TRANSPARENCY INTERNATIONAL UK
fighting corruption worldwide

MANAGING THIRD PARTIES

ANTI-BRIBERY GUIDANCE
CHAPTER 12

Transparency International (TI) is the world's leading non-governmental anti-corruption organisation. With more than 100 chapters worldwide, TI has extensive global expertise and understanding of corruption.

Transparency International UK (TI-UK) is the UK chapter of TI. We raise awareness about corruption; advocate legal and regulatory reform at national and international levels; design practical tools for institutions, individuals and companies wishing to combat corruption; and act as a leading centre of anti-corruption expertise in the UK.

Acknowledgements:

We would like to thank DLA Piper, FTI Consulting and the members of the Expert Advisory Committee for advising on the development of the guidance: Andrew Daniels, Anny Tubbs, Fiona Thompson, Harriet Campbell, Julian Glass, Joshua Domb, Sam Millar, Simon Airey, Warwick English and Will White. Special thanks to Jean-Pierre Mean and Moira Andrews.

Editorial:

Editor: Peter van Veen
Editorial staff: Alice Shone, Rory Donaldson
Content author: Peter Wilkinson
Project manager: Rory Donaldson
Publisher: Transparency International UK
Design: 89up, Jonathan Le Marquand, Dominic Kavakeb
Launched: October 2017

Transparency International UK's Global Anti-Bribery Guidance

Best practice for companies operating internationally

This is a guidance section from Transparency International UK's Global Anti-Bribery Guidance. The full guidance is available at **www.antibriberyguidance.org**.

About the Guidance

This flagship guidance presents anti-bribery and corruption best practice for companies, drawing upon expertise from over 120 leading compliance and legal practitioners and Transparency International's extensive global experience.

This free-to-use online portal expands and updates all of TI-UK's Business Integrity guidance over the last decade. This includes our original Adequate Procedures Guidance to the UK Bribery Act; a leading resource for compliance and legal professionals, which has been downloaded over 45,000 times from TI-UK's website. The guidance has been kindly supported by FTI Consulting and DLA Piper.

For each area of practice, we provide a summary, best practice tips, full guidance, and links to further resources. This is a dynamic resource and we will continue to update it with new content and features. If you have anything you would like further guidance on, or other suggestions, please do contact us at businessintegrity@transparency.org.uk

Many companies are facing increased bribery risks as they continue to expand internationally and become increasingly reliant on diffuse supply chains and complex third-party networks. There are also additional risks around stakeholder expectations, a global strengthening of anti-bribery legislation – requiring better internal mechanisms to ensure compliance – and enhanced enforcement.

Companies will always design their own bribery programme according to their particular circumstances but those following this guidance can take reasonable assurance that they are well positioned to counter risks of bribery, comply with anti-bribery legislation in jurisdictions across the world and to act ethically and positively in the markets in which they operate.

Transparency International UK's Business Integrity Programme

The goal of our Business Integrity Programme is to raise anti-corruption standards in the private sector. We aim to ensure that individuals and organisations do not participate in, enable or endorse corruption. Our approach is to engage positively with the private sector, governments and leading anti-corruption initiatives to identify and advocate best practice.

For more information, please visit **http://www.transparency.org.uk/our-work/business-integrity/business-integrity-forum/**

QUICK READ

Third parties can represent a considerable bribery risk for companies. They may not operate to the standards of the company and can be used by corrupt employees as channels for bribery. Intermediaries, in particular, are high risk; many of the largest settled case have involved intermediaries paying bribes to public officials. The guidance found on this web portal abbreviates TI-UK's 2016 full publication: Managing Third Party Risk: Only as Strong as Your Weakest Link.

Key elements

- **Integrate:** Develop and implement a risk based, integrated and consistent approach to anti-bribery management of third parties across the company's operations. Clearly assign responsibilities for each stage of the company's relationship with its third parties.
- **Due Diligence:** Collect, analyse and store relevant information about all your third parties, including their ownership, how they operate, their integrity and anti-corruption standards and any significant bribery and corruption risks.
- **Be systematic:** Apply a comprehensive and consistent approach to registering, conducting due diligence on and appointing third parties and to the management and monitoring of the relationship.
- **Focus on your highest risks:** Based on risk assessments, categorise and segment your third parties by risk. Focus your due diligence and other anti-bribery efforts on the highest risk third parties.
- **Build trust and constructive relationships:** Aim to develop an environment in which integrity can be fostered and bribery countered.

BEST PRACTICE

- **Integrate your approach:** Develop and implement an integrated and consistent approach for managing third parties across the company's operations. Clearly assign responsibilities for third party management and ensure a cross-functional working and risk-based approach.
- **Build trust and constructive relationships with third parties:** Foster positive relationships with third parties and shared goals to enable better understanding and identification of risks.
- **Identify all your third parties:** Identify and register all your third parties and collect, analyse and store relevant information about them, including their ownership, how they operate, their integrity and anti-corruption standards and any significant bribery and corruption risks.
- **Use a risk assessment process for addressing third party risks and ensure the level of resources provided is commensurate with the level of risk:** Use a risk assessment process to identify, segment, mitigate and monitor the risks and risk factors attached to different types of third parties and use this information to design the criteria used in due diligence and to design and/or improve the overall anti-bribery programme.
- **Apply a systematic procedure for engaging third parties:** Adopt a comprehensive and consistent approach to registering, screening and engaging third parties to ensure that engagements are made to desired standards and that procedures are tailored to the different types of identified risks.
- **Carry out an appropriate level of pre-engagement due diligence on third parties:** Carry out due diligence proportionate to risks identified for different types of third parties, with a focus on those of highest risk. Use pre-defined risk criteria to assess individual third parties for inherent risk and vary the level of due diligence accordingly.
- **Use tailored communications and training, together with advice and reporting mechanisms, to manage third party relationships:** Provide tailored communications and training to third party relationship managers and third party employees, commensurate with the level of risk. Provide third parties with access to confidential advice and speak-up channels and follow up any credible reports.
- **Implement rigorous monitoring procedures to deter and detect bribery incidents and breaches of the anti-bribery programme:** Require high risk third parties to self-certify annually that they have complied with the anti-bribery programme. Repeat due diligence periodically for existing third parties. For high risk parties and where there is a significant bribery concern, exercise contractual audit rights.
- **Review and evaluate the effectiveness of the third party anti-bribery programme periodically:** Report on the performance of the anti-bribery third party management programme to the board and senior management periodically, together with recommendations for improvements.
- **Report publicly on your anti-bribery management of third parties:** Provide up-to-date information in an accessible manner to communicate to stakeholders your company's anti-bribery commitment and anti-bribery measures related to third parties.

GUIDANCE

12.1 Introduction

Increasing exposure to third party bribery risk

Third parties and intermediaries in particular are the single greatest area of bribery risks for companies. These risks are growing as companies move into new markets and put ever more of their operations in the hands of third parties. In this dynamic and challenging arena, anti-bribery programmes need to be tested regularly to provide confidence that they are suitable for countering third party risks and are working effectively.

Wide scope of third party bribery risk

It is important to recognise that bribery risks are attached to many kinds of third party relationships. Companies may think that some types of third parties fall outside bribery legislation. In fact, there is no distinction between different types of third parties under the UK Bribery Act or the US Foreign Corrupt Practices Act (FCPA). Under the FCPA, companies have been held liable or put under investigation for improper actions involving various types of third parties.

Although the focus of this guidance is on preventing bribery originated by or arising from lax controls of third parties, there is another significant source of risk: that originating within the company itself. Invariably, interest by companies in third party anti-bribery management centres on risks originating with their associates, but the reality is that the top 10 FCPA settlements have all involved bribery instigated from within companies and channelled through third parties, including through consultants, agents and joint venture partners.

Third parties provisions in UK and US anti-bribery legislation

UK Bribery Act: Section 1 and Section 6 of the Act expressly prohibit bribes made through third parties. Section 7 makes companies liable for bribery intended to benefit them by associated persons, defined as persons who perform services for or on behalf of the company. Section 8 states that the capacity in which such services are performed does not matter, though there is a rebuttable presumption that employees are associated persons.

The US Foreign Corrupt Practices ACT (FCPA): The Act expressly prohibits corrupt payments made through third parties or intermediaries. The fact that a bribe is paid by a third party does not eliminate the potential for criminal or civil FCPA liability. The FCPA expressly states that a company or individual may be held directly liable for bribes paid by a third party if the principal has knowledge of the third party's misconduct. It is unlawful to make a payment to a third party, while “knowing” that all or a portion of the payment will go directly or indirectly to a foreign official. The term “knowing” includes “conscious disregard” and “deliberate ignorance”. Intermediaries may include joint venture partners or

agents. Third parties and intermediaries themselves are also liable for FCPA violations.

A Resource Guide to the U.S. Foreign Corrupt Practices Act (Department of Justice, November 2012), pp. 21-23[1]

12.2 The enabling environment

12.2.1 Organising for anti-bribery management

Integrate your approach

Develop and implement an integrated and consistent approach for managing third parties across the company's operations. Clearly assign responsibilities for third party management and ensure a cross-functional working and risk-based approach, supported by tone from the top.

Managing third party relationships is complex and involves many different functions spread across the company's operations. Misaligned processes and undefined responsibilities can lead to bribery risk. The company should therefore ensure that the anti-bribery programme reaches across the company and is applied to a consistent and required standard.

