NAVEX GLOBAL®
The Ethics and Compliance Experts

DEFINITIVE GUIDE TO

THIRD-PARTY RISK MANAGEMENT

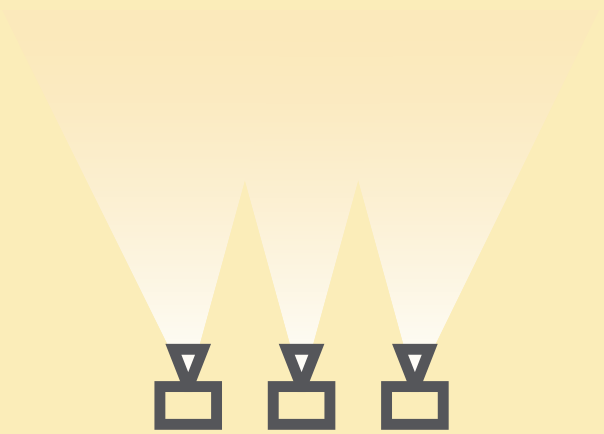
How to successfully mitigate your organisation's third-party risk

OVERVIEW

The Definitive Guide to Third-Party Risk Management is a comprehensive resource full of insight, advice and examples to help organisations identify and address their third-party risk.

A strong third-party risk management programme will help your organisation make smart choices when it comes to engaging with third party business partners. It will also protect your organisation from the risks that third parties can present.

This guide is divided into three main sections: PLAN, IMPLEMENT and MEASURE. In these sections you'll find the information and tools you need to develop a risk-based strategy, define third-party risk and a standard due diligence process, implement continuous monitoring of third parties and identify areas in which you need to improve your programme's effectiveness.



CONTENTS

INTRODUCTION

Why Is Third-Party Risk Management Important?

Who Are Third Parties?

Consultants: Auditors, lobbyists, management consultants

Contractors: Temporary employees, subcontractors

Agents: International intermediaries, domestic agencies, local advertisers and marketers, resellers and sales representatives

Vendors: Data vendors, maintenance, on-demand service providers, offshore service providers

Suppliers: Branded, white-branded or third-party branded material suppliers and manufacturers, as well as those suppliers' suppliers

Distributors: Dealers and resellers, foreign distribution firms and their local resellers

Joint ventures: Partnerships, international joint ventures (factories, manufacturers, dealers), franchisees

These are turbulent times for today's organisations, particularly when it comes to managing third-party risk. How does your organisation screen and monitor third parties? If you don't have a robust programme in place, you could be putting your organisation at significant risk.

There are many important reasons why your organisation should pay attention to third-party risk now.

» **Growing Reliance on Third Parties**
The number of vendors, suppliers and other agents with which organisations engage is growing dramatically—along with the risks they represent. According to a NAVEX Global Benchmark Report, 30 percent of organisations expect an increase in third-party engagements in 2017.[1] More and more organisations use third parties for critical operations. Outsourcing to third parties, however, poses regulatory and reputational risk—and managing this should be a top priority for leadership.

» **Increased Globalisation**
As markets expand and organisations seek to compete, increasing globalisation is inevitable. For many organisations, competing in new markets means working closely with third parties. Yet, according to the Organisation for Economic Co-operation and Development's *Foreign Bribery Report*, intermediaries pose the single greatest bribery risk for companies, concluding that 75 percent of foreign bribery schemes are executed through an agent or other third party.[2]

» **Increased Enforcement**
In the past few years, the UK Bribery Act—along with the Spanish Criminal Code, French Sapin II, German Law on Fighting Corruptions and the updated Dutch Criminal Code—has been gaining

traction in enforcement. To back it up, the Serious Fraud Office (SFO) in the UK is specifically charged with the enforcement of the UK Bribery Act. As reported in the NAVEX Global 2016 Third- Party Risk Management Benchmark Report, respondents saw a 50 percent increase in legal regulatory actions in the past three years.[1]

"Over 70 percent of FCPA investigations involve the actions of third parties."

Karen Brockmeyer
Chief of the SEC's FCPA Unit

Regulatory agencies view third parties as a direct extension of your organisation. You are expected to safeguard against risks facing your entire organisation —including the increasingly complex network of your third parties.

What Is Third-Party Risk Management & Third-Party Due Diligence?

Third-party risk management is the process of assessing and controlling reputational, financial and legal risks to your organisation posed by parties outside your organisation.

Third-party due diligence is the investigative process by which a third party is reviewed to determine any potential concerns involving legal, financial or reputational risks. Due diligence is disciplined activity that includes reviewing, monitoring and managing communication over the entire vendor engagement life cycle.

The Risks Are Real

As we see in the news too often, lapses in leadership around managing third parties have damaged organisations by exposing them to massive fines and penalties. According to the 2016 NAVEX Global Benchmark Report, one-third of respondent organisations have faced legal or regulatory issues that involved third parties, with 50 percent of these involving average costs per incident of £8,000 or more.[1]

Even if the financial penalty can be managed, the reputational impact can have far-reaching consequences for many years.

Third-party risk management is a top concern of compliance leaders, but many organisations are still coming to terms with how best to manage their third parties to limit risk and develop programmes based on organisational risk assessments. The 2016 NAVEX Global benchmark report found that many organisations think they could be doing a better job of third-party risk management. Only 58 percent reported that they do a good job of complying with laws and regulations, and less than 25 percent rate their overall programme as *Good*.[1]

Organisations may be diligent with their ethics and compliance programmes, but for many the risk their third parties represent is a Wild West over which they feel like they have little control.

