WHITE PAPER

Anti-Bribery and Corruption Compliance for Third Parties: Is an off the shelf product enough?

March 2014

Thoughtful approaches to building a scalable, effective and proportionate program for third-party due diligence

By Kelvin Dickenson

A search on the internet under "FCPA," "UKBA" or "anti-corruption" returns an overwhelming range of products that - "off the shelf" - promise to manage third-party due diligence and protect corporations. It should be simple – just pick one and go, right?

The reality is not so easy. Some products offer expensive hands-on research, others provide access to a portal to search databases yourself, and yet more offer complex software to register your counterparties and have them answer long questionnaires. Some even offer reports at no charge to you, with your third parties paying a fee to be verified and included in a database of vetted suppliers. With so many options, what is the right answer?

First, it is important to understand the tradeoffs involved in a spectrum of products. Choosing the most rigorous approach may seem the safest way, but will most likely not be financially and operationally scalable. Choosing too simplistic a process will not expose bad actors and poor business partner choices, opening the door for wrongdoing and leaving your enterprise vulnerable.

What is required is a thoughtfully designed program that is effective, scalable, and proportionate to the unique risks facing your enterprise. It is difficult, if not impossible, to achieve this by purchasing an off the shelf product alone. Think instead about building a tailored program that incorporates the right blend of services, expertise, diligence and product solutions to efficiently and effectively protect your business.

Designing a program

The best place to start in designing your program is to ask the question, what will regulators want to see? In November 2012, the DOJ and SEC issued A Resource Guide to the U.S. Foreign Corrupt Practices Act, which outlines the approach taken to prosecution, including factors considered and the best ways for companies to protect themselves by preventing corruption. In reviewing the Guide, a key principle emerges: the program must be designed to specifically address the unique combination of risks associated with your business.

In a global marketplace, an effective compliance program is a critical component of a company's internal controls and is essential to detecting and preventing FCPA violations. ***Effective compliance programs are tailored to the company's specific business and to the risks associated with that business.*** *They are dynamic and evolve as the business and the markets change.*

A similar theme is evident in the "Bribery Act Guidance" issued by the U.K. Ministry of Justice in March 2011 which calls for "proportionate procedures":

"A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities."

The UK Ministry of Justice guidance establishes "six principles" for compliance programs (Proportionate Procedures, Top Level Commitment, Risk Assessment, Due Diligence, Communication, Monitoring and Review).

The DOJ/SEC guidance expands on this theme in detail, framing out ten hallmarks of an effective anti-corruption program:

Ten hallmarks of an effective anti-corruption program

OVERSIGHT

- Commitment from Senior Management and a clearly articulated policy against corruption
- Oversight by Senior Management with effective autonomy and resources
- Continuous improvement: Periodic testing, Risk Assessment & Review

INTERNAL CONTROLS & BEHAVIORS

- Code of conduct and clearly articulated compliance policies and procedures
- Enforced disciplinary measures for violations and incentives for compliance
- Continuing training for employees and third parties
- Confidential mechanisms for employees to report infractions and efficient, thorough investigation

AUDIT REPORTING/ ACCOUNTING

- Risk assessment and internal audit procedures to ensure compliance with accounting provisions

MANAGING THIRD PARTIES

- Comprehensive, risk-based due diligence on third parties and transactions
- Pre-acquisition due diligence and post-acquisition integration for mergers and acquisitions

We will use the "Ten Hallmarks" to frame the rest of our discussion, beginning with the first two hallmarks within Oversight at the top of the graphic. These two hallmarks are "table stakes" to any program. Commitment by senior management must exist to set the "tone from the top" while effective autonomy and resources will ensure it is also the "tone from the middle" – where culture becomes ethical in practice and not just in words.

When it comes to building an effective program, the first order of business is laid out in the third hallmark: *Periodic testing, Risk Assessment and Review.* To know what needs to be improved, you have to start by assessing your organization's current risk profile.