There are many organisational challenges attached to managing third parties and countering bribery risk. Above all, management and the board may not have a complete picture of the company's activities for countering third party bribery risks and may lack understanding of the risks or fail to give them the required level of attention. A further challenge is integrating the management of bribery risk with other forms of third party risk, such as financial, human rights, data privacy and cybersecurity risks.

[1] https://www.justice.gov/criminal-fraud/fcpa-guidance

[accessed: 20 June 2016].

An integrated approach – examples of good practice

- **Allocate responsibilities:** Give overall responsibility and accountability for third parties to a senior manager and assign clear managerial responsibilities across the company. Business units should have responsibility for managing relationships with third parties and embedding the anti-bribery programme into their activities.
- **Integrate your approach to risk management:** Apply consistent standards, policies and procedures across the organisation, including coherent automated data systems and tools. A central risk management function may be used to guide risk management across the company, including countering bribery in third parties.
- **Involve and empower support functions:** Ensure that functions such as compliance, legal, finance, procurement, internal audit, risk management, security, human resources and corporate affairs are fully appraised of the bribery risks attached to third parties. Clearly communicate their roles in supporting line management and countering bribery in the supply chain and ensure they are adequately resourced to carry this out.
- **Ensure cross-functional working:** Ensure that country and business units and support functions work together. This will involve integrating the approach to managing risks attached to other issue areas within compliance and sustainability.
- **Guide local decision-making:** Ensure there is local application of third party anti-bribery measures. Local management know the local culture and risks and are best able to respond to changing circumstances. At the same time, there will be a balance between central and local management and the company will need to ensure that local management itself is supported to manage risks such as misinterpreting or failing to implement policies and procedures - or even acting improperly. It can do so, for example, through risk-based visits by legal and compliance, enhanced communication for high-risk units and periodic “check-ins”.

12.2.2 Building trust in your relationships

Build trust and constructive relationships with third parties

Foster positive relationships with third parties and shared goals to enable better understanding and identification of risks.

Bribery risk can arise from dysfunctional relationships with third parties, where misaligned objectives and communication gaps can lead to third parties dismissing corporate integrity standards in favour of quicker and cheaper performance. Anti-bribery compliance can easily be seen as a burden by the third party and addressed on a tick-the-box basis, undermining the effectiveness of training, contractual provisions and other controls.

Companies can manage these risks of misunderstanding and compliance fatigue by working to ensure that employees and third parties have agreed on common goals and strive together for excellence and corporate standards of integrity.

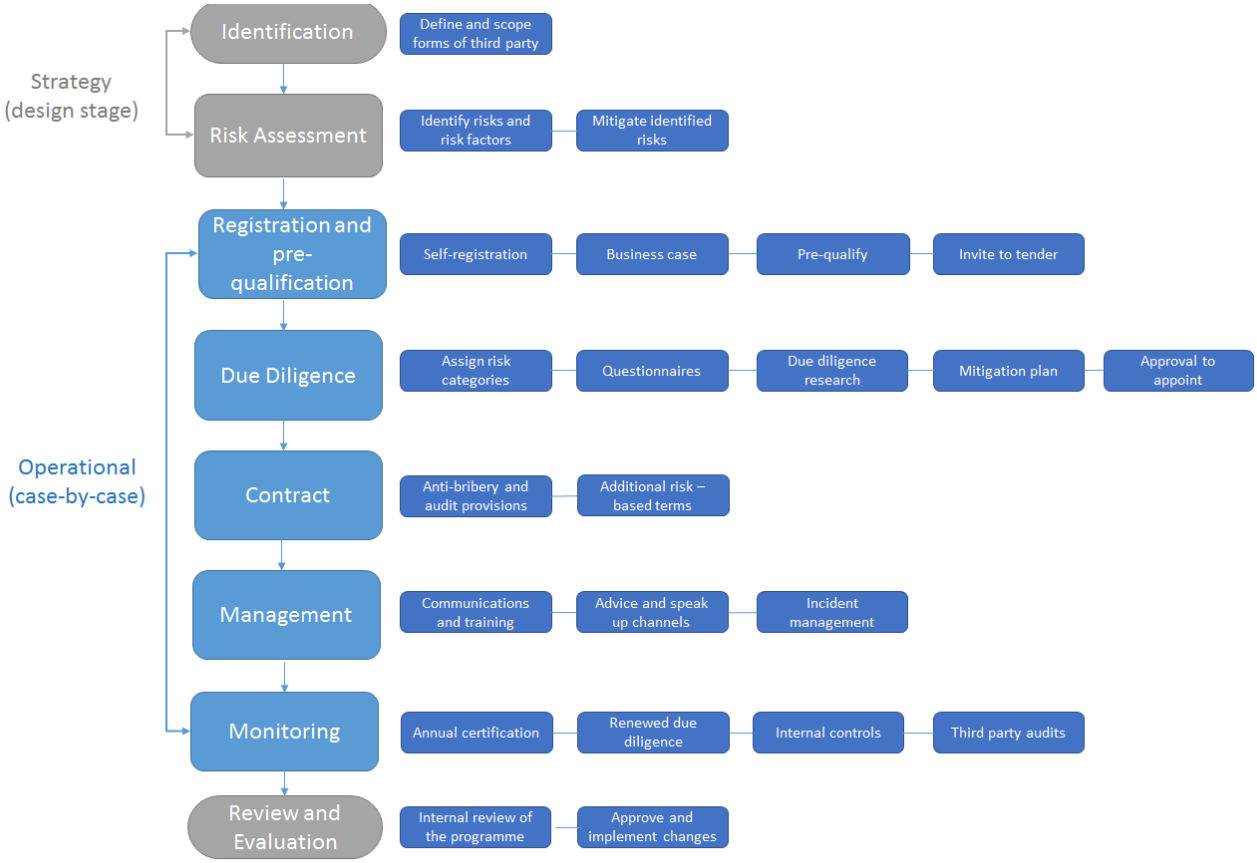
Countering bribery in third parties is more likely to be effective when the company operates positive relationships and builds trust with third parties, aligning objectives and working towards shared goals. Relationship management is a critical tool: the relationship manager is the link between the company and a third party and they should not only manage the contractual aspects but also promote the business value of complying with the company's standards, including the anti-bribery policy.

Building trust – examples of good practice

- **Align your expectations:** Align anti-bribery communications to third parties with wider corporate expectations on integrity, professionalism and quality.
- **Assign formal responsibility:** Give relationship managers formal responsibility in relation to anti-bribery due diligence, training and monitoring of high risk third parties. For example, responsibility can be addressed through job titles, appraisals and performance reviews.
- **Ensure consistency:** Establish initiatives for quality management of integrity and consistency in approach to relationship management. For example, create "ambassadors" or working groups dedicated to anti-bribery third party management and provide tailored anti-bribery resources and training to relationship managers.

12.3 The third party anti-bribery framework

This section sets out seven components that form the core of good practice in third party anti-bribery management: a systematic process for identifying, engaging and managing third parties. This process is outlined in the diagram below:



12.3.1 Identification

Identify all your third parties

Identify and register all your third parties and collect, analyse and store relevant information about them, including their ownership, how they operate, their integrity and anti-corruption standards and any significant bribery and corruption risks.

To achieve effective procedures to counter bribery, the company should have a clear understanding of its third party population. Depending on the size and type of business it conducts, a company may have a handful, hundreds or thousands of third parties and the types of third parties can be homogenous or vary widely.

A third party is any associate with which a company carries out its activities.[2] The company's third party population[3] can include:

- Vendors/suppliers
- Distributors/resellers
- Joint venture partners/consortium partners
- Advisors and consultants (tax, legal, financial, business)
- Service providers (logistics, supply chain management, storage, maintenance, processing)
- Contractors/subcontractors
- Lobbyists
- Marketing and sales agents
- Customs or visa agents
- Other Intermediaries

The highest bribery risk lies with agents, as they are authorised to represent the company. However, bribery risk is also associated with other forms of intermediary, such as lobbyists and law firms. Suppliers can also bring substantial risks, such as bid-rigging and kick-backs.

In order to obtain a high-level view of the risk profile of its third party population, a company should gather basic information on all its third parties, which will be used in the next step of risk assessment. This information gathering step applies to all existing third parties and policies need to be adopted and procedures designed for the systematic gathering of this information for all new third parties.

The information to be gathered includes information about the country in which the third party is based and where the services are provided, the volume of business with the third party and the nature of the work it performs. Categories of work posing higher risks include representing the company before government agencies or other third parties, performing services on behalf of the company and having contacts with government officials.

Identification – examples of good practice

- **Define third parties:** Have a clear understanding and definition of third parties. Label and describe what each type of third party does for the company.
- **Think ahead:** Keep in mind the needs of risk assessment and due diligence, which will rely on an accurate and complete picture of your third party population. Make an initial decision on what information you will need to gather at each stage. This will range from basic data for all third parties to extensive information for the highest risk third parties. Identify what suitable information you already hold.
- **Create a centralised database:** Create a centralised database where all information on third parties will be stored. Ensure enough flexibility to allow for additional categories of information to be added.
- **Plan the process:** Set out a clear process for gathering information and populating the

[2] In this guidance we do not treat subsidiaries as 'third parties' because, as controlled entities, subsidiaries should be subject to the company's anti-bribery programme. See *Business Principles for Countering Bribery* (Transparency International,2013), p.8.

