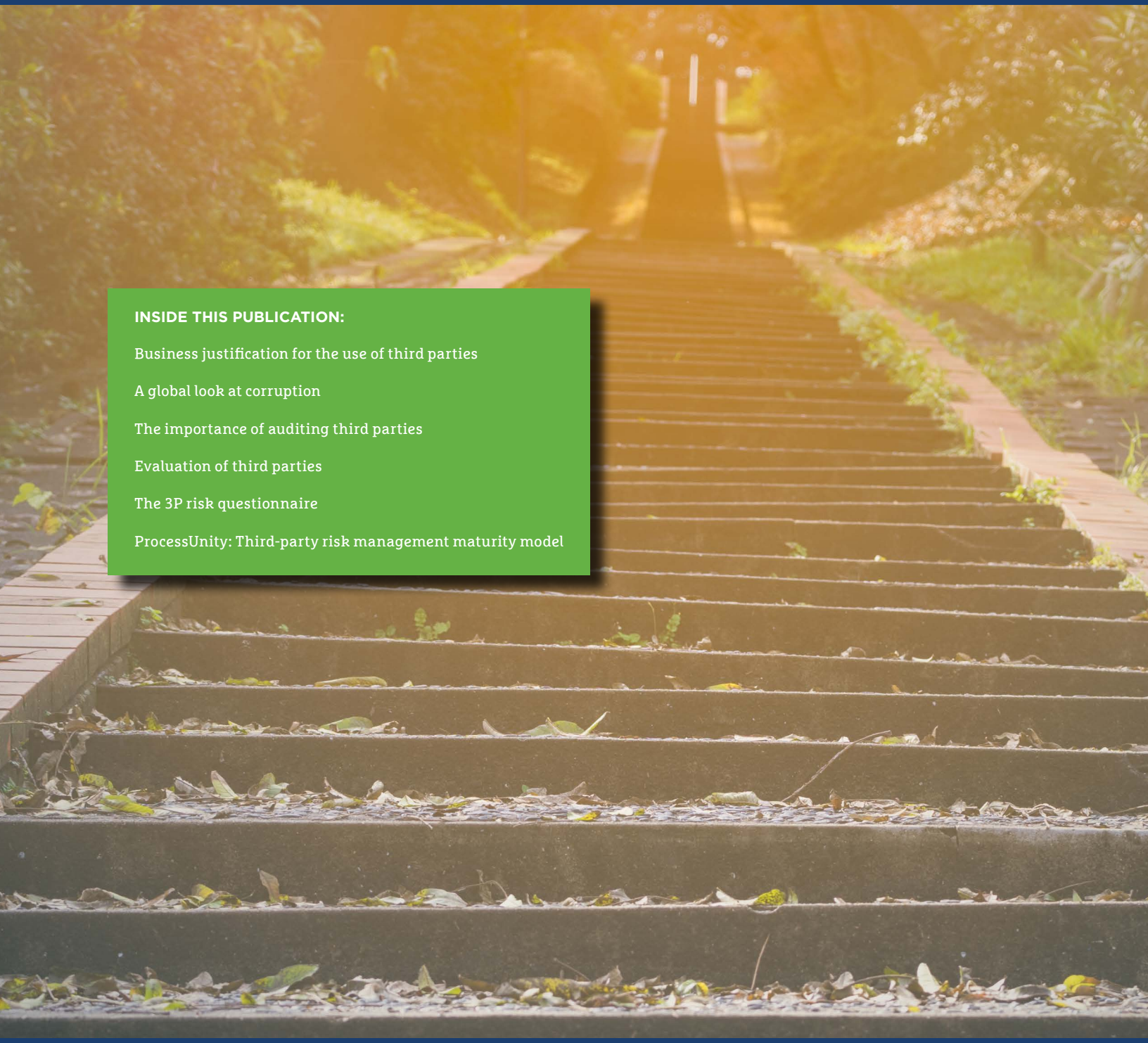
Brought to you by the publishers of COMPLIANCE WEEK



INSIDE THIS PUBLICATION:

Staying a step ahead of **third-party risks**

An e-Book publication sponsored by ProcessUnity

About us

COMPLIANCE WEEK

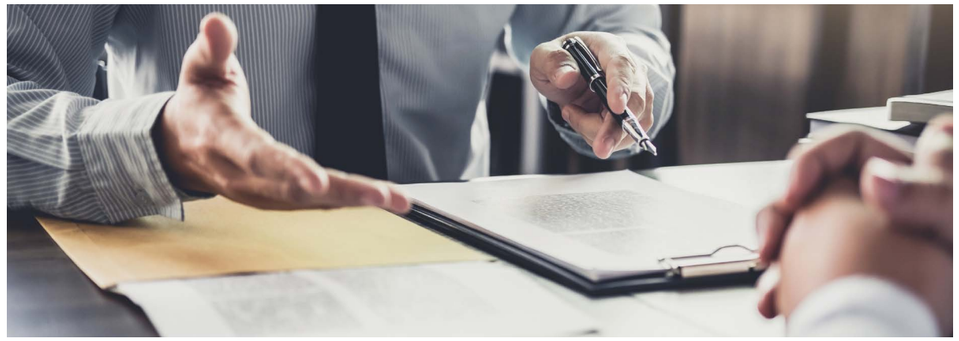
Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives. http://www.complianceweek.com

