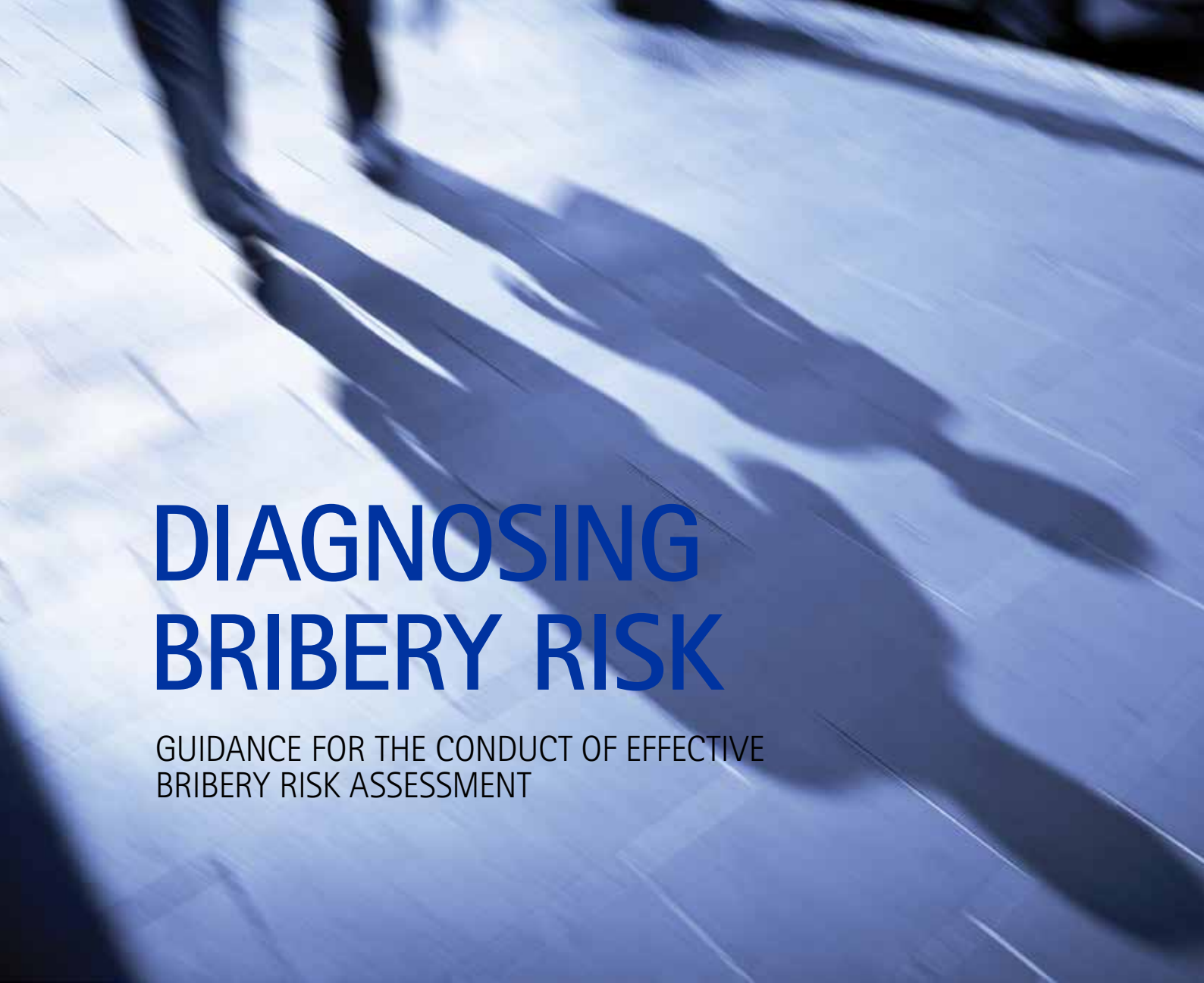




DIAGNOSING BRIBERY RISK

GUIDANCE FOR THE CONDUCT OF EFFECTIVE
BRIBERY RISK ASSESSMENT

Supported by

Transparency International (TI) is the world's leading non-governmental anti-corruption organisation. With more than 90 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 are grateful to the following for supporting this project throughout as members of the Expert Advisory Committee: Chandrashekhar Krishnan, Tamara Northcott, Simon Perry (PwC), Sam Tate and Ian Trumper. We would also like to thank Peter Wilkinson for his review of the text.