[3] *Good Practice Guidelines on Conducting Third Party Due Diligence* (Geneva: WEF, 2013) contains descriptions of each of the types of third parties listed here.

database. Information can be gathered in various ways, such as accounts payable records, contracts held by legal departments and contracting functions and surveys of operating functions to find out who they see as their third parties and the nature of the relationships.

- **Map out lower tiers:** When describing and categorising your third parties, consider the extent to which they in turn rely on associates to conduct their business. If they are highly dependent on subcontractors, lower tiers in the supply chain or Politically Exposed Persons (PEPs), this will be relevant to the risk assessment process and information on these parties should be recorded.

- **Comply with laws:** Review the requirements of compliance with data and privacy laws for the jurisdictions which you and your third parties may fall under. There may be restrictions on the types of data you are allowed to collect, store or disseminate, or the matter in which you are permitted to do so.

12.3.2 Risk assessment

Use a risk assessment process for addressing third party risks and ensure the level of resources provided is commensurate with the level of risk

Use a risk assessment process to identify, segment, mitigate and monitor the risks and risk factors attached to different types of third parties and use this information to design the criteria used in due diligence and to design and/or improve the overall anti-bribery programme.

A third party risk assessment process allows companies to develop a proportionate approach capable of identifying and responding appropriately to higher risk third parties. It does this by identifying and assessing factors driving third party bribery risk and using this information to devise risk categories based on types of third parties and other pre-defined criteria. These criteria are then used in the due diligence process, described at section 12.3.4.

The results of risk assessments should also be used by management to decide the scale of resources to be allocated to due diligence, third party management and monitoring. Management can also use the results of risk assessments to design the approach to phasing and prioritising types of third parties and other risk factors.

Risk assessments should be repeated periodically to allow senior management and the board to judge what is working effectively, understand emerging risks and make amendments to the anti-bribery programme. As risk assessment is used to design criteria for due diligence, periodic risk assessments may also lead to new due diligence requirements for different forms and risk levels of third party, described at section 12.3.8.

Steps in third party risk assessment

Bribery risk assessment is critical to an effective and efficient third party anti-bribery framework. The key objective is to understand the risk factors associated with different types of third parties in enough detail to allow consistent categorisation and proportionate risk mitigation.

The steps set out below focus on third party risk, drawing upon TI-UK's publication *Diagnosing Bribery Risk* which gives a comprehensive description of anti-bribery risk assessment methodology.

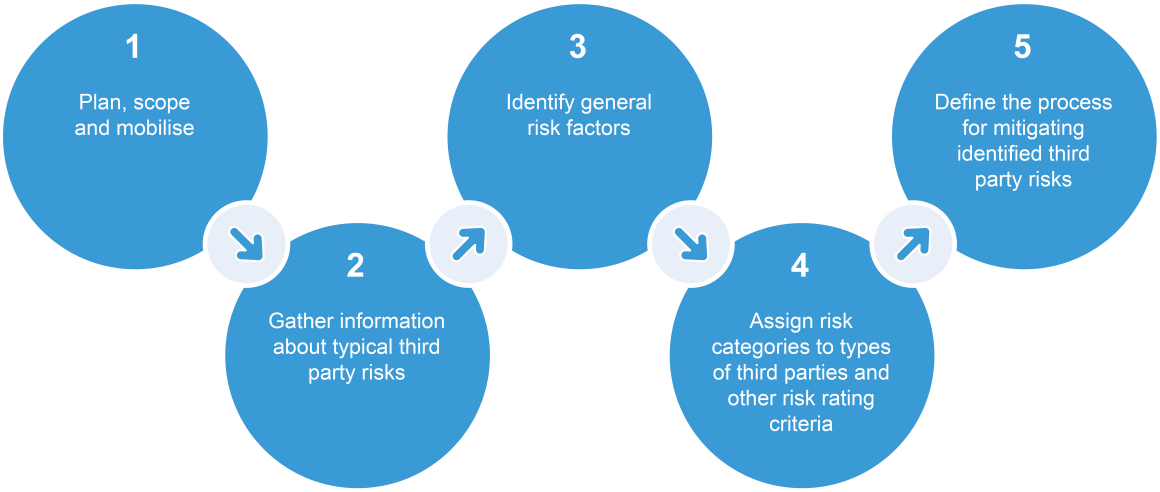


Figure 1: Steps in the third party bribery risk assessment process

Risk assessment step 1 - Plan, scope and mobilise: The methodology and reporting lines for third party bribery risk assessment should be aligned with the risk assessment process for other risk areas (such as sustainability, labour and security). Decisions also have to be made about scope, including the extent to which the process will be applied to lower tier third parties, such as sub-contractors.

Risk assessment step 2 - Gather information about typical third party risks: Obtain sufficient information to form a comprehensive view of the bribery risks related to the types of third parties used by the company (i.e. the ways in which bribery might take place, especially where differing by type of third party). Key information sources are listed in the table below.

Risk assessment - sources of information on risks

- Internal documentation, such as due diligence records, incident reports, whistleblowing reports and audit reports
- Internet research, such as reports of bribery law enforcement
- Company's management and employees, especially those operating locally and those responsible for contracting with and managing relationships with third parties
- Support functions, such as compliance, purchasing and contracting
- Professional advisors and anti-corruption consultants
- The company's third parties
- Trade associations and chambers of commerce, such as reports on sectoral or market corruption issues
- Embassies and High Commissions

In addition, interviews should be held with key third parties, such as major suppliers and contractors operating in high risk jurisdictions and/or sectors, to get perspective on attitudes to due diligence, monitoring and audits, and any cultural considerations related to the subject of bribery and corruption. These interviews should be conducted with the most senior personnel possible at the relevant third party to obtain as informed and complete a view as possible.

Risk assessment - risks and risk factors

A risk is the possibility that an event will occur and adversely affect the achievement of objectives. Third party bribery risk is the risk of offering, paying or receiving a bribe through an intermediary or any third party (individual or corporate) acting on the company's behalf, exposing the company to potential legal and reputational damage.

Some examples of risks posed by third parties are:

- A distributor pays bribes to customs officials to move goods across borders.
- An agent uses part of its fees to bribe procurement officials to award a contract to the company.
- A supplier offers a kick-back to a company employee to award it a contract.

A risk factor is a circumstance, internal or external to the company, which heightens the likelihood of a risk. The difference can be broadly characterised in the questions 'What could go wrong and how might it happen?' and 'Why might it happen and how likely is it to do so?'

Some examples of third party risk factors are:

- Operations in countries with high levels of corruption
- Operations in sectors vulnerable to corruption
- Interaction with public officials
- Provision of critical services
- Dependence on critical licenses to operate
- Reliance on lower tier third parties
- Authorisation to represent the company
- Unusual payment demands, methods or amounts

Risk assessment step 3 – Identify general risk factors: Analyse the information to draw up a comprehensive definition and description of the bribery risk factors attached to the types of third parties used by the company (i.e. the reasons why bribery might be more likely to take place).

For example, the company will want to identify the typical risk factors to which third parties operating in different sectors are exposed. The OECD Foreign Bribery Report of concluded foreign bribery cases identified that two-thirds of the cases occurred in four sectors: extractive (19 per cent), construction (15 per cent), transportation and storage (15 per cent) and information and communication (10 per cent),

although this does not mean that a company in sectors other than those listed will not have a high level of risk.[4] The table below illustrates some sector-specific risks and risk factors:

Risk assessment step 4 - Assign risk categories to different types of third parties and other risk criteria: This step links the general risk assessment process with the due diligence process for assessing individual third parties, described at section 12.3.4.

Allocate each type of third party used by the company to a risk category, based on the typical risk factors associated with this type of third party. The most common framework is to use three levels of risk - high, medium and low – but companies may decide this framework does not work for them. The numbers allocated to each category will vary significantly by sector and by company. Keep in mind that the approach is to stratify third parties to focus attention on those of highest risk. This means keeping an eye on the numbers in the high risk category to make sure they are manageable given the dedicated amount of resources.

Decide whether additional risk criteria are required for the due diligence process to identify high risk third parties. Depending on the typical bribery risks identified for the company's sector and business model, this may include criteria to identify a range of different issues; such as whether the third party has links with local government, whether the proposed relationship includes a long-term and exclusive contract, whether the type of service to be provided will involve extensive and unsupervised interaction with public officials or whether the payment method or amount is unusual.

Risk assessment step 5 – Define the process for mitigating identified third party risks: Once the company's third party bribery risk profile is understood, the company should decide how it can best mitigate these risks, including by tailoring actions for certain types of third parties and for specific risk factors.

This process starts with the design of the third party anti-bribery framework (described at sections 12.3.1 to 12.3.8). A critical first step is to define the methodology for due diligence, working up from the risk categories for types of third parties and any additional risk criteria for risk rating individual third parties (described at section 12.3.4). Depending on the risks identified, the company may decide to take additional actions.

For instance, as a result of identifying new or changed third party risks the company could enhance its enabling environment (described at sections 12.2.1 to 12.2.2). This could include a range of different activities; such as new communications with a greater focus on certain risk factors, introducing enhanced cross-functional monitoring of certain types of high risk third parties or providing additional support for managing relationships with third parties used in certain markets.