ProcessUnity

ProcessUnity's cloud-based solutions help organizations of all sizes automate their risk and compliance programs. Our highly configurable, easy-to-use tools significantly reduce manual administrative tasks, allowing customers to spend more time on strategic risk mitigation. As a software-as-a-service technology, ProcessUnity deploys quickly with minimal effort from customers and their IT resources. Our technology delivers faster, better results, and the ability to scale governance, risk, and compliance programs over time. ProcessUnity's suite of applications includes Third-Party Risk Management, Policy and Procedure Management, Enterprise Risk Management, Regulatory Compliance Management, Product and Service Offer Management, and more. Learn more at www.processunity.com.

Inside this e-Book



Business justification for the use of third parties

With the DOJ, SEC, and IRS all seeking business justification for third parties, companies should definitely make it part of the compliance process, writes **Tom Fox**.

The U.S. Department of Justice's Evaluation of Corporate Compliance Programs, Prong 10, "Third Party Management," asks, "What was the business justification for the use of the third party in question?" This question is one of the most basic tools to operationalize a compliance program and should form the basis of companies' third-party risk management processes.

It is common sense that companies should have a business justification to hire or use a third party and—if that third party is in the sales chain of the international business—it is important to understand why companies need to have that specific third party representing them. This concept is enshrined in the 2012 Justice Department FCPA Guidance, which says "companies should have an understanding of the business justification for including the third party in the transaction. Among other things, the company should understand the role of and need for the third party and ensure that the contract terms specifically describe the services to be performed."

The Internal Revenue Service also considers a business justification to be an important part of any best practices anti-corruption compliance regime. The lack of business justification is essentially a red flag; indeed, the IRS views such a lack of business justification as possible indicia of corruption. With the DOJ, Securities and Exchange Commission, and IRS all noting the importance of a business justification, it is clear this is something companies should use to operationalize their compliance programs.

The business justification also provides companies with the opportunity to help drive compliance into the fabric of everyday operations. The purpose of the business justification is to document the satisfactoriness of the business case to retain a third party and should be included in the compliance review file assembled on every third party at the time of initial certification and again if the third-party relationship is renewed.

It is important companies review their third-party processes regularly to ensure they are satisfying regulator requirements. ■

A global look at corruption

Jaclyn Jaeger explores the Corruption Challenges Index.

Chief compliance officers and chief risk officers have a newly published resource against which to assess corruption challenges and geopolitical risk in the countries where they operate to better inform what level of due diligence to perform on their third parties in certain regions of the world.

The Risk Advisory Group, a global consultancy firm, in their 2018 Corruption Challenges Index assessed 187 countries, assigning each an overall "corruption challenge" score weighted against three factors: corruption threat, regime instability, and accessibility of information. As the report shows, some countries, although they pose a high risk for corruption, also have a high degree of transparency. "Therefore, actually carrying out due diligence on counter-parties in those countries can be less daunting than it might initially appear," says Tom Russell, director of business intelligence at the Risk Advisory Group.

In other parts of the world, however, a lack of transparency—specifically, the accessibility and availability of information—is "broadly commensurate with corruption risk," Russell says, "and that, in our view, is a result of a lack of strong institutions, rule of law, and a higher level of overall political risk." Among the 187 countries assessed, Turkmenistan, North Korea, and Laos scored worst in the ability to source reliable data.

Five countries where companies face the biggest corruption challenges overall are Turkmenistan, Somalia, Libya, South Sudan, and Syria. Others that pose key corruption challenges are North Korea, the Central African Republic, Afghanistan, the Democratic Republic of Congo, and Yemen, noted the Index.

The countries where firms face the least corruption challenges overall are New Zealand, Ireland, Denmark, Belgium, and Hong Kong. Others that pose low corruption challenges are Australia, Germany, Singapore, France, and French Guiana, according to the Index.

By continent, Africa poses the highest corruption challenge for firms, while Europe dominates the list of least challenging. The three industries most exposed to corruption on a global scale overall are construction and development, infrastructure, and oil and gas. ■