This publication has been kindly supported by PricewaterhouseCoopers (PwC), a professional services firm providing a wide range of assurance, advisory and tax services. www.pwc.co.uk

Lead author: Will Kenyon

Editor: Robert Barrington

Publisher: Transparency International UK

Published July 2013

ISBN 978-0-9573410-1-2

© 2013 Transparency International UK. All rights reserved. Reproduction in whole or in parts is permitted providing that full credit is given to Transparency International UK and provided that any such reproduction, whether in whole or in parts, is not for commercial purposes or sold or incorporated in works that are sold. Written permission must be sought from Transparency International UK if any such reproduction adapts or modifies the original content or for any copyright waiver.

Disclaimer: Every effort has been made to verify the accuracy of the information contained in this document. All information was believed to be correct as of June 2013. Nevertheless, Transparency International UK cannot accept responsibility for the consequences of its use for other purposes or in other contexts. Policy recommendations and best practice guidance reflect Transparency International UK's opinion. They should not be taken to represent the views of those quoted or interviewed or of PricewaterhouseCoopers LLP ("PwC") or members of the Advisory Committee or their associated companies. Neither Transparency International UK nor PwC assumes any liability for the information contained herein, its interpretation or for any reliance on it. The document should not be construed as a recommendation, endorsement, opinion or approval of any kind. This Guidance has been produced for information only and should not be relied on for legal purposes. Professional advice should always be sought before taking action based on the information provided. PwC is a limited liability partnership in the United Kingdom.

CONTENTS

1. INTRODUCTION	3
1.1 What type of organisation is this guide for?	3
1.2 Scope and approach of this guide	3
1.3 Legal and regulatory context	5
1.4 How risk assessment fits into an anti-bribery programme	6
2. THE RISK ASSESSMENT PROCESS	8
2.1 Theoretical foundations	8
2.2 Overview of the risk assessment process	11
2.3 Governance over the risk assessment process	12
2.4 Seeking multiple perspectives	13
2.5 Documentation	14
3. RISK IDENTIFICATION	15
3.1 Planning the risk identification	15
3.2 Key categories of risk	19
4. RISK EVALUATION	32
4.1 Purpose of risk evaluation	32
4.2 Evaluation parameters	32
4.3 Differentiating individual bribery risks	35
4.4 Business unit or market-level risk	36
5. NEXT STEPS: USING THE OUTPUT OF THE RISK ASSESSMENT	39
5.1 Mapping risks on to controls	39
5.2 Gap analysis	40
5.3 Remediation	40
5.4 Follow-up, monitoring and enforcement	41
5.5 Reporting	41
ANNEX 1: BRIBERY RISK ASSESSMENT PROCESS CHECK LIST	42
ANNEX 2: RISK ASSESSMENT TEMPLATE – ILLUSTRATIVE DOCUMENTED EXAMPLE	46
ANNEX 3: RISK ASSESSMENT TEMPLATE INCLUDING CONTROLS MAPPING – ILLUSTRATIVE EXTRACT	55
ANNEX 4: GLOSSARY OF TERMS	56

GOOD PRACTICE PRINCIPLES FOR BRIBERY RISK ASSESSMENT

Effective risk assessment will:

- 1 Have the full **support and commitment from the Board** and other senior management
- 2 **Involve the right people** to ensure a sufficiently informed and complete overview of the business and its risks
- 3 Be **comprehensive**, taking account of all activities of the business which may create significant bribery risk
- 4 **Avoid preconceptions** about the effectiveness of controls or the integrity of employees and third parties, and therefore focus on inherent risk
- 5 **Identify and describe** bribery risks in appropriate detail
- 6 **Evaluate** bribery risks by reference to a realistic assessment of likelihood and impact
- 7 **Prioritise** bribery risks to the extent that this is practical and meaningful
- 8 Be **documented** in such a way as to demonstrate that an effective risk assessment process has been carried out
- 9 Be **regular**, performed at appropriate intervals and otherwise in the event of significant changes affecting the business
- 10 Be **communicated** effectively, and designed in a way that facilitates effective communication and the design of appropriate policies, programmes and controls