The company may decide to eliminate or reduce the use of certain high risk parties, such as agents and consultants, with special approval processes where they are required by local laws. Companies may also reduce the number of third parties they have to improve oversight and manage risks more effectively. Care needs to be taken to manage the impact of such rationalisation on other strategic objectives, such as by monitoring for disproportionate impact on smaller or local suppliers.

Some risks may require additional mitigation through action external to the company, such as collective action or working with governments or intergovernmental bodies.

[4] OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials (OECD, 2014), p.8.

Risk assessment – examples of good practice

- **Focus on high risks:** Focus your efforts and resources on identifying and mitigating the inherently highest risks. This may require, for example, devoting more human resources and budget to gathering information on identifying risk factors in high risk locations, sectors or relationships, and seeking external help where the company itself is unable to gather the necessary information to make an assessment of risk factors and best mitigating responses to risks.
- **Take a comprehensive approach:** Ensure a unified approach across operations with cross-functional working, avoiding silos.
- **Integrate your approach:** Align the risk assessment process with those for other issue areas. This can be achieved through inter-company exchanges between different risk owners, or through a central risk function that sets standards and processes.
- **Stay alert:** Avoid falling into habits of routine or rote approaches to risk assessments and being blind to the real or emerging risks. Use checks and validation methodologies to identify emerging issues such as risk scenario modelling, brainstorming, forensic data analysis, statistical quality control and the expertise of employees. Proactively identify new sources of information on the various risk factors.
- **Be open-minded:** Have an open mind about high risk types of third parties. For example, in a 2010 action under the FCPA, six oil and gas companies had to pay a total of US$236.5 million in fines for bribes made on their behalf by their freight forwarder (Panalpina) and for falsely recording the payments as legitimate business expenses.[5] Years ago, freight forwarders may have been seen as low risk. Today, they are commonly subject to heightened due diligence and monitoring procedures.
- **Gain buy-in:** Build the commitment of employees and third parties to the risk assessment process by involving them in its development and through communication and training.
- **Document the process:** Document the risk assessment. This will help guide further risk assessments and will be important for audits and for investigation of incidents. It will also serve as evidence of the adequacy of the process for regulatory investigations.

12.3.3 Registration and pre-qualification

Apply a systematic procedure for engaging third parties

Adopt a comprehensive and consistent approach to registering, screening and engaging third parties to ensure that engagements are made to desired standards and that procedures are tailored to the different types of identified risks.

Bribery risk can arise from third parties being engaged through variable and incomplete processes, leaving the company unable to apply efficient and appropriate controls due to silo working and unreliable standards. Specific risks range from company procedures being undermined by local work-arounds for urgent requirements to deliberate falsification of third party documentation.

[5] https://www.justice.gov/opa/pr/oil-services-companies-and-freight-forwarding-company-agree-resolve-foreign-bribery [accessed 22 June 2016].

To mitigate these risks, a company should devise a policy and procedures to be followed in advance of entering into any future business relationships. These should describe the steps that employees must follow when engaging with third parties, including renewal of such engagements, and should be consistently applied across the entire organization. The policy and procedures may include: a definition of third parties and other relevant terminology (e.g. PEPs, public officials) and relevant examples; a description of the onboarding process; guidance on the responsibilities of different departments, including for approvals/sign-offs; and information on monitoring requirements.

Consistent registration of all potential third parties is the first stage in ensuring that the company is associated only with third parties that meet required standards, including those for integrity and no toleration of bribery. Though beyond the scope of this guidance, general procurement policies and controls can provide an initial basis for building bribery-specific procedures for engaging third parties.

The process outlined in this section relates specifically to new third parties. However, existing third parties also need to be brought in line with the company's standards and the process can be adapted for this purpose, described at section 12.3.7.3.

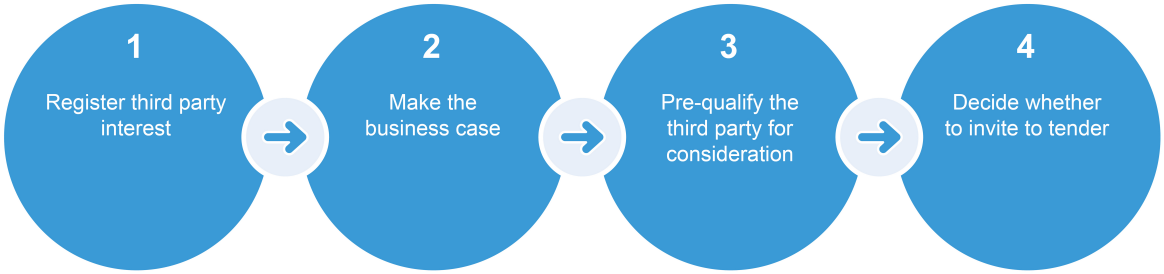


Figure 2: Steps in the registration process

Registration step 1 - Register third party interest: This is the initial point at which a potential third party is recorded in the company's system. It can be an unsolicited online registration by a company wishing to record its interest in becoming a third party or when the company invites a third party to tender. The purpose is to identify and record basic information on those who have or might have a relationship with the company. The registration webpage can also provide a point at which the company first communicates its expectations of third parties.

Registration step 2 - Make the business case: Before inviting companies to bid for a contractual relationship, a business justification is approved by management, with counter signatures and approval thresholds. Any known risks might be highlighted at this point. This stage may not be necessary for third parties being considered for low value, low risk contracts.

Managers should ask questions to challenge the business case put forward and determine the process by which the third party was selected to identify any early risks. For example:

- What is the nature of the services to be provided?
- Is there an alternative to using an external third party?
- Is there already an approved third party that provides the same type of service in the jurisdiction?
- Who introduced the third party to the company?

Registration step 3 - Pre-qualify third party for consideration: Potential third parties are required to provide basic information to allow the company to assess their suitability for being considered further. The majority of this information will relate to the company's general procurement procedure but some aspects will be directly relevant to bribery risk management. Typically the company will require the

potential third party to complete a Pre-qualification Questionnaire (PQQ), covering basic information such as:

- Financial information
- Ownership, directors and officers
- Summary of credentials and capabilities
- Any required certifications or third party attestations, for example related to information security, environmental performance and anti-bribery systems (such as certification under the forthcoming ISO 37001)
- Any past litigation or public administrative sanctions against the company or management, including any related to corruption

If satisfactory information is supplied, the third party is recorded as suitable for invitation to bid but not yet approved for engagement. If the third party proceeds to the due diligence stage then this may involve requests for further information (the overlap between pre-qualification and due diligence is described at section 12.3.4, step 2).

The company may choose to rely on external providers for some of the pre-screening information. For instance, Supplier Ethical Data Exchange (Sedex) is a not-for-profit organisation that gathers data on suppliers globally on sustainability issues and gathers information using extensive questions on business ethics which are completed by suppliers and validated by Sedex audits.[6]

Registration step 4 – Decide whether to invite to tender: Data from the PQQ is evaluated for quality and accuracy before entering into discussion with the third party or inviting bids. Medium and high risk third parties and companies tendering for a large contract may need to satisfy some preliminary due diligence before they can be invited to tender. The due diligence process is described in detail at section 0.

12.3.4 Due diligence

Carry out an appropriate level of pre-engagement due diligence on third parties and repeat periodically

Carry out due diligence proportionate to the risks identified for different types of third parties, with a focus on those of highest risk. Use pre-defined risk criteria to assess individual third parties for inherent risk and vary the level of due diligence accordingly.

Due diligence screens third parties for red flags to enable the company to avoid association with third parties which could lead to reputational damage or legal liability. It is a systematic, periodic process carried out when entering into or renewing a contract or agreement with a third party. It commonly receives the greatest attention in countering bribery in third parties.

[6] http://www.sedexglobal.com/
[accessed 22 June 2016].

Even so, companies struggle to design and implement an effective due diligence process due to large numbers of third parties, variations in their forms and activities, the multiplicity of risks and uncertainty on how best to assess risks.

The due diligence process

Companies must find a suitable methodology for screening their third parties to ensure they obtain the right information to discover red flags and assess the level of integrity and compliance of a third party against consistent criteria. While focused on identifying high risk third parties, the due diligence methodology should be capable of managing large numbers of third parties within the available resources and without disproportionate time and effort for the majority of low risk third parties.

The company can reach a deeper level of understanding of higher risk third parties through a deeper level of diligence. Depending on the circumstances, this may include in-person meetings with senior officials of the third party, a site visit, obtaining information on the third party and principals from specialised databases and engagement of in-country experts to provide additional due diligence. If a decision is made to proceed with the third party, the engagement should be commensurately controlled and monitored, as described at sections 12.3.6 and 12.3.7.

The methodology should be built on the results of the company's third party bribery risk assessment, making use of the risk categories for types of third parties and other bribery risk factors to structure decision-making for individual third parties (described at section 12.3.2, steps 4 and 5). These pre-defined risk criteria allow the company to assess individual third parties for inherent risk and vary the level of due diligence accordingly.

The methodology should also be shaped by the risk approach set by the board and matched against norms for due diligence, including guidance from regulators, professional advisors and anti-corruption initiatives. The company can also learn from past cases and releases by authorities such as the UK Serious Fraud Office, UK Financial Conduct Authority, the US Department of Justice and the US Securities and Exchange Commission.

The methodology suggested in this section can be adapted by companies according to their risk profile and the size and nature of their third party population.