Corruption Challenges Index Results

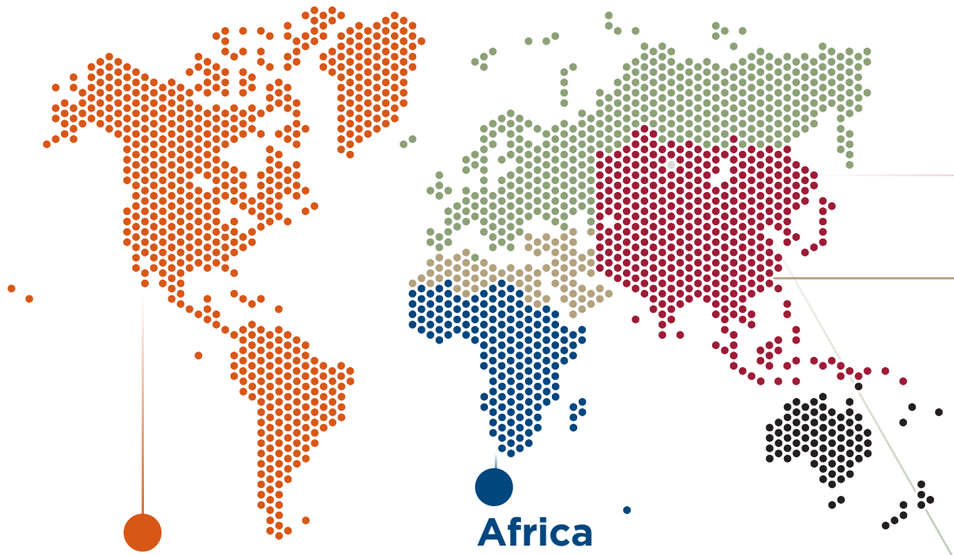
Most Challenging

1	Turkmenistan
2	Somalia
3	Libya
4	South Sudan
5	Syria
6	North Korea
7	Central African Republic
8	Afghanistan
9	Democratic Republic of Congo
10	Yemen

Least Challenging

1	New Zealand
2	Ireland
3	Denmark
4	Belgium
5	Hong Kong
6	Australia
7	Germany
8	Singapore
9	France
10	French Guiana

Source: Risk Advisory Group



Americas and Mexico

In many Central and South American countries, political instability and pervasive corruption often correlate with the availability—or lack thereof—of information, making it difficult for compliance and risk teams to conduct due diligence or investigations. "Exposing narco crimes, corruption, and money laundering—especially if they involve politicians and government officials—can lead to threats and physical violence," Steffi Probst, Risk Advisory Group's head of business intelligence for the Americas, said in the report.

Mexico, especially, continues to be one of the deadliest countries for journalists who attempt to uncover organized crime or political corruption. According to data compiled by Reporters Without Borders, 77 journalists have been killed in Mexico since 2004.

But from a corporate due diligence standpoint, some countries—Brazil, Chile, Mexico, and Argentina—have made "notable progress in improving access to information .. through continuous efforts to digitize public records," Probst said. "The quantity and quality of information about public procurement processes and government contracts in many countries in the region has also improved."

Africa

As a continent, Africa continues to pose a high corruption threat to companies. In fact, nine of the top most challenging 20 countries in the index are African. Even within the continent, however, "there are certain countries where the availability and accessibility of information isn't that bad," Russell says.

Nigeria, for example—while in a notoriously corrupt region of the world—extends a high degree of transparency. According to the Risk Advisory Group, transparency in the region stands upon three main pillars: freedom of the press; the openness and willingness of Nigerians to speak in confidence regarding casework; and the availability and reliability of public information.

Nigeria's Corporate Affairs Commission (CAC) is "probably the most accessible and easily searchable on the continent," said John Siko, Risk Advisory Group's head of business intelligence for Africa. "Even beyond Africa, the CAC is a model for transparency and simplicity."

In Africa, the top three sectors exposed to the highest level of corruption, according to the index, are infrastructure; construction and development; and transportation. "We cannot argue that Nigeria is unchallenging from a corruption standpoint," Siko added. "It is a market in which companies should prioritize due diligence of counterparties." But through diligent casework and thorough research, companies can make informed decisions about potential business partners and investments in the country, he said.

Middle East and North Africa

In some countries—like Iran and Egypt—steps have been taken to address corruption issues in a more public manner, whereby charges leveled against private businesses, state-owned enterprises, prominent merchant families, and politically well-connected executives have been publicized. "Indirectly, these probes have shed light on the lack of regulation and transparency in major deals, including large infrastructure and real estate projects that are supported by public funds," the Index states.

"Navigating the complex web of state enterprises, merchant families, and parastatal entities in the Middle East is challenging," Shahin Shamsabadi, Risk Advisory Group's head of business intelligence for the Middle East & North Africa, said in the report. "Personal connections and political leverage are key to success, yet present corruption and regulatory risks to global partners."

Prudent compliance and risk leaders should use the 2018 Corruption Challenges Index to assess a specific country's corruption challenges risk to better inform their due diligence efforts on their third parties in certain regions of the world. But it's important to keep in mind that indices like this are still just one piece of analysis. Compliance teams, in collaboration with other business units, should always conduct their own thorough risk assessments—and leverage insight from regional experts—in the countries where they operate.

Asia

"While Singapore, Hong Kong, and Japan stand out for their transparency, most other countries in the region lag far behind comparably sized economies in Western Europe and North America." According to the index, countries where it is particularly challenging to conduct anti-corruption due diligence include China, Bangladesh, and Indonesia.

In India, work performed by the Risk Advisory Group in the past year in the real estate sector, especially, "shows an industry beset with demands for bribes for all manner of licenses to obtain rights to develop land," said Brendan McGloin, Risk Advisory Group's head of business intelligence for Asia. "In Bangladesh, one of the most challenging countries to conduct due diligence in the region, much of our work on the country's leading companies all too often shows unethical ties to the ruling Awami League government."