This concept can and should be applied to each of the remaining hallmarks:

1. Internal Controls & Behaviors

- —Code of Conduct: Is it clear and detailed, reflecting the unique risks associated with your business? Do you need a separate externally facing COC for third parties or can you use the same as you do for employees?
- —Policy & Procedures: Do they support the Code of Conduct and are they clear, easy to understand and enforceable?
- —Training programs: Does your company's risk profile require tailored programs for employees and third parties, or will pre-written video training packages be sufficient?
- —Confidential reporting mechanisms: Is an independent program managed by an outside firm or an internal HR or Audit function be better suited for you?

2. Audit Reporting/Accounting

- —Internal audit of accounting and diligence processes

3. Managing Third Parties

As we look at these areas, it soon becomes clear that they are interdependent, no matter how well designed they may be in isolation, they are only as effective in preventing corruption as the weakest link. Any of these areas could and should be the subject of a detailed narrative on their own. For the remainder of this paper, we will concentrate on the requirements for managing third parties.

Why is managing third parties such a critical focus area?

The risks of insufficient third-party diligence have never been greater, underscored as recently as December 2012 in an SEC press release announcing penalties against a major pharmaceutical company. In this release, Kara Novaco Brockmeyer, Chief of the SEC Enforcement Division's Foreign Corrupt Practices Unit stated "_____ and its subsidiaries possessed a 'check the box' mentality when it came to third-party due diligence. Companies can't simply rely on paper-thin assurances by employees, distributors, or customers. They need to look at the surrounding circumstances of any payment to adequately assess whether it could wind up in a government official's pocket."

The last several years have seen a continued increase in regulatory focus on corruption, with billions in penalties assessed by the DOJ and SEC, recent headline cases being pursued by the UK's Serious Fraud Office, renewed focus from the OECD, a new UN convention against corruption which aims to criminalize both supply and demand sides of bribery, and increased regulatory vigor in Russia, Canada, Brazil, China and beyond. The challenge is all the more palpable as it comes at a time when many companies are reliant on high-risk economies for growth.

A review of DOJ/SEC enforcement actions reveal some common trends:

- In 90% of cases historically, and in every enforcement in 2013, third parties were absolutely essential to facilitating bribes
- Companies facing penalties had processes for vetting third parties, but when examined by regulators, they were found to be insufficient or were simply not followed. Often, processes didn't recognize the different level of risk presented by a wide range of third parties and didn't fully investigate identity and suitability
- Processes had not been subject to a thorough "risk assessment" to find the weak spots and bring them current with DOJ/SEC guidance

In every 2013 DOJ/SEC enforcement, **third parties had been used to disguise, negotiate or place bribes:**

Company	Date	Penalty
Archer Daniels Midland	12-20-2013	$ 54,800,000
Bilfinger SE	12-09-2013	$ 32,000,000
Weatherford	11-26-2013	$ 253,000,000
Diebold	10-22-2013	$ 48,000,000
Total SA	05-29-2013	$ 398,000,000
Ralph Lauren	04-22-2013	$ 1,616,000
Parker Drilling	04-16-2013	$ 15,760,000
Koninklijke Philips Electronics	04-15-2013	$ 4,500,000
Stryker	01-24-2013	$ 13,200,000
Total for 2013		**$ 820,876,000**

Source: http://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml
http://www.justice.gov/criminal/fraud/fcpa/cases/2013.html