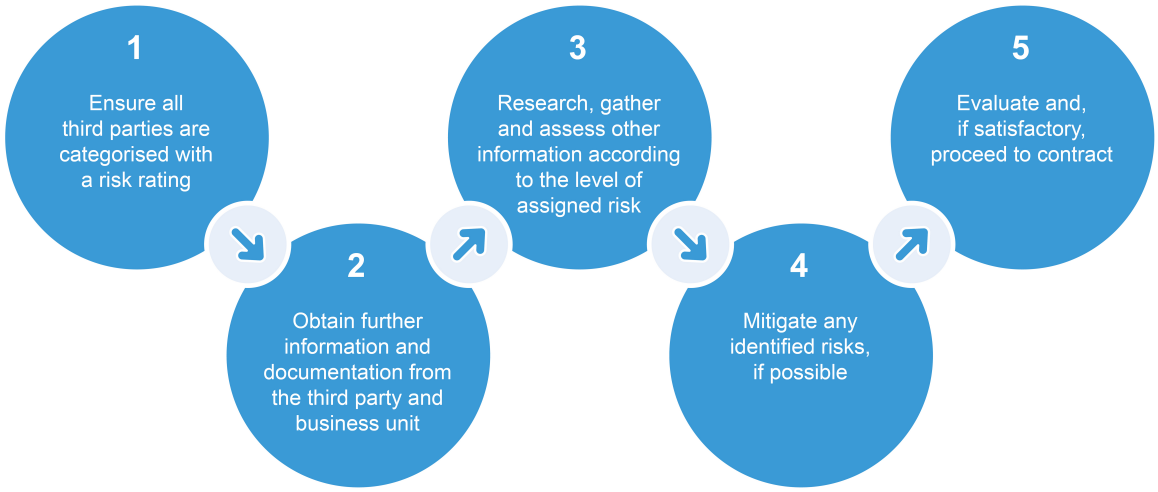


Figure 3: Steps in the due diligence process

Due diligence step 1 - Assign a risk rating: Assign overall risk ratings to third parties by scoring them against pre-defined criteria (developed through the risk assessment process and based on types of third parties and additional risk factors). For example, if using three levels of third party risk, decide in which level the particular third party belongs.

When assigning an overall risk rating to a particular third party, the company will check the type of third party and associated risk category and will also need to look for additional risk factors such as:

- How large is the contract the third party is bidding for?
- Is the contract in question unique/a one-off?
- What is the compensation structure for the third party? (e.g. sales commissions)
- What are the goods or services being provided? (e.g. lobbying, business development)
- How was the third party referred to the company? (e.g. by a public official)
- Does the third party have an anti-bribery programme and does the programme meet the company's own standards?

The overall risk rating assigned to a third party will determine the appropriate level of due diligence. For example:

- **High risk:** This category receives the most attention, with detailed information gathering from the third party and public record research, often supported by market intelligence gathering. This level will often require face-to-face interviews and on-site visits (sometimes called "boots on the ground" due diligence).

- **Medium risk:** This category will typically require some information gathering from the third party additional to the PQQ followed by public record research to verify the information and identify any significant legal, regulatory or reputational issues.

- **Low risk:** This category requires very limited or no further information beyond the initial PQQ. If the relationship owner is aware, either through the PQQ or dealings with the third party, of any issues, this could raise the risk rating to medium risk. Very small contracts or spot purchases up to a specified threshold are not subjected to due diligence unless the PQQ throws up a red flag such as a connection to a foreign public official or past improper behaviour.

- **Sampling:** Due diligence at the level higher than the assigned risk category is carried out on a statistically valid sample of the medium and low risk companies to provide a check that the methodology for assigning risk categories is working.

Due diligence step 2 - Obtain further information: For medium and high risk third parties, further information and documentation is requested using a third party questionnaire and business unit questionnaire. The level of detail of the questionnaires will correspond to the risk category of the third party. Use of an electronic workflow system will enable these and any other communications with the third party to be recorded centrally. It can also serve as a repository for documents provided by the third party, such as a code of conduct, anti-bribery policy or proof of registration. The company should be prepared for red flags or questions to emerge and to expand the gathering of information accordingly in step 3. Red flags may include obscure ownership structures, resistance to requests for information, negative media coverage and links to senior public officials or other PEPs.

It is important that the due diligence requirements imposed on the third party strike the right balance between the information required and the burden of providing this information. Designing a process that requires a well-resourced in-house compliance department to comply with your requirements will make it too burdensome for small and medium enterprises (SMEs) and local companies where the primary language is different from that of the company, amongst others. Using existing standard forms or establishing them through industry bodies or initiatives may help reduce the burden on third parties. It is also worth noting that in some jurisdictions or sectors general awareness of and engagement with anti-bribery and corruption is very low, which has the effect of disadvantaging local companies competing for business. In these cases, the company may consider investing in education, for example through collective action initiatives, to increase awareness and to create a level playing field in jurisdictions where the company operates.

Due diligence step 3 - Research, gather and assess other information: Based on an analysis of the further information provided by the third party, more comprehensive information is sought through company resources and externally. More information may be collected on areas such as:

- Services being provided
- Corporate information (such as proof of ownership, if not requested or provided previously)
- Members of the third party's leadership and those who will be working with the company
- Governance structure
- References from peer companies
- Litigation/criminal or administrative actions disclosure
- Negative coverage in media
- Code of conduct (if not requested or provided previously)
- Anti-bribery programme including policy and training given to employees
- Adherence /alignment to the company's own policies
- Use of sub-contractors /other third parties (and any related policy documents)
- Appearance on sanctions/debarment lists
- Relationships with government officials including director and staff familial relations with PEPs and government officials and employment of PEPs and PEP-owned companies further down the supply chain

Due diligence step 4 - Mitigate any identified risks: Assess the results of due diligence and proceed to seek management approval if all is satisfactory. For high risk third parties, or where specific red flags have been identified for a medium risk third party (e.g. large or critical contracts, lobbying services), legal and compliance should be involved in the assessment.

Carry out further work to mitigate any significant risks identified or decide not to proceed. Mitigation of deficiencies in an anti-bribery programme can be made before appointment or it may be agreed that they will be implemented immediately after appointment by a set date, with a clear follow up mechanism in place.

Due diligence step 5 – Decide whether to proceed to contract: Subject to any identified risks being mitigated, the due diligence report is signed off by management as satisfactory and the necessary management approval is obtained to proceed to contract with the third party. For difficult decisions or where high residual risks remain, the decision whether or not to engage a third party may be referred to legal and compliance or to a special committee with representatives from legal and compliance.

Due diligence – examples of good practice

- **Do not rely wholly on others:** Do not assume that because a third party is used by a peer company or has been certified by an accredited provider this obviates the need for adequate due diligence. Similarly, when third parties are acquired through M&A, do not rely on previous due diligence or a long pre-existing relationship with the acquisition.
- **Balance and integrate your approach:** Ensure due diligence is balanced and integrated with the other components of anti-bribery management of third parties, such as providing tailored communications and training.
- **Use sampling:** Use quality control sampling to provide reassurance that your methodology works and is picking up the high risks.
- **Allow time:** Finish the due diligence process in good time to give the business relationship holder and/or third party an opportunity to mitigate properly any risks identified.
- **Guide local decision-making:** Include the judgement of those close to the business activity, such as relationship managers, in decisions on the results of due diligence. The local decision responsibility needs to be balanced and the company will need to ensure that there is central functional input of setting and monitoring the standards and application of due diligence and that, based on the level of risk, management approval thresholds and counter signature requirements are in place to provide a compliance check.
- **Avoid over-burdening third parties:** Ensure your due diligence process does not over-burden and therefore lead to the unjustified exclusion of smaller and local third parties.
- **Involve legal and compliance:** Involve legal and compliance in decisions using a risk-based approach. Where risks remain high or for difficult decisions, the decision may be referred to a special committee.
- **Document the process:** In all cases, document the decision-making process to show it is thoughtful and thorough.
- **Make a qualitative assessment:** Make use of the judgement of management and employees such as third party relationship managers and compliance officers - this is critical to effective due diligence. Bribery can often occur in unexpected areas and an automated or 'tick box' approach can only follow established channels or flag trends. The company must remain alert to new risks. Those involved in due diligence on third parties should be encouraged to be challenging, questioning and innovative.
- **Deal with issues:** If due diligence has identified issues, consider appointing an external advisor to conduct further research. The issue may also be raised through a face-to-face meeting with management of the third party and a timetable established for correction or mitigation. Exploration and analysis of the risk area jointly by both sets of management can also eliminate risks. Discussions about bribery risk should be handled carefully as they will be sensitive to the third party and cultural differences may also lead to misunderstanding or offence.

12.3.5 Contract

The contract with the third party is more than an agreement – it is a critical anti-bribery control. It communicates explicitly the company's expectations on anti-bribery and ethical behaviour, establishes rights and specifies anti-bribery requirements and processes for monitoring, reappointment, remediation, termination and exit.

The anti-bribery provisions and rights included in a contract will be determined by the extent of the influence of the company in the relationship. As principal, the company will require contractually that its agents and similar intermediaries conform to its anti-bribery programme, but in other associations (such as suppliers, consortia and joint ventures) the company may have insufficient leverage to insist on conformity to all elements of its anti-bribery programme and may have to rely more heavily on due diligence to ensure ethical behaviour by selecting the right partners. In all cases the company should seek a contractual commitment that the third party will comply with anti-bribery and corruption laws and establish its own controls to prevent and detect breaches of this commitment.