Russia, Europe, Eurasia

For the most part, European countries scored well in the Corruption Challenges index, but in some European countries information is not as easily available as in others. This is particularly true of economies built around private wealth management—such as Liechtenstein, Andorra, Malta, and Cyprus.

In Russia, Eastern Europe, and Eurasia, "the governments pursue few if any anti-corruption policies, independent media is suppressed, and basic corporate information is not available," the Index states. Azerbaijan, for example, treats company ownership information as confidential.

Among all countries ranked in the index, companies face the biggest corruption challenges in Turkmenistan, in part because the government does not disclose all its members, according to the Risk Advisory Group. "Also, Turkmenistan's oil and gas commodities give rise to concern over the illicit enrichment of its political elite," the Index states. The Russian government also poses due diligence challenges for companies, since it "has recently classified information about certain g overnment contracts, including those relating to the military sector or supplies to Crimea, while land registry data about properties of top government officials and their families have also been designated as confidential—all in a direct effort to safeguard companies from foreign sanctions." Strictly speaking from a transparency perspective, however, the quality of corporate information disclosure in both Russia and Ukraine is high.

The importance of auditing third parties

Auditing third parties is critical to any compliance program and an important tool in operationalizing your compliance program. **Tom Fox** has more.

Auditing third parties is critical in operationalizing your compliance program. This is a key way that a company can manage the third-party relationship after the contract is signed and a measure that the government will expect you to engage in going forward.

Four to six weeks in advance, you should perform the audit with your legal counsel to preserve privilege, work with the business sponsor to establish key business contacts, and discuss audit rights and processes with the third party. You should prepare initial document request lists for financial information queries, take the time to review findings from previous audits and resolutions, and also review details of opened and closed internal investigations. If there are any code of conduct questionnaires available, take care to review them. Finally, be cognizant of any related Justice Department and Securities and Exchange Commission enforcement actions.

The next step is to determine the entry points of foreign government involvement, both direct and indirect. The direct category includes customs and duties, corporate taxes and penalties, social security or national insurance issues for employees, obtaining in-country visas and work permits, public official gifts and entertainment, training of and attendant travel for employees of government-owned entities, procurement of business licenses and permits to perform work, and areas around police escort and security.

In the indirect category, some areas to review are customs agents and freight forwarders, visa processors, commercial sales agents, including distributors and, finally, those who might be consultants or other channel partners. Document review and selection is important for this process, so you should ask for as much electronic information as possible well in advance of the audit. It is much easier to get database records for internal audits than audits of third parties.

Try and obtain records in database or excel format and not simply in .pdf. Request the following categories of documents: trial balance, chart of accounts, journal entry line items, financial and compliance policies, prior audited financial statements, bank records and statements, a complete list of agents or intermediaries, and revenue by country and customer. ■

Evaluation of third parties

Compliance practitioners at GE Oil & Gas discuss the process by which GE reviews the risks around third parties. **Tom Fox** reports.

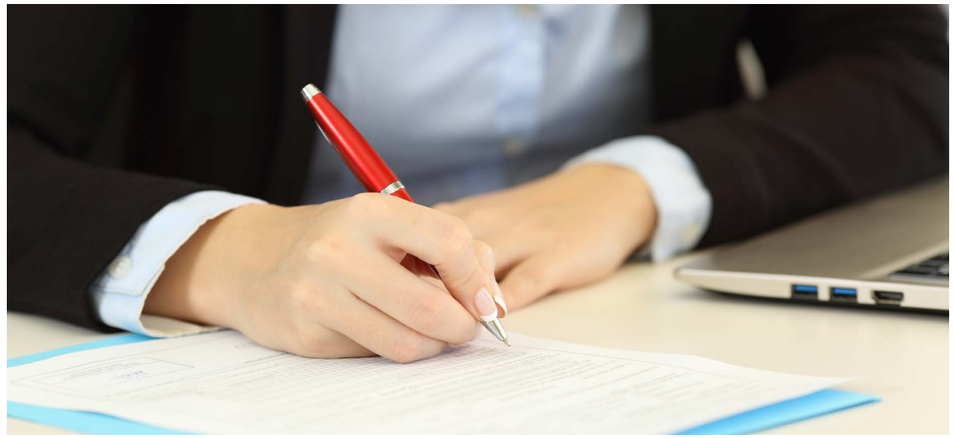
An important aspect of the compliance practitioner's duties is an evaluation of a proposed third-party relationship during the due diligence process. It is mandatory that all red flags be cleared, and there must also be evidence of the decision-making process to provide if a regulator comes knocking. The Justice Department's "Evaluation of Corporate Compliance Program" discusses under Prong 10: "Real Actions and Consequences – Were red flags identified from the due diligence of the third parties involved in the misconduct, and how were they resolved?"

There is no set formula or guideline for clearing red flags or evaluating due diligence. At the 2014 SCCE Utility and Energy Conference, however, Flora Francis and Andrew Baird, compliance practitioners at GE Oil & Gas, described the process by which GE reviews the risks around each of the company's third parties.