Benefits of a Strong Third-Party Risk Management Programme

Managing third-party risk can make a big difference in how well your organisation can identify, manage and limit the liability a third party can represent. Your third party's risk is your risk. You should have confidence that your programme is minimising that risk for you and your organisation.

1. NAVEX Global (2016). *2016 Ethics & Compliance Third Party Risk Management Benchmark Report.*
2. Organisation for Economic Co-operation and Development (2014). *OECD Foreign Bribery Report: An Analysis of the Crime or Bribery of Foreign Public Officials.*

Having a strong third-party risk management programme—including continuous screening, monitoring and risk mitigation of third-party relationships across the enterprise—can help your organisation in multiple ways.

- **Avoid Fines, Regulatory Enforcement Action & Legal Costs**
  A strong third-party risk management programme helps your organisation avoid legal action and fines. But it may also reduce penalties and mitigate regulatory action. Notably, in the U.S. the SEC declined to pursue charges against Harris Corporation for FCPA violations related to the actions of a subsidiary party because of its strong compliance and FCPA due diligence programme. This result demonstrates that the U.S. government may temper regulatory actions against organisations that can show that they invest in and take self-directed action to aggressively limit their FCPA and third-party risks. This stance may eventually make its way to Europe as well.
- **Promote Your Organisation's Culture**
  The FCPA advises that organisations must demonstrate that they are promoting their culture of ethical and responsible behaviour both internally and with their third parties. A clear pathway to accomplish this is through requiring your third parties to understand and abide by your Code of Conduct, attend your third-party ethics and compliance training, and attest to your policies through a policy management solution.
- **Produce a More Accurate Picture of Risk**
  A comprehensive third-party risk management programme—integrated with your ethics and compliance activities across the enterprise—can provide holistic data on where the organisation is most exposed to risk and where it is well-protected. This kind of insight not only is helpful in making training, policy and hiring decisions but also can point to where immediate action may be needed and resources should be allocated.
- **Promote Continuity**
  Disruptions in third-party relationships can be detrimental to the continuity of business practices. Third-party failures can result in legal or regulatory actions that require significant disruption and resources to resolve. In the worst cases, third-party failures can threaten the viability of the organisations with which they are engaged.
- **Protect the Organisation's Reputation**
  As we see in many high-profile cases, a single third-party failure can deeply affect the organisation's trust and relationship with its clients and customers. Ensure that your organisation will be thriving for many years to come by ensuring that you are working with vetted third parties.

In 2016 only **22%** of U.S. companies monitored all of their third-party relationships.

NAVEX Global 2016 Third Party Risk Management Benchmark Report

One Size Does Not Fit All

Many compliance programme leaders worry that they don't know where to start on a third-party compliance program. The good news is that organisations do not need legions of compliance personnel and unlimited budgets to meet the standards recently outlined in a Resource Guide to the U.S. Foreign Corrupt Practices Act (FCPA Guidance) provided by the US Department of Justice and the SEC.

As reliance on third parties continues to grow, so does concern about the number of headline stories depicting regulatory action and reputational damage arising from third-party actions. These are driving many organisations to reconsider how they approach the identification and management of the risks posed by third-parties.[4]

Deloitte *Third Party Governance and Risk Management Report*

A risk-based approach to third-party risk management involves aligning your third-party risk profile with your organisational risk profile and building a programme that optimises both.

FCPA Guidance makes it clear that a risk-based due diligence process will be considered when assessing the effectiveness of a company's compliance programme. Fortunately, it says "the degree of appropriate due diligence may vary based on industry, country, size and nature of the [third-party] transaction, and [the] historical relationship with the third party."[3] So one size doesn't have to fit all—that is, your organisation can build a programme commensurate with your level of third-party risk.

The obligation is on your organisation's leaders to make sure that they understand the qualifications and responsibilities of the third parties your organisation engages. FCPA Guidance states that "the degree of scrutiny should increase as red flags surface."[3]

Almost every organisation has some elements of an effective third-party compliance programme. In the next sections, we provide recommendations and templates for identifying what you already have, determining what you need to develop to best address your gaps, and developing plans and implementing the right strategy for your organisation.

3. U.S. Department of Justice (2012). *A Resource Guide to the U.S. Foreign Corrupt Practices Act.*
4. Deloitte (2016). *Third Party Governance & Risk Management: Addressing the Challenges of Decentralisation.*

PLAN

Define Your Goals & Create a Strategy

Whether your organisation engages with a handful of local consulting firms or thousands of manufacturers around the world, those engagements are relevant to your organisation and their failure could affect your organisation's ability to function effectively. The third-party universe is multidimensional, often with complexities that can surprise even the most sophisticated organisations and leadership.

This section explains how to set up a standard process for third-party risk management—from initial identification of third parties to your due diligence process and continuous third-party monitoring.

Critical Components to Include in Planning

Top-down support. Before, during and after a due diligence programme is implemented, it is critical to have the full support of senior executives and the board of directors. Your programme needs to be structured to work with your managers and executives to help them partner with responsible, professional companies. Your organisation's leadership should regularly communicate about the third-party programme, making clear to everyone in the organisation that relationships with third parties will be subject to risk-based due diligence to mitigate potential corruption risks.