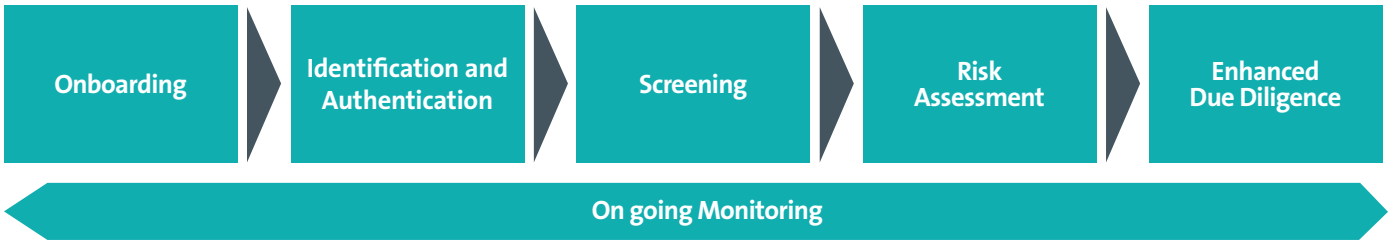
The consequences of not getting this right are overwhelming. With over $820 million in penalties assessed in 2013 alone, not to mention the impacts of declining stock price, lost revenues, reputational damage and the additional cost of remediating processes, rigorous third-party management has become mandatory.

Step I: Taking stock – documenting the current state and understanding the gaps

As we look at third-party due diligence, it helps to start looking front to back at the process used to bring third parties into your business, including how closely the process is followed, how fully it evaluates risk, and how it varies between departments, divisions and countries. Some of the initial questions you should be considering are:

- What is required in order to generate payment to a third-party? Can due diligence be bypassed?
- What information do we have on third parties already? What is available in easily accessible electronic format and what only exists in desk drawers?
- Do we have questionnaires? Are they consistently completed and what action is taken based on the answers? What information is gathered in this process?
- How are payments tracked to see if they are consistent with the intended purpose of the third-party at the inception of the relationship?
- What language considerations exist? Do you interact with your third parties in English or other languages? What translation requirements does this create?
- What criteria are in place to measure the risk associated with any given third-party – is an indirect supplier of commodities treated differently than a third-party intermediary working on your behalf? Is the process the same in every country, for every product?
- How many third parties do you have? Where are they located?
- What do you do today to identify and vet the suitability of third parties? Is this uniformly followed? Does it scale and does it reflect the risk?
- How are third parties monitored after initial vetting and selection?

A paradigm that can be found useful in framing a risk-based/proportionate approach mirrors the acceptance and life cycle of a third party:



While fully documenting each of these stages may require significant effort, it is absolutely necessary to really understand what works, what doesn't, and what gaps need to be filled.

Step II: Defining the future state – how will my program assess the risk of third parties in a scalable manner that is proportionate to the risk?

Among the first things to consider is the nature of your business. Are you growing in countries or regions with high incidence of corruption? Do you sell to governments? Do you sell directly or rely on sales agents and redistributors? Are there other environmental factors that may make my company more susceptible to an FCPA investigation?

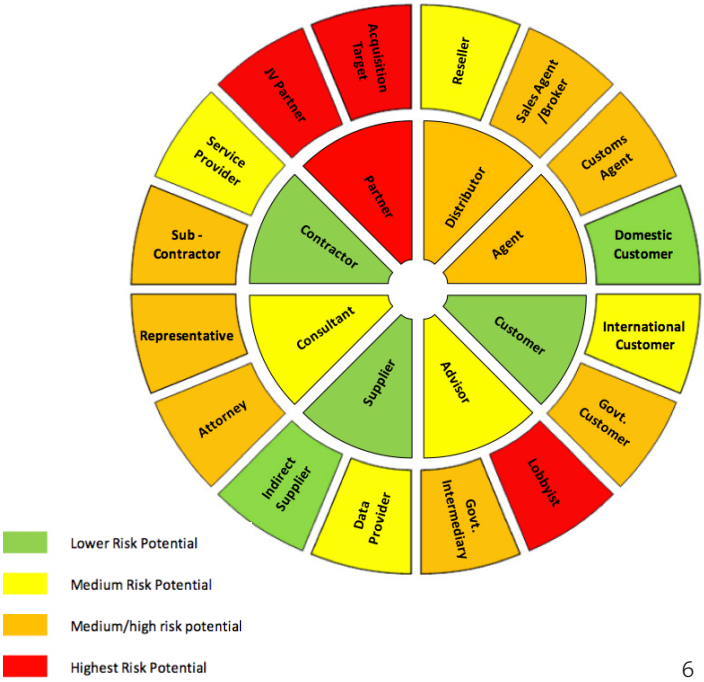
Beyond the level of risk inherent to your company or industry, each third-party will represent a different level of risk. It is in evaluating this risk that we can define appropriate levels of diligence and in doing so create a uniformly applicable policy that is scalable and removes subjectivity from the decision of what level of diligence is required.