Some of the factors GE considers when evaluating a third party, include the following:

» **Business model:** Do we need third parties to reach our customers, or can we build the organization ourselves?
» **In-house capabilities:** Do we already have the organization in place to handle these capabilities?
» **Overlap:** Do we already have a third party in the region/country that can handle our needs?
» **Volume of business:** How much business will this third party bring to the company?
» **Compliance risk:** Where is the third party located? Will they interact with government officials? Do they have the same commitment to compliance?
» **Regulatory environment:** Is it simple or strict? What are the chances of regulatory violations?
» **Reputation:** What is the third party's reputation in the market?

Using a framework will help you manage any risk a proposed third party presents to your organization. The key is to use a framework that identifies your organization's risks and allows you to manage them effectively. Finally, as always: Document, document, document your evaluation going forward. ■



The 3P risk questionnaire

Tom Fox explores an essential piece of third-party risk management, "the questionnaire."

The second phase in the third-party risk management process is the questionnaire. The term "questionnaire" is mentioned several times in the 2012 Justice Department FCPA Guidance. It is generally recognized as one of the tools that a company should complete in its investigation to better understand with whom it is doing business. The questionnaire should be a mandatory step for any third party, and if a third party does not want to fill out the questionnaire or will not fill it out completely, you should not walk, but run away from doing business with such a party.

In 2011, the U.K. Ministry of Justice's (MOJ), discussion of the Six Principals of an Adequate Procedures compliance program noted that a questionnaire "means that both the business person who desires the relationship and the foreign business representative commit certain designated information in writing prior to beginning the due diligence process."

One of the key requirements of any successful anti-corruption compliance program is that a company must make an initial assessment of a proposed third party. The size of a company does not matter, as small businesses can face quite significant risks and will need more extensive procedures than other businesses facing limited risks. The level of risk that companies face will also vary with the type and nature of the third parties with which they may have business relationships. For example, a company that properly assesses that there is no risk of bribery on the part of one of its third parties will require nothing in the way of procedures to prevent bribery in the context of those relationships.

By the same token, the bribery risks associated with reliance on a third-party agent representing a firm in negotiations with foreign public officials may be assessed as significant and, accordingly, require more in the way of procedures to mitigate those risks.

Key aspects of the questionnaire include: ownership structure, financial qualifications, personnel who will handle the business, physical facilities, references, PEPs and UBOs, compliance training, and awareness. Once a company has taken the time to ascertain third-party views, it will give the firm the confidence to move forward with the relationship. ■

THIRD-PARTY RISK MANAGEMENT MATURITY MODEL

Find the Right Standards for Your Program

ProcessUnity

PROCESSUNITY WHITE PAPER

01 INTRODUCTION

Understand where you are today, so you can make improvements for tomorrow.

Your organization probably has some means for managing third-party risk, perhaps most urgently within the onboarding process, or maybe in response to regulatory demands.

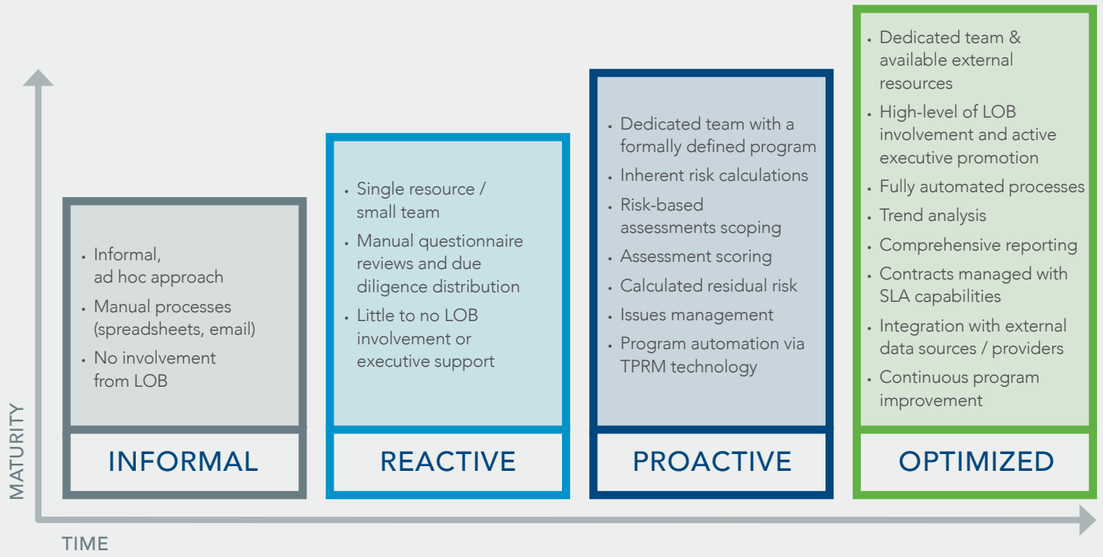
Yet you probably suspect that there remain untapped opportunities for reducing risk while reducing overhead. Or for gaining greater control over your contracting and negotiation processes. Or for simply enjoying greater ROI on your risk management investments.

