool. Once a company has that information, however, the company has to act on red flags, pursue them to the point of resolution and develop risk mitigation strategies to address these red flags.

The second problem with the certification process is that there are no agreed-upon standards governing the certification process. What may be good for one organization may not work for another organization. It would be helpful for an international organization to develop such standards.

Transparency International and other anti-corruption organizations are working together in this area to help bring greater guidance to the international standards process.

My good friend, Judge Stanley Sporkin, has long advocated for an international approval process for reviewing and blessing proposed third-party agents in accordance with an agreed-upon set of standards. Once a third party is approved by this international organization, the third party would be able to satisfy most corporate due diligence screening programs.

The concept of certification process, however, is a good one. As always, the tricky part is in the details and how it is implemented. It is helpful when a potential third party brings to the table a certification.

My warning to everyone is: be careful how you use the third-party certification, look under the hood of the certification process and carefully follow up on important issues. That is

where the work will continue; due diligence screening can never be replaced by a certification process until there is a more robust set of standards applied to the certification process.

Also, it is important to remember that the initial screening is only the beginning of the third-party relationship with a company. After the screening and contract is completed, companies have to monitor their third parties, audit them when necessary and integrate them into their training and compliance programs.

Building Integrated Due Diligence Programs

One of the many challenges in the compliance profession centers on coordination and integration. There are plenty of compliance experts who can describe a perfect world – how to design a specific program and procedures to implement the program. Vendors are ready to line up at a Chief Compliance Officer's door and sell them products to carry out a specific program.

The challenge for CCOs (and for vendors) is to build integrated compliance programs that cut across various functions and compliance needs effectively. For anti-corruption compliance programs, due diligence of third parties is the most important area to achieve an integrated program.

An integrated third-party due diligence program should be based on four basic principles:

- Identify all third-parties and measure their risk
- Respond to specific risks and implement proactive strategies to minimize risk when appropriate
- Weigh business need and justification against risk
- Minimize overall risk to enterprise

The system is built on a system of risk analysis that guides the allocation of compliance resources based on a risk-ranking and monitoring system. The system requires

documentation of every step of the program, including the design and implementation of the program, the establishment of risk thresholds for certain actions and interventions and advice of counsel memos to ensure proper legal analysis and protections.

Once a company defines and identifies all of its third parties (a difficult task for many organizations), the company can apply screening procedures to calculate the risk of each third party. A different formula, which is modified to reflect circumstances, should be applied at the renewal of a third-party relationship. Between initial screening and renewal, the company should conduct periodic and regular risk monitoring calculations, and if the risk exceeds certain thresholds, an affirmative intervention program should be used to reduce the risk.

A formal third-party due diligence audit program should be conducted each year based on risk calculations and use of all audit tools (e.g. transaction testing, specific issue tests, desk audits and formal compliance and financial audits).

A consistent formula for assigning risk values should be applied at each stage: screening, renewal, monitoring and formal audit calculations. The formula can be designed using a number of variables relevant to the business and the specific industry (e.g., country of operation, extent of government interaction (sales and regulatory), percentage of government sales, foreign official or family member ownership, allegations of misconduct and/or corruption and existence of a written contract with appropriate anti-corruption certifications). However the formula is designed and the weights assigned to specific factors, the most important consideration is consistency. A formula that is applied across the board and is not intended to skew results or ignore significant red flags will minimize risk and provide a company significant protection from an enforcement action based on its due diligence program.

The biggest cause of major enforcement actions is a systemic breakdown in compliance controls. A company that is committed to an integrated due diligence program, that carries it out in good faith with documentation and advice of counsel, can never – ever – be

charged with a systemic breakdown. Even in the worst case, a company with an integrated program may miss the risks involved in a third party, but any violation is likely to be contained to a specific third party and can quickly be remedied to avoid any serious compliance breakdown.

Two Remaining Challenges: Monitoring of Third Parties and Vendor Risk Management

You have to admire Chief Compliance Officers for their tenacity and ability to multitask. They are the consummate jugglers of important projects, strategies and tasks. They can never completely finish their tasks – when one is finished, the list continues to grow with more to-dos.

Over the last few years, companies have paid more attention to third-party due diligence. As a result, companies have built effective policies and procedures to screen new third parties and add in required contractual protections to minimize risk.