1. INTRODUCTION

This guide is intended to help commercial organisations identify and evaluate the bribery risks to which their activities may expose them. It also explains how risk assessment fits into the development and maintenance of the organisation's wider anti-bribery programme.

Risk assessment is critical to the effective management of bribery risk. It has further significance because law enforcement and regulators will look for evidence of a company's risk assessment where they are called upon to investigate alleged bribery.

The Business Principles for Countering Bribery state:¹

The Programme should be tailored to reflect an enterprise's particular business circumstances and culture, taking into account such potential risk factors as size, business sector, nature of the business and locations of operation...The enterprise should analyse which specific areas pose the greatest risks from bribery and design and implement its Programme accordingly.

1.1 What type of organisation is the guide for?

This document is necessarily generic and does not seek to address any particular size or type of company, nor focus on any specific industry. It aims to guide the reader on the way in which factors such as size, industry, location and so on may have a bearing on the organisation's risk profile. The principles set out here are those which, to a lesser or greater extent, are applicable in all cases. There is no one-size-fits-all solution to risk assessment, nor indeed to any other aspect of risk management. Users of this document must therefore form their own judgement on the extent to which a particular risk element is relevant to their organisation.

1.2 Scope and approach of this guide

This guide is confined to the risk assessment process itself. The focus is on **inherent risk**, that is the risk associated with a particular activity or attribute of a business before taking account of any mitigating controls. This guide does not, except by way of brief illustration, cover the subject of mitigating controls or, therefore, the residual or net risk.

On risk evaluation and prioritisation, the guide takes a **qualitative approach**. This is because there are considerable practical difficulties associated with ascribing meaningful quantitative values to both the likelihood and the impact of a bribery event (except perhaps the size of financial penalties, which is itself difficult to predict and may only represent a small proportion of the impact of such an event). Many organisations have developed quantitative approaches to the assessment of business risks of all kinds, some of which are quite sophisticated. While not discouraging a quantitative approach, experience suggests that organisations may struggle to apply a meaningful quantitative approach to bribery risk. However, whether an organisation follows a quantitative or qualitative approach, or a combination of both, the basic principles that underpin this guide will still apply.

¹ *Business Principles for Countering Bribery*, Transparency International, Berlin 2009, Section 3 (Development of a Programme for Countering Bribery) paragraph 3.2 and section 4 (Scope of the programme).

Benefits of effective bribery risk assessment

As case studies 1 and 2 illustrate, there are both operational and commercial benefits to assessing risk. Meeting a regulatory requirement – important in itself – is by no means the only reason to carry out a bribery risk assessment. The potential positive benefits are considerable and include:

- Providing a realistic and comprehensive overview of key areas of bribery risk to assist with the design of mitigating processes and controls, training and other communications, and monitoring and review activities;
- Focusing attention and effort on those business activities and relationships which are considered to be most risky;
- Enabling an organisation to recognise where there may be an excessive controls burden in relation to relatively low risk activities and to reduce effort in those areas and/or redeploy resources where there is greater need;
- Helping to determine the level of risk-based due diligence that will be appropriate for particular third parties, building on an informed appraisal of the risks associated with the activities such parties are being asked to undertake;
- Identifying opportunities for efficiency, not only in controls but also in the underlying business activities themselves. For example, in considering third party risk arising from the use of intermediaries in particular kinds of commercial arrangement, some companies have concluded that they could reduce or even eradicate the use of such intermediaries, thereby reducing both risk and direct cost;
- Supporting the promotion of risk awareness generally and a structured, informed approach to ethical decision making in the organisation.