These are truly achievable goals. But to move toward them, you must understand where you are moving *from* and where you stand with third-party risk management right *now*.

When you know where you are and where you'd like to go, you can choose both the appropriate destination and the right map for getting there. Businesses operate at different scales, with a variety of risks that have different degrees of severity–and potential consequences. **There is no one right third-party risk management model, but there is a model right for you**.

This paper will help you find it. To know where to go next, you must begin by understanding where you are now. By locating yourself on ProcessUnity's Third-Party Risk Maturity Scale–Informal, Reactive, Proactive, or Optimized–you gain important insight into your current risks, and viable opportunities for mitigating them.

Third-Party Risk Maturity Model



02 INFORMAL

Ad hoc and on the fly.

At a bare minimum, the "Informal" approach to third-party risk management could just as well be described as "invisible" or even, "nonexistent." Here, organizations do not have established policies or procedures for assessing risk, nor consistent processes for onboarding new vendors and/or negotiating contracts.

No one authority has assumed responsibility for risk management, communications are generally conducted through email, and vendor data (if any) is recorded on disparate spreadsheets that may be held by different persons in scattered repositories.

Everything regarding vendor management is fulfilled on the fly, without regard to standard operating procedures, ongoing monitoring, or subsequent reporting.

Merits

By virtue of its absence, informal risk management is "simple." For the smallest organizations who contract with few vendors, in fields or industries with little risk, simple might be sufficient.

Risks

Today's digital landscape exposes even the smallest businesses to devastating risks. If your vendors have access to crucial business data (such as finances, inventories, staff records) or worse, to your customers' sensitive data, you may be assuming more risk than you realize. Further, your lack of documented third-party risk management policies may discourage clients who demand security, costing you business. Even the bare minimum of risk management–establishing a standard onboarding procedure and documenting your vendor relations policies–can help you mitigate potential damage and reassure customers.

Opportunities

You have a blank slate with which to begin. Without prior precedents, you can build your third-party risk management program on best practices, facilitated by technologies that automate workflows and document progress.

INFORMAL

Informal, ad hoc approach

Manual processes (spreadsheets, email)

No involvement from LOB

03 REACTIVE

Some policies, some procedures…lots of holes.

Welcome to a very crowded club. The "Reactive" alerts–into is the most common among businesses today, populated by organizations that have documented the essentials of their third-party risk policies (often in response to a client request or a risk event), overseen by a single person or small team that has little support, few resources, and scarce budget.

At this stage, vendor risk assessment is unsophisticated, often fulfilled through a single, one-size-fits-all questionnaire that is not tailored to the nature of the vendor's work nor the likely exposures (financial, operational, data security, geographical, etc.) that work faces. Communications remain informal; there is no central repository of third-party relationship data; and once onboarding is complete, there is no formal monitoring to ensure compliance with contract terms or security expectations.

All risk management work is manually executed, opening up vulnerabilities to error, neglect, or redundant effort. Regulators may be comforted by the existence of policies, but will not be pleased by the inconsistencies in the process, the scattered documentation of effort, and the inability to extract meaningful reports from the data that does exist.

Merits

There are policies and procedures in place, a foundation that can be built upon.

Risks

Mind the gaps! Your policies and procedures may fulfill the basics of point-in-time risk assessments, but offer no pathways toward the ongoing monitoring that gives you control and awareness. Without automation, you're exposed to manual errors. Without centralization of data and command of workflows, it's difficult to demonstrate consistent, repeatable processes.

Opportunities

You can learn from your own experiences with vendors, onboarding, contracting, and risk management. By examining what works and what does not, you can determine the best roadmap toward applying automation that is consistent with your needs, policies, and workflows.

REACTIVE

- Single resource / small team
- Manual questionnaire reviews and due diligence distribution
- Little to no LOB involvement or executive support

04 PROACTIVE

Risk management facilitated by design.

The "Proactive" stage represents a significant leap forward in maturity, one in which your organization's intentions are formalized in multiple dimensions.

First, the proactive enterprise has a dedicated, full-time third-party risk management team earnestly supported by senior executives and informed with input from all lines of business.

Second, most risk policies and procedures are fulfilled through a dedicated third-party risk management system that automates workflows, centralizes data, coordinates internal and external communications, archives contracts and other relationship documentation, and enables basic reporting that can draw insights from aggregate risk data.

Third, assessments and onboarding achieve greater sophistication. Onboarding questionnaires are tailored to various risk categories, allowing more refined scoping of due diligence. Alerts and other automated prompts advance ongoing vendor monitoring to ensure compliance.

Merits

Greater automation bakes risk policy into your routine processes, accelerating risk management activities and reducing opportunities for error.

Risks

Tactic by tactic, the Proactive stage covers a lot of ground. But there isn't sufficient integration with other business systems or sources of data to provide the strategic insights necessary for negotiating more appropriate contracts or revising/adjusting risk management policies.