Companies are now focusing on two related areas: first, monitoring of third parties and second, vendor risk management. Building a due diligence program for vendors/suppliers is not as easy as everyone thinks. CCOs know this and are familiar with the practical issues.

Here is a step-by-step outline of the process that needs to occur. This is only a basic outline, and many twists and turns can develop based on specific circumstances.

Step 1: Relationship with Procurement/Vendor Management. The CCO needs to develop a working relationship with the vendor management/procurement function in the company. Nothing will happen unless these two managers agree to coordinate and work together.

Step 2: Coordination of Functions. Vendor managers are required to build internal systems to screen potential vendors/suppliers for financial qualifications, quality, reliability and other important functions needed by the company. In many cases, the procurement side of the business has established procedures for questionnaires on

financial issues and other screening considerations. Anti-bribery issues can be built into this process as a cost-cutting shortcut for the review and screening of vendors/suppliers.

Step 3: Ranking of Vendors/Suppliers. The list of vendors/suppliers is usually very long given the number of items needed by a company to run its business. Some items directly relate to the goods and services provided by the company, and some are needed to support the company's operations. A system for ranking vendors/suppliers needs to be developed to focus the due diligence process based on corruption risk.

At the outset, an important legal issue needs to be defined. Not all vendors/suppliers fall under corruption scrutiny. The tricky issue is to define those vendors/suppliers that can create FCPA liability for your company. What do I mean by that?

Supplier A provides an important item needed by Company X to produce a product. Supplier A has to secure an import license on Company X's behalf to import the item into the country for delivery to Company X. In securing this import license from the foreign government on Company X's behalf, Supplier A can pay a bribe to the foreign official on Company X's behalf to deliver the item. As a result, Company X needs to subject Supplier A to FCPA due diligence.

In the alternative, Supplier B delivers sodas to Company Y's facility for its employees in a foreign country. Supplier B delivers sodas to over 50 companies in the foreign country. Supplier B has to import the sodas but does not do so on Company Y's behalf (since the sodas are fungible for each company receiving the sodas). Company Y does not need to conduct due diligence for any ***legal liability*** under the FCPA. However, Company Y may conduct due diligence if it decides that there is ***reputational risk*** as a result of its dealings with Supplier B.

Under these alternative scenarios, companies need to focus their due diligence efforts on vendors/suppliers by dividing their vendors/suppliers between these two categories. Once the list is divided into legal liability and non-legal liability categories, further ranking can be applied depending on the usual factors – country of operation,

amount of money involved, nature and extent of foreign government interactions, length of relationship between company and vendor/supplier, etc.

These are only the basic issues that need to be examined. As usual when dealing with due diligence issues, a number of factors can arise that are hard to predict in advance.

Fine Tuning Your Third-Party Due Diligence System

I am sure Justice Department and Securities and Exchange Commission lawyers sometimes sit back and marvel at the world they have helped create – companies are devoting more resources to the due diligence process for screening third parties. Companies are building due diligence screening procedures and more sophisticated protocols to minimize risk. The message has come through loud and clear – conduct due diligence and control your third-party risk.

In building these due diligence systems, companies are facing a number of interesting issues. It is a sign of the times that these are the issues that are bubbling up in the third-party compliance area. Here are a few of the most significant questions:

1. How should a company define and apply the term "third-party intermediary"?

A company has to have a clear definition of third parties subject to due diligence review. Companies deal with a variety of third parties, including traditional commercial sales agents who develop business opportunities with foreign government customers. The term should apply to a variety of parties, such as distributors, contractors and sub-contractors, customs agents and freight forwarders, lobbyists, lawyers, tax professionals, advertising agents, event organizers, visa agents, consultants and other professionals. Not all of these categories carry the same level of risk, since they may vary in the number and nature of foreign government interactions.

Many managers and employees may not be familiar with the scope of the third-party definition used in a company policy. It is important to communicate the broad application

of the policy to ensure that the presumption when dealing with a potential third party is to run them through the due diligence program.