As a key anti-bribery control, contractual clauses may also be used to mitigate specific bribery risks. For example, some companies apply additional provisions for high risk intermediaries interacting with government, including detailed record keeping requirements for meetings with officials and for gifts and hospitality.

Contract – examples of good practice

- **Set anti-bribery terms from the start:** Make the contractual anti-bribery terms known at the start of the appointment/selection process when there is still contention for the award of the contract. A third party is more likely to agree terms when its bid is still under consideration than in the final stages when the appointment is all but ready to go. This also makes it less likely there will be late surprises or sticking points in drafting the agreement.

- **Reference codes, standards and laws:** Consider requiring accordance with leading codes such as Transparency International's Business Principles for Countering Bribery, the ICC Rules of Conduct and anti-bribery certifications (such as the forthcoming ISO 37001). References to laws can also be made such as the UK Bribery Act and the FCPA.

- **Provide model contracts:** Provide those responsible for negotiating contracts with standard contracts and anti-bribery terms supported by a commentary and sound legal analysis. This is to ensure consistency and that anti-bribery terms are not deviated from during the course of negotiation and drafting whether through error, omission or external pressure.

- **Engage internally on contract terms:** Ensure cross functional consultation for the drafting of standard contracts and that management understands the provisions, rights and contractual issues related to key risks including bribery.

- **Extend rights to cover sub-contractors:** If the third party relies heavily on the use of sub-contractors, provide for rights extending to third parties, such as the right to be informed of or approve the appointment of all sub-contractors or to set criteria where a third party engages high-risk sub-contractors, engages with foreign public officials or has a past history of bribery incidents. The company may also require a first tier associate to require its own sub-contractors to conform to the company's anti-bribery requirements. Where a supply chain is deemed high risk and the company has sufficient leverage, it should ensure that it has full visibility over a first tier associate's suppliers. In exceptional cases where the supply chain is tightly integrated, this could include a contractual requirement that, in its own contracts with lower tier third parties, the first tier associate will include audit rights for the company itself or its representatives. In any case, the company should assure itself that the first tier associate has in place and is able to exercise audit rights over its own third parties.

- **Update contract terms:** For long-standing relationships or those arising from acquisitions, do not overlook updating contract terms. For high risk third parties, implement a procedure for regular review of contracts by legal and compliance. Laws and regulations, business environments, needs and other circumstances are ever changing. For instance, the coming into force of the UK Bribery Act meant that many contracts were updated to reflect the Act's provisions. Over time, interpretations in legal cases relating to third parties may need to be reflected in third party contracts.

- **Define the process for responding to potential breaches:** To encourage open discussion of bribery risks, set out clear expectations of how the third party should handle bribery incidents. Depending on the company's leverage, define processes and timetables for the investigation, reporting and remediation of weaknesses in the third-party anti-bribery programme.

- **Create a detailed exit plan:** For significant contracts, prepare a plan on how the company will exit the contract in the event of a breach of the anti-bribery requirements. This is particularly important for joint ventures and consortia where an exit can be complicated.

- **Maintain comprehensive records:** Maintain complete and up-to-date inventory of third party relationships and contracts using an aggregated data system.

12.3.6 Management

Use tailored communications and training, together with advice and reporting mechanisms, to manage third party relationships

Provide tailored communications and training to third party relationship managers and third party employees, commensurate with the level of risk. Provide third parties with access to confidential advice and speak-up channels and follow up any credible reports.

Communications and training

The due diligence process should provide evidence of a satisfactory anti-bribery programme appropriate to a third party's risk profile. Even so, it cannot be certain that a third party's employees will have sufficient understanding and skills or even act in the desired way. Therefore, a company will need to communicate clearly and accessibly to third parties the importance it attaches to countering bribery, the ways it expects third parties' employees to act and how to recognise and deal with particular risks.

Contracts and communication of the code of conduct and expectations for third party business conduct are the platform for conveying the company's anti-bribery requirements of third parties.

> "Education is key. That initial investment of time makes a big difference. We are an iconic company and want to make sure that we do not partner with a potentially damaging third party."
>
> **Interview, senior compliance officer**

Training should be a standard component in the toolkit for third party anti-bribery management and considered a requirement for high risk third parties, however, it is often neglected by companies.

Communications and training should focus on high risk third parties, such as sales agents, but it should not be assumed that large global companies do not need attention. Though they can be expected to have substantive anti-bribery programmes, continuing bribery enforcements involving large companies show that this is not a guarantee of good anti-bribery practice. The employees of large third parties and their sub-contractors may benefit from specialised training and tailored communications when working on behalf of a company.

Communications and training – examples of good practice

- **Take a risk-based approach to training:** For example, use customised and more frequent and face-to-face training (considered more effective) for higher risk levels and remote online training for low level risk, and a hybrid of both approaches for medium level risk.
- **Integrate your messaging:** Position anti-bribery communication and training in the context of corporate standards and processes, other sustainability issues and responsibility commitments. Anti-bribery communications must be precise and prominent among the many corporate communications for the message to get through.
- **Ensure tone from the top:** Involve third party senior management in training and communication as much as possible, such as appearing at the introduction to say a few words.
- **Make it accessible:** Communicate the anti-bribery requirements, guidance and training in local languages and in a style that explains clearly and in a non-legal manner what is expected of associates.
- **Train your employees:** Give regular tailored training for employees who engage with third parties – this should be consistent with identified third party risks and match the messages given to third parties.
- **Integrate employee and third party training:** For some third parties, such as sales agents, match training to that given to employees and consider extending it, through agreement with parties involved, to high risk lower tier subcontractors, such as customs brokers appointed by agents. Where appropriate, involve third parties in employee training sessions or modify in-house training – this can be cost effective.
- **Provide tailored codes of conduct or business conduct guidelines:** For example, publish a dedicated page on the company's website which sets out guidelines for suppliers, subcontractors and other third parties, including standards of conduct and expectations of suppliers in specific issue areas, such as gifts and entertainment and conflicts of interest.[7]

Advice and speak-up channels

Advice channels provide information and answer queries about the anti-bribery programme. Speak-up channels (also called whistleblowing channels, hotlines or helplines) are provided for employees to raise concerns or report instances of bribery. Less commonly, they are made available to business associates.

Companies should consider providing speak-up channels for third parties. Because whistleblowers often suffer from their actions, third party employees may be reluctant to report concerns. They can be encouraged by how well the company handles reports and deals with issues and by explaining

[7] See, for example: http://www.bechtel.com/supplier/ethics/ [accessed 20 June 2016].

confidentiality and protection. Use of an external provider for the speak-up channel may also encourage a third party to report their concerns in the knowledge that the line is being manned by an independent body. To further encourage use of the channels, the company should consider making them available both in English and relevant foreign languages.

Advice and speak-up channels – examples of good practice

- **Encourage third parties to speak up:** Extend internal speak-up channels to third parties.
- **Check for existing channels:** Include the presence of a speak-up process in the third party as a due diligence criterion.
- **Build trust in the process:** Overcome reluctance or concerns about reporting by third parties by building their trust in the procedure for speaking up by. For example, explaining and reminding about legal protections for whistleblowers, using an independent agency and/or reporting on number (not nature) of incidents and number of incidents resolved.
- **Provide training:** If the company provides tailored training for third parties' employees, include discussion of speak-up channels in the course. This will be subject to agreement with the third party as it may be a sensitive topic.
- **Encourage direct reporting:** Make clear that concerns should be raised through the company whether through the relationship manager, compliance manager or the whistleblowing channel.

Incident management

No anti-bribery programme will guarantee that a company will be free of bribery incidents in its supply chain. A procedure is necessary to anticipate and manage incidents promptly, thoroughly and efficiently. Incidents can be revealed through monitoring, audits, whistleblowing (including internal tips from speak-up lines or a report to authorities) and media allegations or by the authorities as a consequence of other investigations. The nature of the incident may vary from a suspicion to a high likelihood that bribery has occurred.

On receiving information or allegation of an incident, management should inform and consult the legal and compliance departments and flag the incident immediately to senior management. All alleged bribery incidents should go through triage to establish their credibility, as well as the scale and severity of the issues involved, which will determine the appropriate level of response. The company should have an internal and external communications and escalation plan and, in the case of a major incident, investors will need to be informed of the potential severity and the actions to be taken.

The company should investigate whether its controls failed and there is a potential exposure under bribery laws. As part of an investigation, the company will likely need to exercise its contractual third party audit rights, protect and review documentation and electronic files and conduct internal and third party interviews. This can involve the use of outside firm with investigatory expertise. If an employee(s) is alleged to have participated in bribery with the third party, the company may need to suspend them as appropriate.

Incident management – examples of good practice

- **Cooperate with the authorities:** Establish a policy and procedure to report to and cooperate fully with the authorities if it is likely that bribery has taken place, managed by your legal department.
- **Decide whether to continue or terminate the relationship:** Decide if the relationship can be continued during the course of the investigation or should be suspended. For example, you may decide to continue the relationship where the third party is a critical partner or the bribery incident is contained to one function of the third party and does not reflect the whole company. If the association is continued, end contact with those involved in the bribery allegations or investigation. The conclusion of a legal case against a company will likely be followed by remedial actions, including change of management and strengthening of the anti-bribery controls. Even so, you may decide to terminate an association with a third party where the conduct in question has been egregious and concerns remain. The decision making process should be thoughtful and documented.
- **Learn from incidents:** Once an incident has been concluded, improve your third party management in the light of any lessons learned.