Opportunities

At this stage, third-party risk management is no longer a black hole of inconsistency and confusion, but a fully transparent process that enables more effective management and encourages greater confidence among regulators.

PROACTIVE

- Dedicated team with a formally defined program
- Inherent risk calculations
- Risk-based assessments scoping
- Assessment scoring
- Calculated residual risk
- Issues management
- Program automation via TPRM technology

05 OPTIMIZED

Leveraging strategic advantages to reduce costs, improve service quality.

The "Optimized" stage amplifies all the virtues of its Proactive predecessor with greater automation and systems integration, plus the incorporation of additional powers that take third-party risk management from the tactical to the strategic level.

Here, the risk management program is integrated into key business systems, like ERP, to share relevant vendor data without redundant keying. Automated scoping generates tailored risk questionnaires mapped to relevant risks and compliance issues specific to each potential vendor. Managers can actively monitor, not only conformance to risk policy, but vendor performance against precisely defined KPIs and SLAs. Your risk program can incorporate external content sources–such as financial status reports and/or "persons of interests" alerts–into its operations. Finally, the program produces customizable "scorecards" that incorporate multiple metrics into actionable reports that can inform subsequent contracting and other vendor negotiations.

Merits

In one word, control. At every level within your organization, authorized personnel have access to current, accurate information that reveals the risk status of every vendor relationship.

Risks

No risk management program, even an optimized one, is a "one-and-done" proposition. Risks and regulations change over time and as they do, risk policies, processes, and procedures must be adjusted to accommodate them. Fortunately, an optimized program is one prepared for ongoing change, able to provide the visibility and produce the reports you need to make informed adjustments.

Opportunities

An optimized program allows enterprises to enter vendor negotiations with a powerful advantage: accurate, actionable data that gives them crucial insights on the vendor's ability to meet KPIs, SLAs, and other risk performance metrics. With this information on hand, managers can negotiate for reduced fees/expenses, for increased service levels–or opt out of renewals altogether.

OPTIMIZED

- Dedicated team & available external resources
- High-level of LOB involvement and active executive promotion
- Fully automated processes
- Trend analysis
- Comprehensive reporting
- Contracts managed with SLA capabilities
- Integration with external data sources / providers
- Continuous program improvement

06 CONCLUSION

Start where you are and be prepared to grow.

Your goals ultimately determine the extent of your third-party risk management investment. No matter where you are, there is always an opportunity for growth: your program is one that will mature over time, increasing in value as you gain in experience.

But the key thing is to start with an honest assessment of where you are and where you'd like to go. Use the following Maturity Matrix as a check-up, or as a foundation for further inquiry among your colleagues, to help you determine where you are and where you'd like to go:

Maturity Matrix

INFORMAL	REACTIVE	PROACTIVE	OPTIMIZED
The Organization			
• No formal team exists (typically, a part-time resource works assessments). • There is no / minimal involvement from the business. • There is no / minimal executive sponsorship or support. • The program is not formally defined • The organization does not support third-party risk activities.	• A single resource or small team is dedicated to the program. • The business is reluctantly involved in processes (if at all). • There is minimal executive sponsorship or support. • There is minimal corporate investment to support third-party risk activities.	• A dedicated team works a formally defined program. • The business is engaged, ensuring their third-party risk is acceptable. • Full executive sponsorship exists. • The program is budgeted. • Subject Matter Experts assist in reviewing areas of their expertise.	• A fully dedicated staff operates a formally defined program. • Outsourced expertise is utilized when needed/applicable. • The business actively participates in third-party risk activities. • Executives promote risk reduction and compliance from third parties. • Budget exists to continuously enhance the program.
Policy and Procedures			
• Policies are nonexistent (or at least undocumented).	• Policies are documented. • Policy reviews are informal. • Communication around policies is ad hoc. • Policies are loosely followed. • Policies focused on onboarding activities with very little ongoing monitoring of existing third parties.	• Policy and procedures are documented. • Reviews and updates occur periodically. • A central library of policies and procedures exists. • Policies and procedures are leveraged for audits.	• Policy and procedures are documented. • Reviews and updates occur periodically. • A central library of policies and procedures exists. • Annual "read and understood" certifications are conducted with all relevant employees. • Employees are trained on all relevant policies and procedures. • Policies and procedures are leveraged for audits.