2. How should a company assess risk for an initial due diligence?

The key is to keep your eye on the ball; it is easy to categorize someone as a "third party" falling under the third-party due diligence policy, but it is more important to focus on the nature and number of foreign official interactions. A risk assessment will focus on this issue and should give a company a way to rank most third parties, extending even to risk ranking of a whole category of third parties (e.g., directors of local subsidiaries from the local country).

The problem in the initial assessment phase is the absence of any track record of performance or data. The company is starting from scratch and has limited information. But you have to start somewhere and the company may be wise to conduct a more comprehensive due diligence then necessary at renewal or when dealing with a third party with whom the company has had prior relations.

3. How do I apply due diligence requirements to suppliers/vendors?

One of the most intractable issues is the application of due diligence to suppliers/vendors. Many companies have thousands and thousands of suppliers/vendors. There are two basic questions that can be applied to the list to remove several of the suppliers/vendors from the due diligence process.

First, there is a definitional issue. Not all suppliers/vendors are created equal when it comes to FCPA liability. What do I mean?

If a supplier/vendor provides the company with goods or services, which the company in turn uses to provide its product, the risk may be lower. For example, the risk to the company may be that the supplier/vendor would bribe a customs official to allow delivery of the goods to the company. It is not clear that the company, the purchaser of the goods and services, would be liable for the bribe paid by the vendor/supplier; it is unlikely

that the specific bribe can be tied to the benefit of the purchasing company, as the bribing supplier/vendor likely has a number of customers who would benefit from the bribe. Further, the transaction does not fit under the traditional third-party representative model under the FCPA statute. The purchasing company, however, would face reputational risks for associating with a company engaged in bribery.

Second, a number of suppliers/vendors can be removed from due diligence review based on annual revenues. The company should establish a minimum threshold below which due diligence may not be applied. Moreover, a review of active suppliers/vendors is likely to result in the removal of a number of suppliers/vendors who are no longer active.

Renewing a Third Party's Due Diligence

Happily married couples like to renew their wedding vows. It is a great celebration of love. When you meet the spouse of your dreams, it is a wonderful ceremony. I look forward to such an event with my wonderful wife, Rosetta.

Things may not be so smooth when it comes to a company renewing its relationship with a third party. Hopefully, it will be a smooth review and renewal process.

Companies need to include a renewal process in their due diligence programs. Luckily, companies have a lot more information to evaluate the third party and the risks of corruption once there is a track record of performance and compliance.

The due diligence process has to be modified to reflect this track record. If the company had a long relationship with the third party (over 10 years) without any blemishes, a due diligence review will be less onerous than the renewal of a third party after an initial three-year term.

As always, due diligence begins with the collection of information. The first source is always within the company. The sponsor of the third party should provide information about the relationship, how it has been operating and the identification of any problems. The sponsor should complete a questionnaire.

Similarly, the third party should be required to complete a questionnaire, which must be tailored to the individual circumstances. If there has been a long-standing relationship, the questionnaire should reflect this reality.

It is always important to confirm ownership of a third party and the absence of relationships with current and former foreign government officials. This inquiry is always required no matter the relationship between the third party and the company.

The due diligence process should include a review and evaluation of internal controls. The internal auditors and controller should be consulted to ensure that third parties are complying with invoicing requirements and payment arrangements. If additional certifications or representations are needed, they should be requested from the third party.

The internal auditors need to provide results of any audits of the third-party books. If anything unusual has been identified, or if the third party resisted the audit, these issues need to be resolved before renewal of the contract with the third party.

If there is any fresh information about possible corruption allegations involving the third party or anyone associated with a third party, these need to be examined as well.

It is a good practice to interview the key owner of a third-party representative before renewing your vows. Past performance is not an absolute guarantee of future performance, depending on the length of the relationship with the third party.

It never hurts to conduct an interview and only helps to ensure that business going forward is based on a fair and objective view of the relationship and relevant risks.

Just to be clear, I am not advocating a due diligence renewal for happily married couples seeking to renew their vows. After all, when it comes to matters of love, the heart always can tell you the truth. That same principle does not apply when it comes to matters of business.

Building a Due Diligence Package

FCPA bloggers can be repetitive; we like to rehash important points. How many more times do we have to remind everyone of the importance of documentation?