Case study 1

In the case of third parties, Company A found that, having assessed their universe of existing third parties:

- They had numerous third parties supplying a particular service with widely varying commercial terms. They have subsequently consolidated and reduced cost in this area;
- They were able to strengthen their negotiating position once the range of existing commercial terms in place was better understood and to improve monitoring of performance;
- They were able to correct data errors in their master vendor list regarding out of date contracts and payment terms;
- Cutting the number of third parties also reduced due diligence and other compliance costs as well as helping to contain compliance risk.

Case study 2

Company B initially thought that the UK Bribery Act would require setting up a completely new compliance organisation. However, having a detailed understanding of their higher risk areas and existing controls demonstrated to them that they could effectively embed anti-bribery risk management within their existing Compliance Governance framework.

1.3 Legal and regulatory context

A good practice organisation will not approach its anti-bribery programme simply as a matter of legal compliance. It will seek to prevent bribery because this is the right thing to do. However, it is important to take account of the attitude of legislators, law enforcement and regulators around the world, as these certainly reinforce the importance of effective bribery risk assessment and risk management.

A commercial organisation operating internationally may find itself exposed to a number of laws simultaneously. These include the laws of the country in which it is based, the laws of an overseas country in which it is doing business, the laws of a third country into which its business may be exporting and possibly others – where the organisation has a secondary stock market listing for example.

Organisations operating internationally may find themselves exposed to the laws of multiple countries.

Most countries around the world have anti-bribery legislation of some kind. The importance of a comprehensive bribery risk assessment is underpinned by all the authoritative guidance on anti-bribery procedures, including the US Foreign Corrupt Practices Act (FCPA) Guidance, the UK's Ministry of Justice (MoJ) Guidance, the Business Principles for Countering Bribery and TI's Adequate Procedures Guidance.² For example, the MoJ Guidance outlines six key elements of an effective anti-bribery programme, which it refers to as the 'six principles'. Principle 3, Risk Assessment, is summarised as follows:

The commercial organisation assesses the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The assessment is periodic, informed and documented.³

Furthermore, all the other MoJ principles are in one way or another influenced by the need for an effective assessment of risk in order to fulfil the objectives of the relevant aspect of the overall anti-bribery programme.

The FCPA Guidance also contains clear messages about the importance of risk assessment as a means of focusing anti-bribery efforts:

Assessment of risk is fundamental to developing a strong compliance program... One-size-fits-all compliance programs are generally ill-conceived and ineffective because resources inevitably are spread too thin... Devoting a disproportionate amount of time to policing modest entertainment and gift-giving instead of focusing on large government bids, questionable payments to third-party consultants, or excessive discounts to resellers and distributors may indicate that a company's compliance program is ineffective.

² A Resource Guide to the US Foreign Corrupt Practices Act, jointly issued by US Department of Justice (DoJ) and the US Securities and Exchange Commission (SEC); Bribery Act 2010: Guidance to help commercial organisations prevent bribery, Ministry of Justice, London, 2011; The 2010 UK Bribery Act Adequate Procedures Guidance, Transparency International UK, London, 2010 (MoJ Guidance).

³ MoJ Guidance, page 25.

Law enforcement and regulatory pronouncements consistently emphasise the importance of risk assessment.

Bribery risk is the risk of offering, paying or receiving a bribe through an officer, employee, subsidiary, intermediary or any third party (individual or corporate) acting on the commercial organisation's behalf.

An effective bribery risk assessment process gathers sufficient, relevant information about the organisation's business activities and relationships to enable it to determine how those features expose it to bribery risk.

Alongside the UK's MoJ Guidance, the UK's Financial Services Authority (FSA) has to date issued two reports detailing the scope and findings of thematic reviews in relation to the effectiveness of anti-bribery programmes in two of its regulated sectors: insurance brokers⁴ and investment banks.⁵ In both these reports, the FSA highlighted the importance of good bribery risk assessment as a pre-requisite for effective anti-bribery controls. In practice, the FSA found a widespread lack of effective risk assessment, low levels of understanding of the risks, and significant gaps and weaknesses in anti-bribery controls.