INFORMAL	REACTIVE	PROACTIVE	OPTIMIZED
Processes			
• Processes are ad hoc. • There is no consistency across organization. • No central repository exists for third-party risk information/assessments. • There is no issue resolution/ tracking for outstanding issues. • Contracts are signed prior to due diligence.	• Processes are defined. • Third parties are not monitored. • Processes are executed inconsistently. • A central location for third-party information/assessments exists. • Existing third parties are assessed for risk. • Issues are documented, but not tracked to resolution.	• Processes are defined. • Third parties are monitored periodically. • External content is used to augment the program. • Processes are executed consistently. • A central location for third-party information/assessments exists. • There is a formal third-party onboarding process. • Existing third parties are assessed for risk. • Some on-site control assessments are conducted on critical third parties. • A formal issue management process exists.	• Processes are defined with an emphasis on continuous improvement. • Third parties are monitored continuously. • A central location for third-party information/assessments is integrated with ERP, Procurement, and/or GRC solutions where applicable. • There is a formal third-party onboarding process. • Existing third parties are assessed for risk continuously. • On-site control assessments occur for critical third parties. • A formal issue management process exists. • KPIs, KRIs and SLAs related to third parties are actively monitored.
Risk Assessment Methodology			
• A standard question set does not exist. • There is no standard risk assessment methodology. • Reviews are limited to single categories of third-party risk. • Risk assessments are qualitative (if they occur at all). • Activities are focused on gathering documents/policies versus analyzing risk.	• A standard set of questions is used for all third parties, regardless of risk level. • There is no standard risk assessment methodology. • Reviews are limited to single categories of third-party risk. • Assessments are qualitative risk ratings.	• Inherent risk screening questions are used for onboarding. • Standard sets of questions/ questionnaires are used based on the third parties' inherent risk level. • Inherent and residual risks are calculated on all third parties (new and existing). • Multiple risk categories are assessed for each third party. • Inherent and residual risk is analyzed quantitatively. • On-site assessments are conducted on third parties.	• Conditional inherent risk screening questions are used based on service, product, location, branch, etc. • Standard sets of questions/questionnaires are used based on the third parties' inherent risk level. • Inherent and residual risks are calculated on all third parties (new and existing). • Multiple risk categories are assessed for each third party. • External content is leveraged to enhance third-party risk assessments and monitoring. • Inherent and residual risk is analyzed quantitatively. • On-site assessments are conducted on third parties. • Ongoing risk assessments (based on SLAs and other continuous monitoring activities) can trigger additional assessments.
Third Parties			
• Communication is delivered via manual email or phone. • Lack of central repository can result in repetitive/duplicate information.	• Communication is delivered via manual email or phone. • There are sporadic instances of duplicate efforts on similar vendors. • Reviews are performed at an overall level and do not take into account sub relationships under the third party (such as services, products, locations, branches, etc.).	• Communications are delivered via automated email and/or a technology portal. • Assessments are completed within a technology (online) portal. • Reviews are conducted at various levels (service, product, location, branch, etc.).	• Communications are delivered via automated email and/or a technology portal. • Assessments are completed within a technology (online) portal. • Issues related to third parties are actively managed via the portal. • Reviews are conducted at various levels (service, product, location, branch, etc.). • Third parties actively maintain their own company and/or service profiles. • Third parties actively manage their own key contacts and questionnaire routing within their organization.

INFORMAL	REACTIVE	PROACTIVE	OPTIMIZED
Supporting Technologies			
• Typically, spreadsheets and email are used.	• Programs are supported with email, spreadsheets, homegrown databases and/or survey tools.	• Programs are powered with a dedicated third-party risk management solution/tool.	• Programs are powered with a dedicated third-party risk management solution/tool. • The third-party risk system is integrated with other critical business application to share relevant third-party data (ERP, Procurement, Ticketing, GRC, Contracts, etc.).
Regulatory Preparedness / Stature			
• The lack of formally documented policies and procedures results in full regulatory reviews with limited positive recourse.	• Policies exist, but inconsistent execution of policies results in full regulatory reviews with limited positive recourse.	• Fully documented policies and procedures allow regulators to focus efforts on critical areas of review. • A dedicated third-party risk management solution/tool allows the organization to easily evidence activities conducted against various third parties and showcase how they have automated portions of third-party risk management program.	• Fully documented policies and procedures allow regulators to focus efforts on critical areas of review. • A dedicated third-party risk management solution/ tool allows the organization to easily evidence activities conducted against various third parties and showcase how they have automated portions of third-party risk management program. As a result, there is minimal regulator intervention and fewer requests. • The organization is recognized by regulatory agencies as a best-practice organization.
Standards Alignment			
• The organization does not leverage best-practice standards or control sets within risk its methodology or assessments.	• The organization may leverage best-practice standards to derive question sets for assessments.	• Questionnaires align to best-practice standards and/or best-practice control sets to facilitate deeper reviews of highly critical third parties.	• The organization actively aligns, reviews, and assesses risk assessment methodologies, questionnaires, and control sets to ensure they are up to date and aligned with the most-current best-practice standards.

When you determine your program's future path, ProcessUnity can help get you there. We are a leading provider of Third-Party Risk Management software tools that organizations use to automate and streamline their programs. We work with organizations large and small, with different levels of maturity, helping them advance their programs to realize greater value and reduce more risk. Working together with our experts, we can prepare your organization to meet any future changes and challenges with confidence.

To learn more about ProcessUnity and third-party risk management contact a ProcessUnity risk management expert at **info@processunity.com** or visit us online at **www.processunity.com**.

To see ProcessUnity in action, watch our **5-minute Vendor Cloud demonstration**.

ProcessUnity

www.processunity.com

info@processunity.com

978.451.7655

Twitter: @processunity
LinkedIn: ProcessUnity

ProcessUnity
33 Bradford Street
Concord, MA 01742
United States