A unified approach. There may be multiple divisions and locations within the organisation that engage with and manage third-party relationships. It is critical that all key stakeholders, including those on the front lines of engaging with third parties, are aligned to use the same third-party relationship management systems, including the risk management solutions you pursue. A siloed approach can greatly increase an organisation's exposure to risk if, for example, your procurement department is unaware of information uncovered by your compliance department related to a third party. A key component for ensuring programme consistency is a distributed automated system.

Automated, continuous monitoring. Manual third-party screening and monitoring processes—or an approach to monitoring some but not all vendors and third parties—is no longer a viable approach

BEST PRACTICE:

Use a Standard Process

Identify and prioritise. Identify your universe of relationships and prioritise them by risk.

Assess. Conduct due diligence on a risk-adjusted basis to uncover and assess risks.

Mitigate. Take steps to mitigate any risk that was uncovered.

Monitor. Conduct continuous monitoring to keep third-party information current and to ensure that policy compliance is in force.

to effective risk mitigation. You will never be able to predict whether any particular third party you work with will engage in unethical behaviour. Instead a systematic, holistic and rigorous approach to due diligence must be in place to ensure that your company is kept informed and the right information is delivered when an issue arises.

Adequate resources. Everyone deals with capacity, resources and budget issues. Beyond the time and costs involved in the initial screening of third parties, there are additional costs to keep in mind as you set up your programme. Consider the operational and business costs related to:

- The frequency of ongoing monitoring, which is determined by your risk profile and your third-party risk profile
- The number of third parties to monitor—and which ones you need to monitor more often than others and why
- Your contingency plans for when a third party fails—how to disengage and limit repercussions
- To what level you'd need to disengage. Would it require full disassociation or partial? Would it have an impact on all business units or only on those directly affected?
- The specific assurances you need to reengage with a failed third party and how long the reengagement process would take
- Your expected costs in terms of lost productivity, downtime, open time of the relationship, and rescreening, reengagement or finding a replacement vendor when a failure occurs
- Effective, automated solutions that can save on resources (including full-time employees), increase productivity and drive down operational costs

Third-party due diligence vendors can help you make a compelling business case if you are facing internal resistance to assigning adequate resources to this programme.

Appropriate translation and cultural outreach. Many high-risk third parties reside in emerging markets where English is not the native language. In many cases third parties find the scrutiny of the due diligence process to be both high stakes and confusing, especially when the information being communicated is not in the third party's local language. Providing notifications, instructions and interview questions in the third party's local language can make the third party more comfortable with the process and help answer important questions, such as *Why is the process important?* and *How will our information be used?*

Third-party training. Organisations should consider, where appropriate, extending organisational compliance training (especially on codes of conduct) and policy attestation (available in NAVEX Global's PolicyTech® solution) to their agents, contractors and suppliers. Decisions about when and in what form to offer training support should reflect the third party's risk profile and the degree of corruption risk in the relationship. A top-tier ethics and compliance training programme offers customisable training for third parties and can be easily added to your ongoing compliance training.

Identify Your Third Parties

The landscape of business partners continues to expand in breadth and complexity for most organisations. As organisations look to grow, there is an abundance of third parties with deep expertise and broad capabilities that can extend the organisation's ability to succeed. When faced with a build or outsource decision, trends show that many organisations opt to work with trusted third parties to

take on processes they lack the resources to accomplish on their own. These days many organisations are actively expanding their business capabilities through their third-party engagements, with or without a risk-based third-party risk management programme in place.

Your immediate supply chain and distribution channels represent direct relationships between your organisation and the third party, yet it is increasingly common these days to see your direct third parties engaging on your behalf with outside specialty consultants, agents and contractors with whom your organisation has no direct relationship. When your third parties have a network of indirect third parties—sometimes called fourth parties—they need attention, too.

The Landscape of Business Partners

Source: NAVEX Global

Your Third-Party Risk Profile

After identifying your universe of third parties, it is important to be forthright about the implications of your engagements for your organisation's success. This means not only defining the depth and breadth of your third party engagements but also understanding the costs of your programme's success or failure. It means defining measures of success and planning for all the possible programme limitations.

Evaluate your risks by defining the following:

- The regulatory environment and industry in which your organisation operates
- The number of third parties with which your organisation engages
- The number of those third parties that are critical to your business
- The types of third parties with whom you are working (suppliers, resellers, distributors, manufacturers) and where they are located
- The financial and reputational risks to your organisation

When assessing your position, consider the regulatory environment in which your organisation and your third parties operate. Some industries are more regulated than others, and some types of third-party engagements draw more legal and regulatory attention. To best protect your third-party programme and your organisation, start by knowing the threats and opportunities present in the environment in which you operate.

The number of third parties with which your organisation engages is one indicator of your level of risk. It can help you define your challenges—much more so than the size of your organisation in terms of employees or revenue. In fact, the proportion of third parties to your organisation size is a clearer indication of your risk level than total numbers. For example, there are global manufacturing firms that facilitate manufacturing through large third-party networks while directly employing very few staff, and there are huge multinationals that work with very few third parties.

Part of your risk profile is defined by how deeply your third parties are integrated into your organisation.

BEST PRACTICE:

When to Conduct Due Diligence

The best practice is to conduct due diligence *before* entering into a new business relationship with a third party. Organisations should also ensure that their current third-party relationships do not pose significant corruption risks. To do this, organisations may decide to perform a general review of their existing third parties, using a list of key risk factors to identify those that may be high risk, and develop appropriate mitigating plans in the context of existing contractual agreements.