Key factors to include in your calculation of risk include:

- Scope of service – what will the third-party be doing for you?
- Geographic location
- Information from the internal business sponsor who selected the third-party
- Responses to vendor questionnaires

Scope of service:

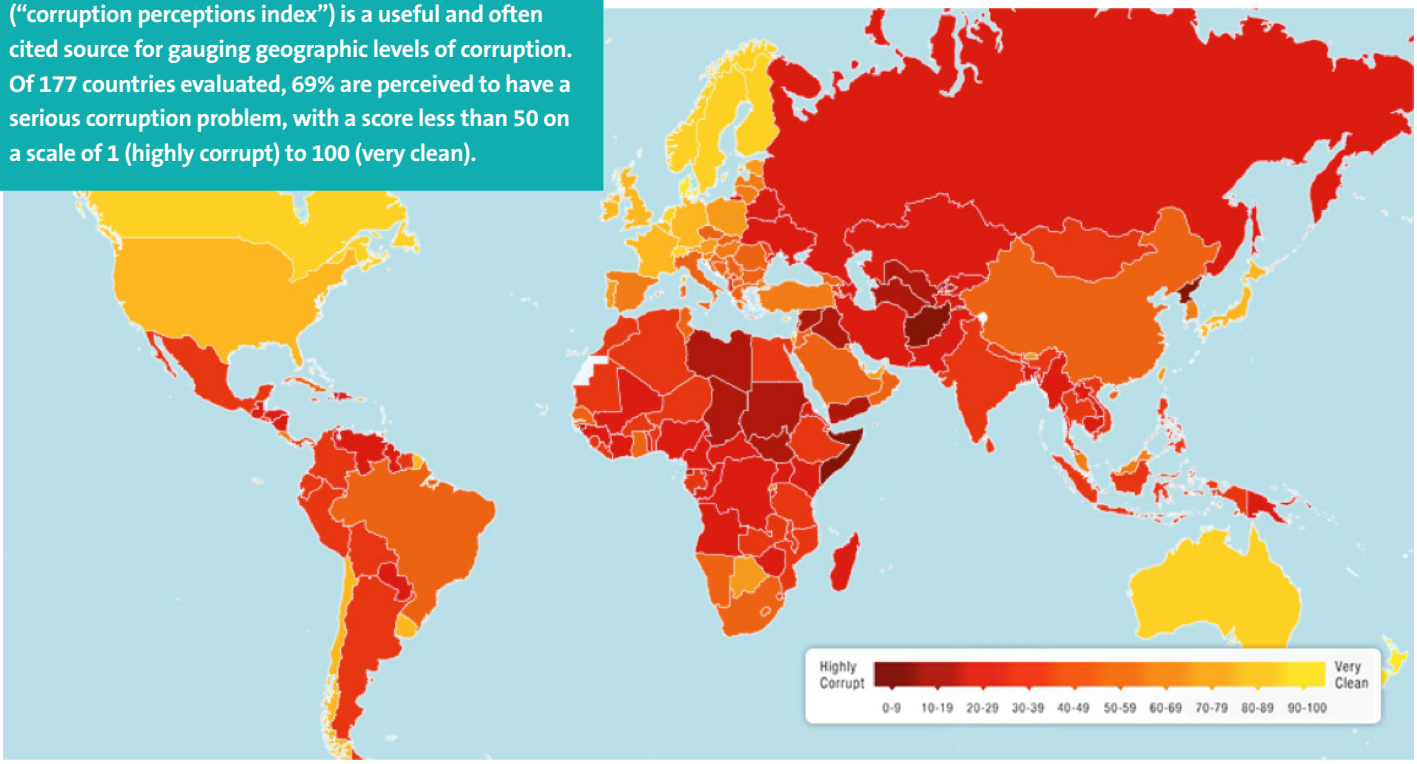
Scope of service is one of the most fundamental criteria to assess the level of potential risk. A sales agent who is helping you broker a contract with a state owned company or a government agency is much more at risk of being a vehicle for a bribe than a supplier of commodities or goods that you use in your business. The below graphic gives you an example of a mapping of key stakeholders and their levels of risk (although this mapping will vary for every company and industry):