How does this Guide fit with existing risk assessment processes?

Any specific methods, approaches or formats that are discussed or exemplified in this document are intended to be illustrative rather than prescriptive. Many organisations have their own established methodologies and documentation standards for the assessment of business risks generally, and it may be appropriate and helpful to adopt these for the assessment of bribery risk. The contents of this document will help users determine whether or not the adoption of such existing approaches is helpful in the assessment of bribery risk.

For the sake of clarity this guide looks at risk assessment as a relatively formal and discrete process. But the principles outlined are equally applicable to the more fluid, real-time thought processes associated with day-to-day decision making. Risk assessment should not be an isolated, theoretical exercise that only certain people in an organisation are engaged in, but a way of thinking and looking at situations that is adopted by everyone in that organisation. No risk management system is foolproof. No set of policies and procedures, however comprehensive, can anticipate and legislate for every conceivable situation. What ultimately determines the effectiveness of an organisation's anti-bribery programme is the ability of management and employees to recognise and assess bribery risk in their activities and to apply anti-bribery policies and procedures that are underpinned by appropriate ethical values.

Elements of a bribery risk assessment may be conducted under legal privilege. Some organisations may choose to do this when dealing with material that could have significant legal implications. However, for most organisations it is unlikely to be standard practice in a bribery risk assessment.

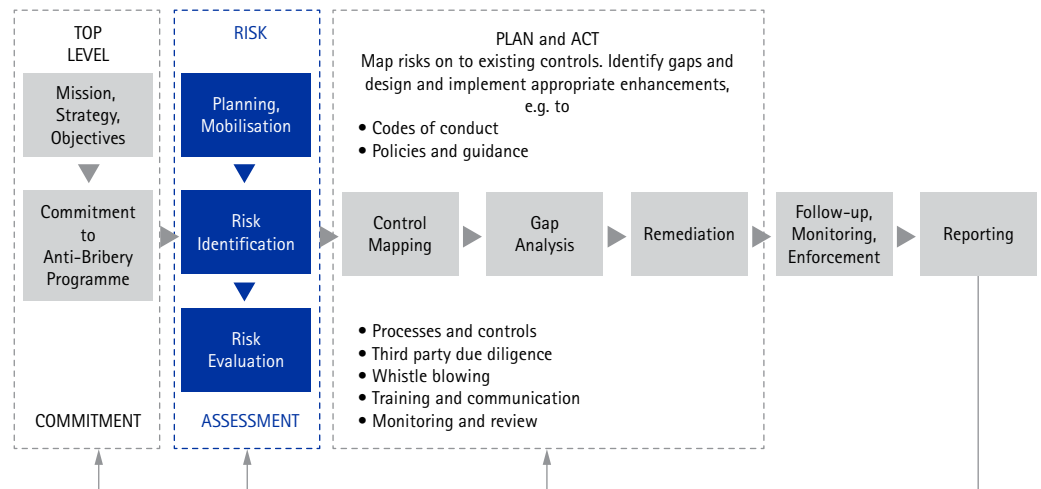
1.4 How risk assessment fits into an anti-bribery programme

Bribery risk is the risk of offering, paying or receiving a bribe through an officer, employee, subsidiary, intermediary or any third party (individual or corporate) acting on the commercial organisation's behalf. An effective bribery risk assessment process gathers sufficient, relevant information about the organisation's business activities and relationships to enable it to determine how those features expose it to bribery risk. The information gathered must be drawn from people and other sources which, collectively, present a reasonably comprehensive understanding of what the business does, how and where it does it, and how those characteristics may give rise to bribery risk. To be relevant, information needs to be up to date. This means that the risk assessment must involve the right people, draw on appropriate other sources of information and be repeated – or refreshed – on a regular basis.

⁴ FSA report entitled *Anti-bribery and corruption in commercial insurance broking* (May 2010).

⁵ FSA report entitled *Anti-bribery and corruption systems and controls in investment banks* (March 2012).

This diagram shows where risk assessment fits into the development and maintenance of the organisation's wider anti-bribery programme.