When considering how many of your third parties are critical to your business performance, keep in mind how much of an impact it would make if you had to rapidly reduce or ramp up your engagement with a third party or a set of third parties or to disengage from them entirely. While you have the ability to directly manage your organisation's internal ethics and compliance programme, you have less visibility into your third party's programmes—no matter how deeply engaged you are. Therefore the capacity of a third-party's failure to affect your ability to operate is a question of risk.

When reviewing the potential for financial and reputational risk to your organisation, it is important to keep in mind your organisation's ability to adequately manage and mitigate third-party risk. In some cases, the risks of doing business with a third party outweigh the potential benefits. You need to set the criteria for that decision well in advance or define a programme champion who has the authority to veto or approve borderline decisions.

Though it seems cliché, your organisation should objectively evaluate third parties regarding their trustworthiness and the risk they represent to your business. In some cases, factors like geography, industry and line of business might feel good or bad in your gut but require factual analysis to fairly evaluate what's good for your organisation.

There have been many cases in which an organisation becomes misaligned with its actual risk, preferring to go with their gut and place trust in third parties that don't deserve it. Best practices advise screening and monitoring all of your third parties, independent of traditional or assumed risk factors.

The adage *Trust but verify* is apt in terms of third-party risk. Use data, tools and an active third-party risk management programme to define your actual risk.

Define a Third-Party Due Diligence Process

Develop a consistent, structured process for assessing and assigning risk to each third party. While process consistency delivers efficiencies, a risk-based third-party risk management solution requires that you assess each third party based on your relevant risks and the distinct risks the third party represents.

It is helpful to start by looking at all the current pieces of your third-party due diligence process. In many cases, a picture of the process, such as a diagram, is worth a thousand words. Creating a Third-Party Due Diligence Process Map (or tailoring the one on the next page) will help you get your arms around due diligence processes.

Questions to ask:

- Which departments in the organisation complete which tasks?
- Are we duplicating efforts?
- Which components require input from external third parties?
- What approvals are required from whom and at what point in the process?

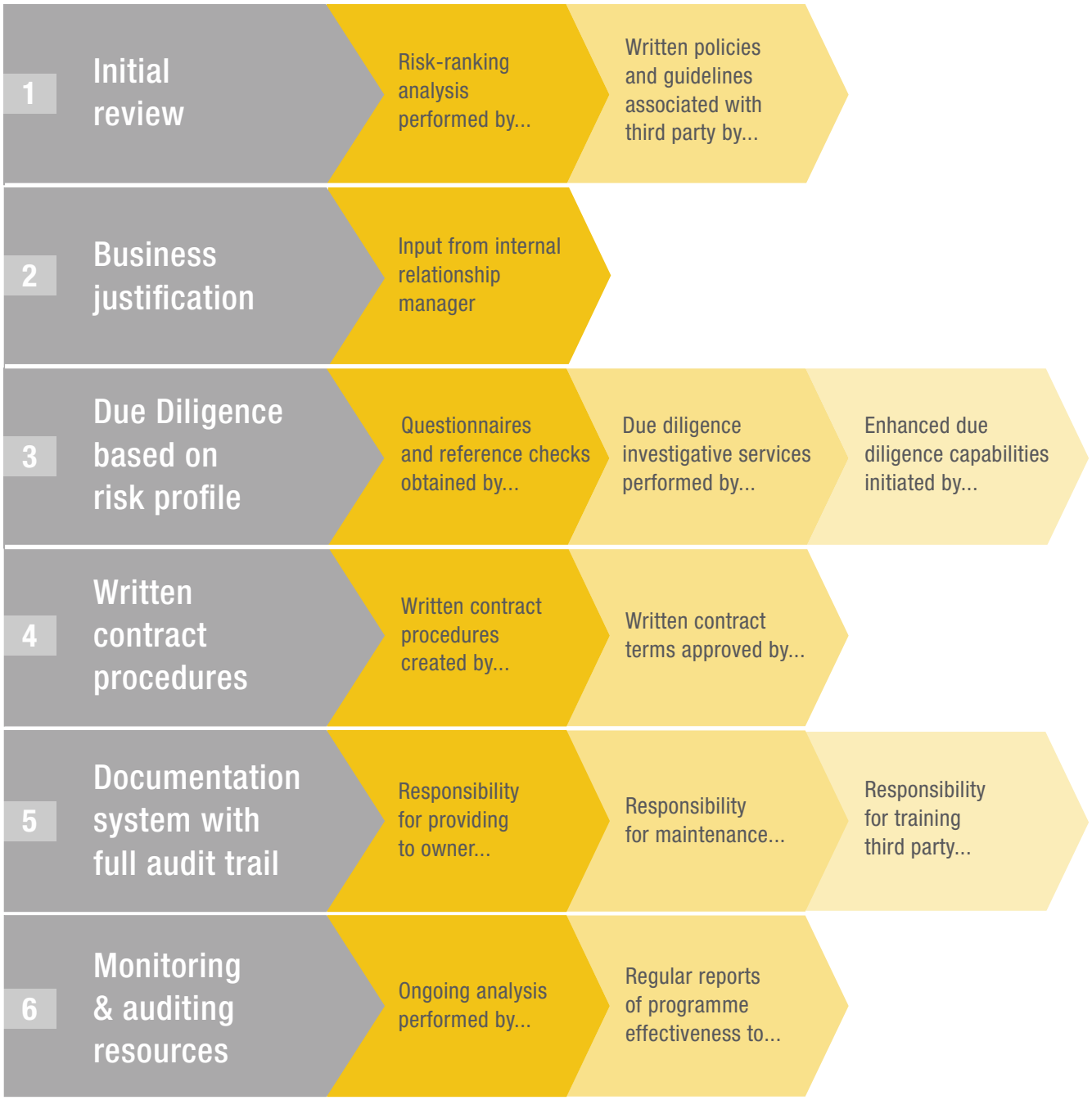
"Under many legal frameworks, organisations may indeed be held liable for acts of corruption by their third parties, i.e., their agents, consultants, suppliers, distributors, joint-venture partners, or any individual or entity that has some form of business relationship with the organisation."[5]