Geographic Location:

Corruption Perceptions Index 2013

The widely recognized Transparency International's CPI ("corruption perceptions index") is a useful and often cited source for gauging geographic levels of corruption. Of 177 countries evaluated, 69% are perceived to have a serious corruption problem, with a score less than 50 on a scale of 1 (highly corrupt) to 100 (very clean).



However, in determining the appropriate approach to diligence, we need to incorporate additional geographic considerations:

- How involved is the government in business affairs?
- What laws restrict the access to and use of data used for due diligence in specific countries?
- Is it necessary to conduct investigations using local language and alphabets in order to obtain true results?
- What local nuance comes into play around address formats, common names, name format and in some countries the widespread use of aliases?
- What information is available on company ownership, officers/principals etc.?
- How will you interact with third parties in the onboarding/approval stage – remotely in English or will you have decisions distributed with local interactions in the native language? If so, how will you audit this? What translation will be required?
- What open source and public record data is available in English and accessible from outside the country?

Information from internal business sponsor:

Even prior to having the third party complete a questionnaire, we should understand from the sponsor seeking to use the third party;

- Why is this specific third party being selected?
- How were they sourced? Were they referred and if so by whom?
- What other third parties were considered?
- How does the cost compare to other candidates?
- How have we validated the third parties qualification and suitability for the scope of service contemplated?
- Is the business sponsor comfortable putting their own "stamp of approval" on the third party, as they are often in the best position to know?

In many prominent FCPA cases, a third party used to disguise a bribe was introduced by the customer seeking the bribe—and was either not a legitimate company or else was a company under their control or that of a close relative. Careful review of the selection process can identify red flags at an early stage in the onboarding process.

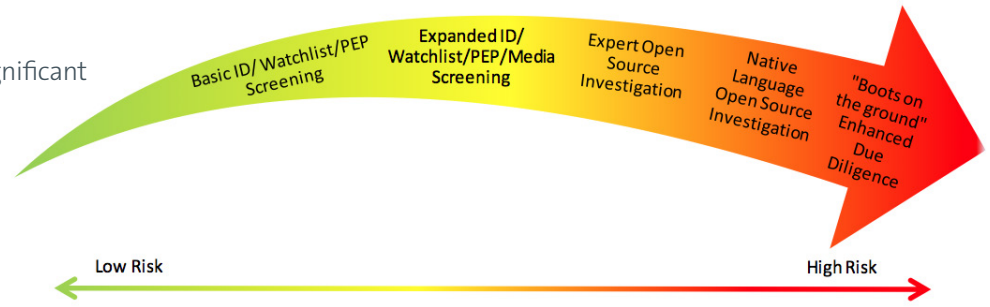
Responses to questionnaires:

A carefully crafted third-party questionnaire will yield valuable, albeit self-reported information to aid in determining the level of diligence required. While questionnaires need to be brief to ensure completion, we should learn from them;

- Does the third party have a Code of Conduct and anti-bribery training program?
- Do they have connections with and/or transactions with government entities?
- Will they be interacting with any government agency in relation to the services being provided?
- Who are the owners of the business?
- Is the third party properly positioned to fully comply with other laws that impact your company and industry (for example, privacy, export controls, financial regulations, etc.)?