Key points to note from the diagram:

- Top level commitment is essential. The Board and other levels of management are responsible for setting strategy and objectives as well as for promoting the right culture, including an unequivocal commitment to the anti-bribery programme;
- Effective risk assessment is vital for effective risk management, as it informs the evaluation of existing controls and the identification of control gaps for remediation;
- Monitoring and enforcement are important for assessing and demonstrating the extent to which the anti-bribery programme is actually working;
- The programme as a whole is iterative, with the results of monitoring and enforcement fed back into the ongoing improvement of the programme. Iteration also ensures that the risk assessment is kept up to date and relevant.

2. THE RISK ASSESSMENT PROCESS

2.1 Theoretical foundations

There is an extensive body of both academic and commercial literature on the theory and practice of risk management and the role risk assessment plays within such wider programmes. It is not the purpose of this guide to delve in any depth into the theoretical aspects of risk management. Assessing bribery risk in a commercial organisation is fundamentally a practical task with an important practical goal. Nonetheless, effective practice requires discipline and structure and these may be informed by some of the themes common to the various risk management theories and models.

What is risk?

There is a broad consensus that risk assessment is fundamental to effective risk management (whatever the nature of the risk). The term 'risk' is variously defined. However a reasonable definition for present purposes is the one given in the 'Internal Control – Integrated Framework' produced by COSO⁶ (the COSO Framework):

Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives.

Establishing objectives

This widely accepted definition of risk pre-supposes that an appropriate objective, or set of objectives, has been established. Once this is done, risks can be identified that define events which may disrupt the achievement of those objectives. For many areas of business risk, both the objective and the related risks are highly concrete, specific and quantifiable. In the case of bribery risk, both the objectives that may be adversely impacted and the definition of the risks are often less so. They are important nonetheless.

Bribery can adversely impact a wide range of business objectives.

Objective setting

Objective setting is a precursor to the risk assessment process and therefore a full discussion is not within the scope of this guide. It is a critical part of the overall risk management programme. The objectives likely to be affected by bribery risk will include some very broad ones capable of being affected by other risks as well. Examples of broader objectives that could be negatively impacted include:

- Maintenance and enhancement of the corporate reputation;
- Compliance with all applicable laws and regulations; avoiding prosecutions or fines;
- Conducting business in accordance with defined ethical standards, including the avoidance of bribery or other forms of corruption;
- Revenue, profitability and share value targets;
- Achievement of corporate social responsibility and/or sustainability metrics.

⁶ *Internal Control – Integrated Framework* (May 2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Zero tolerance is an articulation of how an organisation views acts of bribery on its behalf, that it does not permit them under any circumstances, and that it can be expected to respond robustly and decisively to such acts.

Zero tolerance does not guarantee zero bribery, but it does commit the organisation to reasonable and proportionate steps to minimise the risk.

Objective setting – *continued*

More operationally focused objectives which could also be impacted might include:

- Maintaining strong relationships with government and/or business partners;
- Fulfilling ethical compliance requirements imposed by a customer;
- Access to particular markets (e.g. public procurement opportunities within the EU).

The above items are purely illustrative and by no means exhaustive. Each of the objectives listed may be adversely affected by allegations of bribery, as is well documented by past bribery cases. A failure to recognise how a broad range of business objectives might be affected by bribery risk is likely to result in an underestimation of the significance of bribery as a risk.

Risk tolerance

A second important precursor to the risk assessment stage is the definition of risk tolerance.

This is often also referred to as risk appetite. Borrowing again from the COSO Framework, risk tolerance can be defined as:

... the acceptable level of variation in performance relative to the achievement of objectives.⁷

Risk tolerance is therefore closely related to the definition of objectives and should logically be considered and determined in conjunction with the establishment of those objectives. The level of risk tolerance will vary depending on the nature of the risk. For many business risks, it is legitimate and quite normal for different organisations to take different positions on the level of tolerance of the same risk.