World Economic Forum

Good Practice Guidelines on Conducting Third-Party Due Diligence

5. World Economic Forum (2013). *Good Practice Guidelines on Conducting Third-Party Due Diligence.*

Sample Third-Party Due Diligence Process Map



The following are basic components of a due diligence process to use as a guide. Because a due diligence process should be designed to address your organisation's unique risk profile and operational structure, there is no standard Third-Party Due Diligence Process Map. The yellow arrows at left show examples of how to identify which operational units contribute to which stage.

Identify Elements That Can Be Automated

Use Technology to Streamline Processes

Third-party due diligence providers are increasingly leveraging technology to automate due diligence processes and procedures. The reduced complexity and time and the cost savings are significant. More importantly, automation forces you to set clearly defined standards. Enforcing adherence to those standards in turn helps organisations avoid bias and error.

Identify processes that could be automated by considering the following questions:

- What third-party due diligence processes require input from multiple people, such as approval by a committee?
- What third-party due diligence processes require information from external parties, such as questionnaires from potential business partners?
- How are updates conducted, such as checking third-party business partners against watch lists, politically exposed persons databases, and other resources?

Additional areas to consider for automation are organising and archiving documents; certification of acceptance of policies (using an automated policy management system such as NAVEX Global's PolicyTech® policy and procedure management software); data collection from potential third-party business partners; and document access (taking your processes off email). Use your Third-Party Due Diligence Process Map to think about each component of your current approach step by step.

Who Should "Own" the Third-Party Risk Management Programme?

Planning and implementing the third-party risk management programme should be a collaborative and inclusive process that involves representation from a number of departments, including compliance, legal, human resources, internal audit, security, risk management, procurement and IT. Stakeholders need to partner to ensure that the programme is implemented smoothly and that all departments effectively get what they need from the programme.

According to best practices, the responsibility of the risk assessment and due diligence processes should lie with those in the organisation who are looking to enter into a third-party relationship in consultation with key experts in the organisation—usually the compliance and legal departments. The people responsible for the risk assessment should document the rating process in reasonable detail and renew the assessment periodically (e.g., once every three years).

IMPLEMENT

Manage Your Third-Party Risk Management Programme

Implementing your organisation's third-party risk management programme should follow a continuous process of onboarding, screening, monitoring and life cycle management. Alongside these activities, you should include ongoing communications with management and other key stakeholders about programme processes, successes, performance and anticipated changes.

When you implement your plan, be transparent, communicate well and ensure that all relevant parties are on board. Work closely with your third parties on education and enforcement of your ethics and compliance standards. Informing and training your third parties on your code of conduct and behaviour expectations up front and continuously can protect you and the third party from conduct and compliance breaches throughout the life of the engagement.

Communicate About the Programme

One of the most critical aspects of managing your programme is communicating a clear, written policy about third-party risk management. Make sure that the third-party, procurement and supply-chain policies clearly state the current organisation's third-party policy. Policies should be reviewed regularly, updated as necessary and included in regular compliance training.

An organisation should make clear to managers and employees that any abuse or disregard of the third-party due diligence process may lead to disciplinary action, including termination in appropriate circumstances.

Strong compliance programmes incorporate secure, accessible channels through which employees and third parties can raise concerns and report unethical behaviour without fear of reprisal—most often as a whistleblower, hotline or web reporting programme. Organisations may want to inform third parties about these channels and encourage them to seek advice when questions arise and to report suspected wrongdoing.

Mitigate Risk

Once you have identified and defined your risk-based third-party due diligence processes, make sure you effectively manage your programme toward mitigating risks. This does not mean you must have a fully constructed programme in place before you get started, but it does mean that your objectives, milestones, basic success metrics and fail-safes are set to your risk profile and agreed on by your stakeholders.

Many of the programme initiation elements can be done in-house before engaging any third parties. These initial steps may include defining and sharing objectives, structuring programme parameters, identifying stakeholders and programme champions, putting a management system in place and acquiring a budget, among other items. This initial programme setup may take months to get to the point at which your first third-party onboarding and screening takes place.

Particularly when organisations work within a complex third-party landscape and assurances on programme efficacy are critical, stress-testing your processes and capabilities through a limited early-adopter programme can help ensure programme success and stakeholder confidence.

A structured programme should usher third parties through a set sequence of events that ensure cradle-to-grave process consistency. Your programme should include standardised documentation and

practices managed through a centralised system with a well-defined chain of command for any programme changes, exceptions or enhancements. This ensures that when changes are made, everyone in the organisation can be equally informed of them.