In the interest of originality, I wanted to address documentation for a due diligence package of third-party agents. Every FCPA enforcement case involves deficiencies in the hiring and supervision of third-party agents. If a company has to prioritize its compliance program projects, third-party due diligence has to be at, or near, the top of its list.

For each third-party agent, I like to keep a file with complete documentation of the due diligence process. Nothing is left to word of mouth – everything is recorded with either handwritten notes or, preferably, succinct memos.

As a first step, the company has to identify the third party, explain how the third-party agent was identified or referred to the company, detail the services to be provided and list all preliminary information known to the company. The company also must identify the current and past countries and industries in which the agent is working or has worked in the past.

After all this information is gathered and documented, the company needs to conduct an open source intelligence check with a third-party intelligence provider. Most companies buy a license to such services and integrate such checks into their due diligence protocols. This check is a critical part of the due diligence inquiry and will identify any possible connections the proposed agent has with foreign government officials, any reports of prior corruption, criminal charges or civil enforcement matters or any other relevant facts to assessing the reliability of the agent.

The initial third-party interview should follow a questionnaire that is adapted to include relevant issues. Any due diligence process must take into account new information as it is learned. An inflexible formula that does not take into account new issues is a recipe for disaster. The questionnaire should never be completed by the third-party agent, but by the company's interviewer. The third-party agent should review the questionnaire and then sign it to verify the answers. Some companies conduct third-party interviews over the

phone, given the cost of traveling to far away places. It is preferable to conduct face-to-face interviews, but the company has to be practical.

A key part of the process that is often over looked is obtaining and interviewing business references. These interviews and documents can often ferret out questionable agents and provide important information to build a due diligence file.

Your file is now getting thick. Assuming that there are no significant issues, there needs to be further discussions on the terms and conditions of a contract. The company needs to focus on a few issues: compensation, commissions, specific services to be provided, invoices, representations and warranties and audit rights. The negotiations do not need to be recorded unless some issues come up. Any written draft contracts, changes to written contracts and final contracts should be preserved.

The most important question is: *what exactly is the agent going to do for the company?* This should be outlined in as much detail as possible. The more the agent does, the better. It is important to emphasize that invoices should include detailed descriptions of the services the agent provides. In a sense, the due diligence process has to detail the reason for paying the agent for his services. The more justification included in the file, the more defensible the hiring of the agent will be down the road.

The compensation package should be considered carefully. There is nothing wrong with commissions, there is nothing wrong with retainers and there is nothing wrong with reimbursing agents for their expenses. Any package has to be justified as reasonable in the market. Extravagant commissions should be avoided as a self-inflicted red flag, but there is no hard and fast rule on commissions. Common sense is the company's guidepost.

If the agent is unwilling to represent and warrant that he or she has not violated the FCPA, or will not do so in the future, that is not just a red flag, it is a "Run Away!" red flag. The company needs to be realistic; the representation is more symbolic than anything else, since it will rarely be enforced. It is a good test to see the third-party agent's reaction.

The more difficult issue is audit rights. When I use that term, I mean not just the right to audit transactions between your company and the agent, but the right to audit the agent's entire business operation. If I were an agent, I would never agree to such terms, much less any of the model provisions floating around which require the agent to keep such records for a period of five years. If the agent is willing to agree to this provision, that is a great sign. If not, the agent needs to explain the reasons for not agreeing to full audit rights. It is important to document that the company asked for full audit rights and the agent denied the request and provided various reasons.

This step-by-step outline, however, assumes that there are no significant issues or any red flags. If there are significant issues, a "deeper dive" due diligence may be needed. Again, the compliance market has numerous services, some of which have "boots on the ground" in various countries to gather more information. If possible, "boots on the ground" are always preferable to other data collecting services.

A detailed report may be necessary to confirm certain facts or negate allegations or suspicions. The crafting of the assignment and the report should be tailored to the specific risk issues identified. The company needs to be involved in this process and make sure that the report prepared by the investigative company is reviewed and finalized by the company consistent with the due diligence inquiry. The company should make sure that unsubstantiated or "stray" allegations of misconduct against the agent are not included in the report unless such information is corroborated.

In order to finalize the due diligence package, company officials need to review and approve the due diligence inquiry and the hiring of the agent. Each review step needs to be documented and reflected in the file. If follow-up is requested, it should be completed before moving up the ladder.