12.3.7 Monitoring

Implement rigorous monitoring procedures to deter and detect bribery incidents and breaches of the anti-bribery programme

Require high risk third parties to self-certify annually that they have complied with the anti-bribery programme. Repeat due diligence periodically for existing third parties. For high risk parties and where there is a significant bribery concern, exercise contractual audit rights.

Rigorous monitoring procedures act as a deterrent to third parties and to employees contemplating bribery and are a way to bring to light suspicions or incidents of bribery.

A company should regularly collect new information on third parties by requesting updated information directly from them, requiring them to self-certify compliance with the company's anti-bribery programme, conducting renewed due diligence, exercising audit rights and/or using technology to automate some of this process. A detailed account of third party audits is described at section 12.3.7.2.

The results of monitoring will be reported to management regularly and provide information for the company's public reporting on its anti-bribery measures.

Monitoring – examples of good practice

- **Update information:** Ask all third parties to complete an online questionnaire each year updating basic information about their company such as ownership, acquisition and annual reports.
- **Require annual certification:** Require an annual self-certification from a director or the chief executive of high risk third parties that a) their anti-bribery programme is implemented and has been subject to review during the year and b) there have been no bribery incidents. The certification can include a statement on any achievements, developments or issues that could touch upon the implementation of the programme.
- **Renew due diligence:** Subject all contracted third parties to periodic repeat of due diligence as well as on reappointment. For high risk third parties, a timeframe of every two to three years should be considered.
- **Use technology:** For certain types of high risk third party, consider monitoring their risk profile continuously using adverse media or broader data screening technology. Transaction monitoring and date analytics tools can also be used (described at section 0).
- **Showcase achievements:** Encourage third parties to showcase any achievements in countering bribery such as collective action. This builds the relationship and can also provide valuable learning to be applied across your third parties.

Internal controls

Once a contract is in place, the anti-bribery programme's controls need to be applied to all third party relationships, with a focus on those of highest risk. The company's anti-bribery programme will incorporate internal financial and accounting controls, such as approval thresholds, countersignatures and segregation of duties, but these may need to be refined for certain types of third parties to counter identified risks.

Third party transactions should be monitored against the controls during the course of the relationship. Technology systems can help monitor where activities are operating effectively and highlight where transactions or patterns of behaviour are out-of-line. For example, data analytics on procurement patterns can identify suspicious or anomalous payments and radio-frequency identification (RFID) tracking tools can be used to track high value goods and identify incidents of substitution, diversion, counterfeit or theft, activities that are often enabled by bribery.

Internal controls – examples of good practice

- **Check activities against company policies:** Check that activities invoiced conform to the company's policies for hospitality, travel expenses, gifts, donations, sponsorships and "facilitation payments".
- **Scrutinise high-risk expenditure:** Provide additional scrutiny around payments for high risk expense types (including visas, customs, taxes, government certificates, licences, bonuses, commissions, gifts, entertainment, travel, donations, marketing).
- **Test your controls:** Check controls by selecting transactions, making sure that reliable third party documentation is kept and transactions are recorded accurately.

- **Enforce thresholds and countersignatures:** Enforce thresholds and countersignatures for approvals of contracts, payments and transactions.
- **Implement checks and approvals:** Introduce and enforce for accounts receivable write-offs, third party credit terms and the re-purchase of inventory sold to third parties.
- **Limit jurisdictions:** Only make payments in the jurisdictions where the third party is based or operates.
- **Prohibit cash payments:** Do not make cash payments and enforce strong petty cash controls.
- **Segregate duties:** Ensure that no single employee handles every aspect of a relationship with a third party.
- **Check payments against goods and services rendered:** Check that payments are appropriate for the goods and services rendered.
- **Provide supporting documentation:** Ensure invoices for payments are supported by full documentation.

Third party audits

Audit rights are a standard part of agreements with all third parties, yet whether and how to audit third parties is a great concern for many companies. Surveys show that many companies do not exercise audit rights. A 2015 survey by KPMG found that more than half the companies surveyed with right-to-audit clauses did not exercise them (see: Anti-Bribery and Corruption Global Survey 2015 KPMG, 2015, p.3.). Often, rights are only exercised when there is a serious issue with a third party and the relationship is likely to be terminated.

The lack of take up of audit rights often lies in the resources and costs needed to carry out audits, the demands of audits on other issue areas or resistance from third parties to the audits. There are also a number of challenges:

- Third parties can be adept at window dressing, manifesting good practice and telling auditors what they want to hear.
- Auditing first tier companies may be insufficient. First tier associates may channel bribes through sub-contractors or rely on suppliers and intermediaries for services where bribery is systemic such as in logistics or obtaining licenses.
- A satisfactory result does not guarantee integrity. Lessons can be drawn from heavily audited issue areas such as labour or safety where major incidents have occurred despite evidence of prior satisfactory audits.

For all this, audit rights are a useful deterrent, clearly signalling to third parties the company's commitment to anti-bribery and corruption. Further, while the main intent may be to heighten the attention that a third party gives to its anti-bribery programme, failure to exercise audit rights may be seen as a deficiency by the authorities in the event of an investigation.

Third party audits – examples of good practice

- **Focus on the highest risks:** Focus third party audits on higher risk third parties but consider auditing a control sample of lower risk third parties selected randomly.
- **Audits as due diligence:** See audits as a continuation of due diligence:
    - Applied consistently, periodically and in a proportionate way to all high risk third parties
    - Carried out on any third party where there is a significant bribery concern
- **Use external auditors:** Engage external auditors to obtain an independent view. They are able to draw on a wide experience of best practice and have greater credibility with stakeholders. They may also be more acceptable to third parties.
- **Consider lower tiers:** Consider relationships with subcontractors and keep in mind that the real risks may lie in the lower tiers.
- **Conduct on-site visits:** Remember that these are an important aspect of audits.
- **Manage the cost:** Lessen the pressure on resources by carrying out audits on a rolling basis spread across time, types of third parties, business units and locations. Using collective industry initiatives where appropriate, such as Sedex, can also lower auditing costs.
- **Counter resistance:** Where a third party provides arguments, delays or hurdles to resist an audit, try to find a workable solution to reassure the third party and enable an audit to take place. For example, a discussion can be held with the owner or chief executive to explain why the audit is needed, how it would take place and respect their concerns about intellectual property or market confidential information. Their interests could be protected by redacting information in reports or using an independent auditor.
- **Develop an audit plan and audit protocols:** Develop these based on your needs, experience and benchmarking best practice. If you use independent auditors they will have a model plan and protocols but you should evaluate these against your own to ensure the approach is suitable for your purposes. Examples can be found in guidance from professional bodies and advisors. An example is the Institute of Internal Auditors' Practice Guide, Auditing Anti-bribery and Anti-corruption Programs.[8]
- **Be consistent:** Apply the same auditing standards across all issue areas. This prevents cherry picking, allows for sharing of best practice and increases confidence in the results of anti-bribery audits.
- **Make use of experience:** Use experienced interviewers and reviewers with knowledge of best practices and ability to recognise red flags.
- **Value substance over form:** When testing transactions the emphasis should be on reaching an understanding of the substance, or business purpose, of a transaction over its legal form.
- **Make connections:** In testing, connect financial to non-financial information.
- **Follow up:** Carry out follow-up interviews or requests as needed to obtain clarification.

[8] Practice Guide: Auditing Anti-bribery and Anti-corruption Programs (IIA, 2014).

Applying the framework to existing third parties

The framework described in the previous sections refers primarily to the process of engaging new third parties. However, once the policy and procedures for third party management have been set, they should also be applied retrospectively to the company's existing third party population. Further, existing third party relationships may need to be reviewed periodically as a result of changes to bribery risk criteria or enhanced anti-bribery programme controls.

Retrospective due diligence

During the identification and risk assessment process, the company will have gathered information on its existing third parties and used this to define categories of risk. The company should then assign a risk rating to each of its existing third parties using the same process described at section 0.

Once it has assigned risk categories to its existing third party population, the company should conduct retrospective due diligence on them. Relationship managers should explain the process to their third parties, issue them with PQQs and questionnaires, identify red flags and hold discussions with their management if and when potential issues are identified. They should communicate all changes to the anti-bribery third party management programme and new expectations and requirements that existing third parties are likely to face upon the renewal of a contract. Where significant issues are identified, mitigation plans should be put in place and, where residual risk is too high, a decision will be taken on whether to renegotiate a contract, terminate a relationship or simply not renew a contract after it expires. This decision should involve legal and compliance and, for difficult decisions, it may be referred to a committee.

The main challenge for the company will be allocating resources. For a company with a large third party population, this will be a major undertaking and it should take a risk-based approach, whereby conducting due diligence and mitigating risks for its highest risk third parties is a top priority and the focus of its resources.