Onboarding & Initial Screening

Develop clear expectations of each third party based on the work to be done. Clearly define individual executives and contacts by name and by role, service-level agreements, performance expectations, specific criteria for termination and who can take actions to pursue termination, and under what conditions other actions should be taken. Though it may be simplest to identify contacts by name, be sure to identify key roles as well, to be prepared for inevitable personnel changes.

Your third-party onboarding processes should be familiar and standardised so that you do not miss any key requirements—and so your third parties can easily move through them. Be sure to include third-party education on your key policies and requirements. Using a policy management solution to acquire third-party attestation to your policies is a best practice.

Every organisation will have a few unique reporting needs or assurances, but the core steps of onboarding a third party, including initial due diligence inquiries, are likely to be similar. Process and document standardization will help you address and include steps that may not be obvious to you when initially defining your onboarding processes.

Though you will define the timeline and your organisation's particular requirements to formally onboard a new third party, at some point you will need to conduct a deeper screening of the third party. Screening can include financial and reputational background checks, multiple internal review channels and multiple experts engaging with and conducting independent research on the third party and its officials. The outcome of a screening process should be an approval, disapproval or deferment of the engagement.

Screening & Monitoring Third Parties

Screening third parties typically involves doing initial and informal research, sending a detailed questionnaire to the third party and scoring the outcomes of their responses, and conducting deeper reputational research.

Though initial internal screening may reveal cursory results and some third parties may be quickly cleared or rejected, we highly recommend conducting deeper screening. With deeper screening, we see two primary levels of research. Keep in mind that beyond your initial screening, similar research and monitoring should continue throughout the life of the engagement.

Standard Screening

At a minimum you should screen against reputational indicators that may be pathways to deeper research and reporting requirements.

- **Adverse Media**
  Look for reports or stories in published media that mention the third-party organisation or its key stakeholders.
- **Sanctions Watch Lists**
  Check governmental reports for organisations on which official sanctions are placed and the reasons for doing so.
- **Politically Exposed Persons**
  Seek resources that reveal the political connections of executives and individuals associated with the third party and their implications.

Financial background checks are also advised because they can reveal details about a third-party organisational's history, performance and business practices. In many cases, financial screenings may inform other screening criteria.

Although organisations may conduct initial third-party research on their own, best practices advise employing outside screening organisations to conduct due diligence research. By doing so you can be confident that the right details are captured and the reporting is consistent.

When selecting a screening organisation, look for an organisation with the following qualities.

1.

Is independent and can deliver unbiased reporting.

2.

Has global reach. Even if your third parties are local, their third parties may not be, and you need to know with whom you are working.

3.

Is reliable and uses reputable sources for their reporting, including adverse media.

4.

Is flexible enough to meet your unique organisational risk-based requirements. Do they deliver data and insights as you need them, or do they force you to dig through data on your own?

5.

Provides filtering capabilities that allow you to see only material risk.

6.

Includes ongoing monitoring, which delivers continuity and consistency in reporting and will alert you to any changes in your current portfolio, allowing for proactive risk management.

7.

Has an option for human analysts to review your information, creating a first line of defense against false positives.

Additional Due Diligence

Though standard screening should capture the vast majority of your reporting requirements, there will be occasions when deeper dives are warranted. Depending on how your risk-based programme defines your third-party assurances, you may find that 10 to 20 percent of your third parties require additional due diligence after standard screenings, before doing business with them.

Organisations should have the freedom to develop multiple filtering frameworks that configure the results of their screening efforts to meet specific risk tolerances, which can differ due to the size and nature of a contract, geography and industry groupings. In essence, you should be able to screen high-risk clients from one jurisdiction against all available data; high-risk clients from another jurisdiction against another subset; and, still further, low-risk clients against a smaller data set. This filtering significantly improves the quality of the alerts returned, substantially enhancing both relevance and materiality for each level of risk.

An aggressive risk-based approach is recommended where there are higher levels of risk. Based on factors such as geographic location, type of third party (e.g., agent), contract value and government interaction, enhanced due diligence can deliver the assurances you need.

When engaging in these higher-risk relationships, it is important to identify beneficial ownership concerns—which can involve multiple layers and complexities—uncover litigation records and conduct interviews of former associates, regulators and partners of the third party. Further, you should identify any possible risk factors, which can range from bribery and corruption to child labor, environmental crimes and human rights violations, to ensure that your bases are covered. An automated system can help you properly stratify your risk and guide the processes that will ensure that proper due diligence reveals any potential risks across the engagement.

Monitoring

According to FCPA Guidance, a guiding principle of third-party due diligence is that "companies should undertake some form of ongoing monitoring of third-party relationships."[3] Continuous monitoring may involve periodic rescreening of existing third parties or rescreening driven by an alert about a change in the third party's status. Things change. With any effective compliance programme, one of the critical factors is regular monitoring and auditing to ensure that you are made aware of anything new that surfaces that might change a risk profile.

Consider:

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

Red Flags & Rejections

When you have a risk-based third-party risk management programme in place, you can continuously assess your third parties against the criteria you've predefined. There will be occasions when your evaluation criteria will result in a third party's receiving a yellow flag or red flag or otherwise being rejected for a business engagement.