Before final approval, the company needs to include a review by counsel – preferably outside counsel. For routine reviews, the counsel's memo does not need to be very long, but it should include a statement that counsel has reviewed the entire file and finds that it

is complete. The memo should include a general conclusion that based on all the facts contained in the file, counsel has not identified any significant risk of FCPA (and/or any other applicable law) violation, which would prevent the company from engaging the third-party agent.

With all of this information now in the file, the company is ready to proceed. Everyone can breathe a sigh of relief at the end for a job well done. For the company compliance officers, the work is just beginning – now they have to monitor the third-party agent's performance.

About the Author

Michael Volkov is the CEO of The Volkov Law Group LLC, where he provides compliance, internal investigation and white collar defense services. His practice focuses on white collar defense, corporate compliance, internal investigations, and regulatory enforcement matters. He is a former federal prosecutor with almost 30 years of experience in a variety of government positions and private practice.

Michael maintains a well-known blog: Corruption Crime & Compliance (http://blog.volkovlaw.com) which is frequently cited by anti-corruption professionals and professionals in the compliance industry. Michael has extensive experience representing clients on matters involving the Foreign Corrupt Practices Act, the UK Bribery Act, money laundering, Office of Foreign Asset Control (OFAC), export controls, sanctions and International Traffic in Arms, False Claims Act, Congressional investigations, online gambling and regulatory enforcement issues. Michael has assisted clients with design and implementation of compliance programs to reduce risk and respond to global and US enforcement programs.

Michael has built a strong reputation for his practical and comprehensive compliance strategies. He served for more than 17 years as a federal prosecutor in the U.S. Attorney's Office in the District of Columbia; for 5 years as the Chief Crime and Terrorism Counsel for the Senate Judiciary Committee, and Chief Crime, Terrorism and Homeland Security Counsel for the Senate and House Judiciary Committees; and as a Trial Attorney in the Antitrust Division of the U.S. Department of Justice.

Michael also has extensive trial experience and has been lead attorney in more than 75 jury trials, including some lasting more than six months. His clients have included corporations, officers, directors and professionals in, internal investigations and criminal and civil trials. He has handled a number of high-profile criminal cases involving a wide-range of issues, including the FCPA and compliance matters, environmental crimes, and antitrust cartel investigations in countries all around the world.

Representative Engagements

- Successfully represented three officers of a multinational company in two separate criminal antitrust investigations involving a criminal antitrust investigation in the District of Columbia and the Southern District of New York.
- Defended pharmaceutical company before the Food and Drug Administration and Senate Finance Committee relating to application for approval of generic drug.
- Conducted internal investigation which exonerated company against allegations of false statements in submissions to the FDA and against improper conduct alleged by Senate Finance Committee.
- Represented company before the US State Department on alleged violations of ITAR which lead to voluntary disclosure and imposition of no civil or criminal penalties.
- Advised several multinational companies on compliance with anti-corruption laws, and design and implementation of anti-corruption and anti-money laundering compliance programs.
- Advised hospitals, pharmaceutical companies and medical device companies on compliance issues relating to Stark law and Anti-Kickback law and regulations.
- Conducted due diligence investigations for large multinational companies for anti-corruption compliance of: potential third party agents, joint venture partners and acquisition targets in Europe, Africa, Asia and Latin America.
- Represented individual in white collar fraud case in Alexandria, Virginia and secured dismissal of criminal charges and expungement of criminal record.
- Represented company before Congress and Executive Branch in effort to modify Justice Department regulations concerning use of federal funds.
- Advised and assisted World Bank in review of global corruption policies, enforcement programs and corruption investigations and prosecutions.

About Corporate Compliance Insights

Launched in December of 2008 and sponsored by Conselium, a compliance-focused executive search firm, (www.conselium.com), Corporate Compliance Insights is a knowledge-sharing forum designed to educate and encourage informed interaction within the corporate compliance, governance and risk community.

Corporate Compliance Insights combines featured articles written by some of the most experienced compliance and ethics professionals in the world with regular updates of important news events in the world of governance, risk, and compliance. Additionally CCI offers an events calendar, professional company directory, leadership library and compliance jobs board.