Re-engagement due diligence

Due diligence should be repeated upon re-engagement of all high risk third parties and other third parties depending on the company's risk approach. However, where a third party has already been subject to pre-engagement or renewed due diligence and regular monitoring, it is not necessary to start from scratch. Rather, the company should review information held on the third party to check that it is up-to-date and complete and identify any potential issues or red flags. Where there is missing or inadequate information or the relationship manager has concerns, the company should conduct web searches, hold discussions with the third party's management and request information to address these issues and identify any developments, such as changes to the shareholding or management structure, anti-bribery programme or business model and any allegations, incidents or sanctions involving the third party that have not been reported to the company. These checks should be conducted for all high risk third parties; if significant issues are discovered, the company should consider conducting full due diligence, including "boots-on-the-ground" due diligence, and perhaps engaging an external due diligence provider.

Incorporating results of the risk assessment

Where the company's risk assessment has identified new third party risks that were not previously addressed by the company's third party management programme, or pre-existing risks that were not adequately categorised or mitigated, the company should apply the new due diligence criteria and, where possible, monitoring procedures – including audits – to existing third parties where the risks are highest. This may involve re-negotiating individual contracts.

Applying the framework to existing third parties – examples of good practice

- **Use a phased, risk-based approach:** Where higher bribery risks are associated with certain geographies or lines of business, phase the retrospective due diligence process in line with higher risk company structures and divisions.
- **Align with existing business processes:** For low and medium risk third parties, reduce duplication and improve resource efficiency by aligning retrospective due diligence with existing business processes, such as contract review cycles.

12.4 Public reporting

Report publicly on your anti-bribery management of third parties

Provide up-to-date information in an accessible manner to communicate to stakeholders your company's anti-bribery commitment and anti-bribery measures related to third parties.

Public reporting is a way in which companies can demonstrate to stakeholders that they manage third parties responsibly and have appropriate systems in place to counter risks, including corruption. This reinforces the anti-bribery messages being communicated in other ways by the company to its current and prospective employees and third parties. The business value of reporting should not be overlooked as it can drive reputation, quality, performance and change.

Anti-Corruption Policy for Representatives

> "Microsoft Corporation, and all of its subsidiaries and joint ventures worldwide ('Microsoft'), requires its channel partners (for example, resellers, software advisors, original equipment manufacturers, and distributors), suppliers, vendors, consultants, lobbyists, and any other third-party representative (collectively, 'Microsoft Representatives') to comply with this Policy… Partners are responsible for training all employees who work on behalf of Microsoft. We provide online training free of charge and other resources in the materials to the left."

Microsoft website[9]

Public reporting – examples of good practice

- **Define key content:** Include a description of the anti-bribery programme, risk assessment processes, due diligence processes applied to third parties and the programme's contribution to sustainability. Key content can also include the commitments the company requires from its third parties, such as compliance with anti-corruption laws, a code of conduct, a conflicts of interest policy and a gifts and entertainment policy.
- **Engage with stakeholders:** Learn from stakeholders what they consider to be material and what they want to know about the company. Make this a valuable business process which is acted on rather than a superficial process designed purely for communication.
- **Define materiality:** When deciding what to report, bear in mind that material issues are those that are important to stakeholders and that can impact the company's ability to deliver its strategy.
- **Identify business value:** See reporting as a way to increase value. For example, by reinforcing confidence of investors, communicating key anti-bribery messages and driving quality and performance.
- **Promote tone from the top:** Show the leadership's commitment to no toleration of corruption

[9] https://www.microsoft.com/en-us/legal/compliance/anticorruption/default.aspx?Search=true

through messages and reports on their actions (e.g. site visits).

- **Monitor external expectations:** Monitor and align to the rapidly changing external expectations and regulations for transparency and reporting for both voluntary and mandatory reporting.
- **Integrate communications:** Integrate internal and external communications and reporting as they are mutually reinforcing.
- **Include performance measures:** Use and report on performance measures such as training given, collective action initiatives, availability and use of speak up lines, quality systems used, certifications, third party perceptions of the enterprise's commitment to integrity, contracts terminated, trust of third parties in the company and their understanding of the anti-bribery programme, audits, etc.
- **Tailor reporting:** Provide adapted public reports for your third parties. For example, focused on region, country or nature of relationship.
- **Make it accessible and up-to-date:** Report on third party management in annual reports, sustainability and social reports and dedicated webpages.

12.5 Information management and technology

12.5.1 Documentation

A documentation procedure for third party anti-bribery management is a key aspect of internal controls. It is important for a number of reasons, including:

- **Legal compliance:** In the event of a bribery investigation, the UK authorities will seek evidence of adequate procedures for documentation. Failing to keep adequate documentation is a frequent basis for enforcement under the accounting provisions of the FCPA.
- **Providing an audit or investigation trail:** A full record of transactions will be needed for audits and investigations of a bribery incidents by the authorities.
- **Detection of bribery:** Gaps in documentation, inadequate or falsified books and records of third party transactions are red flags for bribery.
- **Countering bribery:** A strong documentation system can deter bribery.
- **Tracking internal compliance:** Documentation can help track compliance with the anti-bribery programme.
- **Continuous improvement:** Records can provide information to simplify processes or improve controls.

Documentation – examples of good practice

- **Tailor your approach:** Tailor if necessary, the documentation policies and procedures to support third party anti-bribery management.
- **Integrate documentation and workflow:** Integrate the documentation system into the electronic workflow system.
- **Require alignment:** Require the documentation procedures of the third party to match those of your company and monitor their implementation.
- **Record risk assessments and due diligence:** Document fully the risk assessments and due diligence reviews.

- **Clarify accounts codes:** Ensure fully descriptive titles for accounts codes and accurate recording of vulnerable transactions, such as consultancy fees, hospitality, small bribes ('facilitation payments').
- **Maintain meeting records:** Record negotiations and meetings, including any significant informal discussions with third parties especially where they touch upon integrity or ethical behaviour.
- **Tailor retention periods:** For third parties where contracts or relationships extend beyond standard retention periods, consult with the legal department on needs related to anti-bribery and other legislation.

12.5.2 New technology and data management tools

Developments in technology are providing companies access to new sources and an increased amount of supplier data. New technology is speeding up the digitisation of most forms of company information and these are increasingly accessible through electronic means. However, the greatest developments are in the access to information that had hitherto been inaccessible; for example through social media and other forms of big data collection and analysis. This surfeit of data also presents challenges in terms of the technology and the human resources and expertise required to process and analyse the data and turn it into useful information.

The following categories show the various ways that new technology and data management can be used to support the management of third party relationships:

Due diligence on third party relationships

Official and unofficial data sources can be used to gain a more complete overview of a third party's business, directors and management, potential conflicts of interest, relationships with PEPs or other high risk individuals and ultimate beneficial owners. Depending on the perceived risk and availability of information, non-traditional sources including data in other jurisdictions, news aggregators and social media can be considered. Be aware of any local data-privacy restrictions (see "Data Protection Laws" below).

E-procurement systems and vendor management

Technology can also make it easier for third parties to comply with due diligence requirements through the use of self-service portals where the third party can fill in and upload the requisite data and update it periodically. Such systems can greatly reduce the time and cost of preliminary due diligence for both parties. Supporting systems can pick up anomalies in any data entered and raise red flags.

Continuous monitoring of existing relationships

Automation of ongoing monitoring is often overlooked[10] but, if well designed, a good system will pick up exceptions such as any changes of ownership, new allegations or court cases, breaking news stories (positive or negative) and any other information that may be relevant for the ongoing commercial management of the relationship. The level of sophistication of such a monitoring system should be in line with the size of the contractual relationship and the level of perceived risk.

[10] Kroll and Compliance Week, 2015, p.21

Management of existing relationships

Good data management and storage will of course allow for better management of the ongoing relationship. In addition, such systems will be invaluable in the case of any bribery incident or investigation.

Examples of how such a system can be used:

- **Relationship management:** Documenting, analysing and tracking a relationship throughout its course, including contracts, transactions, meetings, negotiations and progress, performance and results, including audits.
- **Compliance:** Tracking compliance with the company's anti-bribery programme using key indicators for internal controls, red flags and non-compliance.
- **Audit trail:** Providing accessible records that can be used as evidence in the event of investigations by auditors or the authorities.

Data accessibility

Information can be processed centrally and made accessible to employees locally through the internet and mobile devices. Access can be given to all employees so that they know which third parties are registered or accredited, or access can be restricted by function or geography as appropriate.

Data protection laws

Due diligence and monitoring processes must comply with data protection laws in the jurisdictions where the company and its third parties operate. Data protection laws can be a significant constraint to carrying out due diligence by preventing companies gaining information on third parties. For example, the UK's Data Protection Act 1988 requires that personal data must not be kept for longer than is necessary. The EU Data Protection Directive provides that data should not be processed at all, excepting where conditions are met in three categories of transparency, legitimate purpose and proportionality. There will be some information that is protected under privacy protection laws and will be restricted to the compliance or legal departments. Some of the information held on a company's system will inevitably be sensitive, such as evidence of bribery risk, conflicts of interest, improper behaviour, weaknesses or red flags.

New technology and data management tools – examples of good practice

- **Consult legal advisors:** Involve legal advisors in the design and implementation of systems to ensure compliance with legislation.
- **Develop and apply new technology:** Decide whether to use commercial software systems, which are widely available for all sizes of company, or whether to design your own solutions. Discuss the design with those in the company who will use the system as well as third parties who may have to input data.

RESOURCES

Managing Third Party Risk: Only as Strong as Your Weakest Link, TI-UK, 2016

www.antibriberyguidance.org