In the case of bribery risk, most business people (and all regulators and law enforcement agencies) take the view that the appropriate level of tolerance is zero. 'Zero tolerance' is a phrase much used in corporate policies and codes of conduct, and in regulatory and law enforcement pronouncements. It is important to be clear what it means and, equally, what it does not mean. In essence, zero tolerance is an articulation of how an organisation views acts of bribery on its behalf, that it does not permit them under any circumstances, and that it can be expected to respond robustly and decisively to such acts, if they occur. Zero tolerance does not mean that an organisation will expend unlimited resource on eradicating the very possibility of bribery (which is clearly not a practical objective⁸), but it does commit the organisation to taking reasonable and proportionate steps to minimise the risk.

⁷ COSO Framework: Framework and Appendices, p. 61.

⁸ See, for example, discussion of "reasonable assurance" in COSO Framework: Framework and Appendices, p.4.

It's not just about identifying and measuring risk; the objective is to help an organisation determine an appropriate response to the risk.

Responses to risk

Before looking at the risk assessment process itself, it is important to remember that the purpose of the exercise is not simply to identify and measure risk for the sake of it, but to equip the organisation to determine the appropriate response to a given risk. Just as organisations may adopt different levels of risk tolerance to a range of risks, so they may also choose different responses to each of those risks. The COSO Framework identifies four basic categories of response, which it labels as follows:⁹

- **Acceptance** – in effect, treating a risk and its consequences as a cost of doing business. This may be appropriate for risks which are not critical to the achievement of key objectives and where the costs of mitigation might outweigh the benefits;
- **Avoidance** – this is where an organisation decides to cease a particular activity or exit a market in order to eliminate the risk completely. This is a drastic, but sometimes necessary, response to mission-critical risks which cannot otherwise be mitigated;
- **Reduction** – this encompasses the implementation of programmes, processes and controls designed to reduce risk to acceptable levels and is the standard response for many typical business risks;
- **Sharing** – this includes insurance, outsourcing, joint ventures and other forms of business partnering.

It will be apparent that, of the above alternatives, risk reduction is generally the appropriate response to bribery risk. Acceptance is clearly not an option. Avoidance may be a strategy where particular markets or opportunities are so fraught with bribery risk that an organisation may choose to steer clear, but obviously cannot be applied across the whole business. Sharing does not work for bribery, because criminal liability cannot be devolved to others simply by outsourcing an activity, nor can it be insured against. Furthermore, the reputational and other collateral consequences of being associated with acts of bribery are not reduced by sharing. It will almost invariably be the principal that is treated as ultimately morally responsible for acts of bribery carried out on its behalf – whether in the eyes of business, employees or public opinion.

Zero tolerance does not mean expending unlimited resources on risk mitigation.

Cost/benefit analysis of responses to risks

Connected to risk tolerance and risk response is the question of how much resource an organisation is prepared to expend on the mitigation of a given risk. The adoption of a zero tolerance stance to bribery or any other risk does not mean that the organisation must therefore expend unlimited resources on risk mitigation. The organisation should make reasonable efforts to prevent bribery occurring, and follow a zero tolerance approach if bribery is suspected or discovered.

Inherent risk, control risk and residual risk

Effective risk assessment depends on distinguishing between certain different levels of risk.

- **Inherent risk**, sometimes referred to as 'gross risk', is risk before consideration of the mitigating effect of any controls. Consideration of inherent risk therefore ignores the existence of controls and makes no assumptions about the effectiveness of such controls;
- **Control risk** is the risk that a control will fail either to prevent or to detect some event that has an adverse effect on the achievement of objectives;
- **Residual risk**, sometimes referred to as 'net' risk, is the risk of an adverse event after taking account of the mitigating effect of controls.

⁹ COSO Framework: Framework and Appendices, p.75.

Unless the selected response to a risk is complete avoidance, it is in practice rarely, if ever, possible to reduce residual risk to zero. There will always remain some residual risk as a result of a combination of: (a) the decision to manage a risk down to an acceptable level but not to seek to eradicate it completely; (b) the inherent fallibility of people and the controls they operate; and (c) the remaining risk that those responsible for the operation or oversight of controls may deliberately seek to undermine or circumvent them for some reason (sometimes referred to as the risk of 'management override').