When this happens you must have a preexisting, well-defined and agreed-upon process for escalating and resolving the yellow or red flag. An individual within your organisation must decide what to do about the yellow or red flag and be able to support and stand by their decision. It may require the actions of a committee or an escalation up the chain of command to the compliance or legal department. When implementing your programme, be sure that these risk mitigation processes are in place.

A Centralised System

Your organisation's reputation is critical to the growth and profitability of your business. It's not enough to screen and monitor your third parties. You must have a standardised system, including a centralised risk assessment, that evaluates and tracks the due diligence process. This will help you respond efficiently and appropriately to reports and limit the potential liability associated with illegal and unethical conduct.

A damaged reputation will have an impact on sales, limit your ability to grow and to attract and retain top talent, and affect your shareholder value and stock price. Given the extensive array of reputational risks facing companies globally and the perceived cost of monitoring them, the challenge facing organisations is where to start. This requires the ability to conduct risk assessments, manage and adhere to policies, evaluate and track the due diligence process and monitor and report—all from one centralised system.

A sophisticated third-party risk management solution allows your organisation to centrally document every third-party issue, as well as the actions you have taken to investigate each issue; the final disposition of the investigation; and the nature of any disciplinary or other resulting corrective action.

Do You Need to Automate?

The US DOJ and the SEC have already made clear that automation is expected. For example, look at the following language in A Resource Guide to the U.S. Foreign Corrupt Practices Act, issued by the DOJ and the SEC in 2012, regarding gift, meals, entertainment and travel compliance programs.

> "For example, some companies with global operations have created web-based approval processes to review and approve routine gifts, travel, and entertainment involving foreign officials and private customers with clear monetary limits and annual limitations. Many of these systems have built-in flexibility so that senior management, or in-house legal counsel, can be apprised of and, in appropriate circumstances, approve unique requests. These types of systems can be a good way to conserve corporate resources while, if properly implemented, preventing and detecting potential FCPA violations."[3]
>
> *U.S. Department of Justice (2012). A Resource Guide to the U.S. Foreign Corrupt Practices Act, p. 58.*

3. U.S. Department of Justice (2012). *A Resource Guide to the U.S. Foreign Corrupt Practices Act.*

There is little doubt that automation is the future of many third-party due diligence processes. The volume of information available makes it increasingly impossible to stay on top of everything. Complexity, training and information management remain challenges, especially for many organisations facing a lack of resources and processes. One area in which third-party risk management programmes could achieve greater efficiencies when it comes to addressing these kind of concerns is by adopting automation.

Compliance is rapidly embracing automated, technological solutions. In the next five years, every organisation's compliance programme will need to automate key parts of its processes to ensure that they remain effective (with an emphasis on *effectiveness* as defined by DOJ and SEC guidelines).

This underscores the fact that the DOJ and the SEC recognise that different companies require different compliance processes to make their programmes "effective." There is no one-size-fits-all approach. In addition, the DOJ and the SEC are conveying that they expect to see companies integrate technological solutions as they become more effective and feasible.

In evaluating the cost/benefit ratio of automation, consider how much time and money your organisation spends on third-party risk management. Automation allows you to rebalance the equation, trading monetary resources to save time that may be better spent elsewhere.

Questions to ask:

- ☐ How well are we protected from risk related to all of our third parties and vendors—not just a select few?
- ☐ Are our processes being adequately documented so that records can be easily obtained if a government inquiry arose?
- ☐ Do human errors result in a slower or inaccurate process? What is the cost of this over time?
- ☐ Do logistical delays caused by manual processes hinder the speed of business?

Benefits of Automation

An automated approach to third-party due diligence is a critical risk mitigation tool to help employers avoid lawsuits, the dismissal of key personnel, and eliminating a supplier or vendor or receiving a fine from a government agency. The following are three key benefits of automating your third-party risk management screening and monitoring.

- **Efficiency**
  The time from initial interaction with a third party to approval or denied status should be consistent, efficient and uniform across the organisation. People engage with third parties to solve a business problem, and a long delay—due to inconsistent processes, collecting evaluations, paperwork, global distances and time zones—can push the engagement back months or longer, testing patience and allowing the original problem to go unaddressed. An automated programme allows for efficient evaluation timelines, processes, workflows and documentation.

- **Transparency**
  Another key benefit of automation is the comparative review of all third parties affiliated with the organisation. By screening and monitoring the records of all third parties, an organisation can respond to actual risk—not simply react to educated guesses based on instinct. Having access to real-time data gives organisations insight into where their greatest exposures to risk lie and where to take action. A key part of an automated risk-based program is being able to use reporting data to appropriately apply resources to better mitigate risk.

- **Organize & Categorise Your Policies**
  Categorise documents by departments, topics, regulatory guidelines or any other structure you use to delineate access to your documents. As your business changes, simply update the taxonomy or categorisation without breaking folder hierarchies, directories or links.

- **Immediate Notification**
  Another value of an automated monitoring programme is to have 24/7/365 alerts in place. An automated programme can report violations and risks more immediately than people typically can. In some cases, a 12-hour lag in learning about a serious violation is fatal to a company. Automation can enable near-real-time notifications.

MEASURE

Track & Improve Your Programme's Effectiveness

The overall purpose of measuring your third-party risk management programme's effectiveness is to ensure that the programme is meeting its goals and your organisation is well protected from risk.