Step III: Depth of Diligence

Once a set of criteria for measuring the risk is established, we can begin mapping diligence methods and requirements to that risk, progressing from a light touch automated process for lower risk third parties, to robust local "boots on the ground" investigations for the highest risks.



Acquisitions will require an even more significant depth of scrutiny, potentially leveraging specialized investigative, legal and accounting firms, interviews with key employees of the target and reviews of books and records. Beyond this, post-acquisition review, integration and remediation of the acquired company's portfolio of third parties is both critical and urgent, as is bringing their diligence process in line with your own.

Step IV: Monitoring

A common gap we often see is that once a third party is vetted, there is no ongoing review for changes in status or risk. A well thought out program will provide for monitoring of both internal and external factors, preferably with automation to allow for scale, remove redundant work and create efficiency.

- Is the actual transaction—the amounts paid to the third party —consistent with the scope considered during diligence? A program that ensures spend is properly tracked and only authorized within the approved scope will be invaluable in revealing potentially suspicious transactions
- Presence on sanctions/restricted lists, criminal activity, relationships with government entities/PEP (politically exposed persons) and adverse media should be checked not just in onboarding but on an ongoing basis, either through automated ongoing checks or through a periodic re-screen
- Changes in ownership or status, changes in management such as new CEO should also be detected and evaluated
- When a greater depth of diligence is required, such as native language open source investigation or local on-site investigation, the program and policy should include a reasonable frequency for this to be updated

A bridge to the future state – keys to success

Many of the changes that need to be made in third-party diligence will require significant change to business processes, will impact multiple constituents, and could meet with some resistance both from internal stakeholders and from the third parties seeking to provide products and services to you. It is imperative that a well thought out project plan incorporate:

- Strong and overtly articulated commitment from senior management
- Full and proper assessment of all the required policy and process changes
- Elimination of all "loopholes" in process that can allow diligence to be bypassed
- A realistic roll-out project plan that considers phases, geographic priorities and available resources
- Treatment of not just new third parties but also a defined approach to completing diligence on the existing portfolio of legacy third parties
- Procurement of outside expertise, services, products and technology
- Properly aligned budgetary authority, clearly indicating where within your organization costs will be born

Conclusion

At a time when many corporations are looking to global markets for growth, almost 70% of countries scored by Transparency International have serious corruption problems. Corruption remains a pervasive global issue, with new cases of bribery hitting the headlines with alarming regularity. Third parties are consistently at the heart of the vast majority of these matters.

While the U.S. has been leading the charge over the last decade, and accounts for most of the enforcement actions, the pressure to prevent corruption is mounting globally, with new investigations in the U.K. and a significant crack down on both supply and demand sides of corruption in China and other countries.

The traditional approaches to managing diligence around third parties, including reliance on off the shelf products alone and ad-hoc processes, have not proven sufficient in preventing bribery nor in protecting companies from the consequences. In each enforcement action we can see that third parties were not evaluated in a depth proportionate to the risk.

Buying a product off the shelf is no longer effective; a more thorough and thoughtful approach to building a risk-based program is the key to protecting your organization against the bribery issues that have cost so many organizations, so much.

About the author:

Kelvin Dickenson
D&B Global Compliance Solutions

Kelvin Dickenson, , has over 28 years' experience managing risk and regulatory compliance. Prior to his 8-year tenure at D&B, Kelvin directed regulatory compliance, credit, loss prevention, and collections activity for the commercial arm of a major credit card bank. In addition to directing these operational divisions, Kelvin's body of work includes designing compliance policies and procedures, leading development of IT solutions for compliance and credit processes, developing compliance training and writing lending policies. He is now focused almost singularly on regulatory compliance relative to third parties. Kelvin is a member of the advisory board at the Association of Certified Financial Crime Specialists.

Mr. Dickenson is not an attorney and this White Paper is not intended to provide legal advice.