Measuring effectiveness is often unique to each organisation based on its industry, its geographic location and the type of third parties engaged. There are multiple ways to measure the effectiveness of your programme:

- The scalability of your unified and centralised solution
- The speed and accuracy through which you can onboard new third parties
- The consistency and actionability of your programme reporting
- The time frame and costs associated with remediation of screening and monitoring alerts

Alternatively, you can compare your programme performance with an earlier state through:

- The improved quality of your third-party engagements in terms of the number of red flags you're seeing
- Your ability to more accurately identify third-party characteristics that represent increased risk to your organisation
- Your ability to better manage or mitigate associated risks, including swapping out poorly performing third parties for more responsive partners
- The relative business costs of onboarding, screening, monitoring and life cycle management, as well as the impact of your solution to shorten downtime and reduce the related costs

Beyond that you may be able to demonstrate the value of your solution by contrasting the relative number of and costs associated with legal and regulatory actions that your organisation saw prior to and after putting a well-constructed solution into place.

Ultimately, when you review your programme performance, you must take into account the initial risk assessment you undertook. The risk assessment you pursued when planning your programme can inform your return on investment. When you calculated your risk based on the regulatory environment, the number of third parties with which you engage, their criticality to your organisation and the financial risks your third parties represented, you created a risk score.

That risk score can be contrasted against the goals of a third-party risk management programme and your progress on them. Those goals are:

- Avoid fines, regulatory enforcement action and legal costs
- Promote your organisation's culture
- Produce a more accurate picture of risk
- Promote continuity
- Protect the organisation's reputation

Where your programme helped the organisation avoid fines, improved defensibility and drove programme precision through documented processes, protocols and outcomes, you can link it to a reduced risk score.

Every organisation should have processes in place to monitor the third-party due diligence process; periodically review its suitability, adequacy and effectiveness; and implement improvements where needed to adapt to the changing circumstances of the organisation. In particular, the compliance department should conduct spot checks to ensure that the due diligence process is properly applied and to deter any potential abuse.

If you use a third-party risk management vendor, you will have access to strong reporting tools so that you can effectively detect problems, analyse trends and automate the programme without relying on in-house staffing and reporting. The best, most effective reporting programmes are ones that take advantage of the data and use it to gauge the success of interventions, assess the need for additional training, track trends and evaluate the overall health of third-party relationships.

Benchmarking

To measure overall ethical health, your organisation should benchmark your third-party activity against that of similar organisations. NAVEX Global's *2016 Ethics & Compliance Third Party Risk Management Benchmark Report* provides insight into how almost 400 organisations are funding, staffing and executing their third-party risk management programme. Download the full report at www.navexglobal.com/resources.

CONCLUSION

An effective third-party risk management programme is in your best interest. Not only can you more confidently engage with a growing network of vendors, suppliers, resellers and distributors; but when done effectively, you can have a positive impact on the effectiveness and efficiency of your broad ethics and compliance programme.

NAVEX Global research has shown that organisations pursue strong ethics and compliance programmes for myriad reasons, but at the top is a desire to cultivate and maintain a culture of ethics and respect. A strong third-party risk management solution helps organisations realise that objective through engaging with third parties that abide by codes of conduct, that are transparent and communicative and that you can be proud to do business with.

Effective third-party risk management is an emerging demand as more organisations understand its place in a strong ethics and compliance programme. As this paper has shown, an effective programme requires commitment, focus and structure. You too can better manage your third-party risk. It does not necessarily require a large budget or staff, but you do need to have a programme in place that is reasonable for the level and types of risks your organisation faces in its dealings with third parties.

In the end you want to be able to answer the two questions the government will ask if an investigation is opened:

- What kind of due diligence review did you conduct to identify red flags?
- How did you assess and resolve any red flags relating to the third party?

A strong third-party risk management programme—especially one that offers automation of key tasks—helps your organisation protect its people, reputation and bottom line.

ADDITIONAL RESOURCES

NAVEX Global offers many valuable resources related to your third-party risk management programme. Visit our resource center at www.navexglobal.com/resources to find these tools and more:

- 2016 Ethics & Compliance Third Party Risk Management Benchmark Report
- **White paper:** A Prescriptive Guide to Third Party Risk Management
- **Blog post:** If Things Have to Be Risky for Your Third-Party Risk Management Programme to Be Valuable, You're Doing It Wrong
- **Webinar:** Benchmarking Your Third-Party Risk Management Programme in 2016
- **eBook:** Bribery & anti-Corruption Compliance in UK & Europe

ABOUT NAVEX GLOBAL'S THIRD-PARTY RISK MANAGEMENT SOLUTIONS

RiskRate™ Enterprise Due Diligence

NAVEX Global's RiskRate platform gives you the flexibility to carry out deeper levels of due diligence to meet your unique compliance needs. With multiple report levels, analyst reviews and enhanced investigation options available, you can be confident that your third-party risks are uncovered and mitigated as quickly and efficiently as possible.

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organisations protect their people, reputation and bottom line. Trusted by more than 12,500 clients, our solutions are informed by the largest ethics and compliance community in the world. For more information visit www.navexglobal.com.

NAVEX GLOBAL®
The Ethics and Compliance Experts

AMERICAS

5500 Meadows Road, Suite 500
Lake Oswego, OR 97035
United States of America
info@navexglobal.com
www.navexglobal.com
+1 (866) 297 0224

EMEA + APAC

Boston House, Little Green
Richmond, Surrey TW9 1QE
United Kingdom
info@navexglobal.com
www.navexglobal.co.uk
+44 (0) 20 8939 1650