An effective risk assessment starts with a consideration of inherent risk. Detailed consideration of controls should be left until later.

An effective risk assessment starts with a consideration of inherent risk. There is a temptation to jump straight into a consideration of controls, but this should be resisted. If the risk assessment is to be robust and sufficiently comprehensive, preconceptions about the design and operating effectiveness of controls should not be allowed to inhibit open thinking about where inherent risks might exist. It is all too easy to think that 'such and such could not happen' because there are controls in place to prevent it. This may ultimately be valid, but at this stage no controls have been tested and, in any event, there will still be some level of residual risk. The right way to approach the identification of inherent risks is to ask what adverse events the organisation could reasonably be said to be exposed to by virtue of its activities, assuming no mitigating controls were in place. This enables such risks to be comprehensively and systematically catalogued and then proper consideration given to how they are mitigated. Starting with controls heightens the risk that only those risks which have in the past already been identified and mitigated by controls will be considered as part of the exercise.

2.2 Overview of the risk assessment process

The two key stages

This guide considers risk assessment in two key stages: risk identification and risk evaluation. As ever, different models may use different terminology and may break the process down in different ways. However there is broad agreement that:

- Risk identification is a step, or series of steps, which aims to identify, characterise and – where appropriate – quantify a set of risks;
- Risk evaluation is a separate but related step, or series of steps, which seeks to evaluate the potential significance of those risks, providing an indication of the relative importance of each risk to the organisation concerned.

Planning the risk assessment process

The two key steps are risk identification and risk evaluation, supported by planning and information gathering and captured through appropriate documentation.

Combining risk identification and risk evaluation

While this guide treats risk identification and risk evaluation separately for the purposes of outlining the approach to each, in practice the conduct of a risk assessment exercise may bring the two elements together in a more integrated fashion. For example, if the exercise involves one or more workshops with knowledgeable people from line and functions, it may be most efficient to have such groups consider both elements within the same workshop rather than seeking to convene separate events. Furthermore, the collation of input relevant to one or other element will be achieved by a variety of activities within the overall risk assessment process. As with many such projects, the process is likely to be non-linear and iterative.

A structured overall plan is helpful to ensure timely and comprehensive execution of the risk assessment. The table sets out some of the key steps in planning the risk assessment exercise.¹⁰ Once the process is established and has been built into the ongoing risk management routines, subsequent iterations of the risk assessment, may require less effort or formality for some of the suggested steps. However, in principle, all the elements are likely to remain applicable.

Key steps to planning a risk assessment exercise

Phase	Objectives	Actions
Planning, scoping and mobilisation	• Determine overall scope and approach • Obtain Board/senior management buy-in • Allocate appropriate resources • Establish a realistic work plan	• Obtain Board level buy-in • Appoint project lead • Define stakeholders, team, responsibilities and reporting lines • Identify potential information sources • Establish risk assessment framework • Draft risk assessment plan • Design any information capture templates required • Obtain necessary approval for the plan • Communicate appropriate context and instructions to contributors
Information gathering and analysis	Obtain sufficient relevant information to form the basis of a comprehensive bribery risk assessment	• Review of internal and external documents and data • Workshops/interviews • Distribution and return of questionnaires, risk assessment templates, etc • Collate and review information gathered from the above sources • Follow-up and challenge incomplete, inaccurate or inconsistent information
Risk identification	Use information gathered to identify a comprehensive set of potential bribery risks	• Consider key risk areas: country risk; sectoral risk; transaction risk; business opportunity risk; business partnership risk; other risk considerations
Risk evaluation	Use information gathered to evaluate and prioritise risks	• Consider key risk factors affecting likelihood and impact
Documentation	Record the risk assessment process in a way that will support communication of risks and the identification or design of effective mitigating controls	• Record results in the agreed format and validate with stakeholders • Communicate findings as required

2.3 Governance over the risk assessment process

Top level commitment is critical. The Board should ensure that appropriate resources are devoted to the risk assessment process.

This section considers certain aspects of governance as they pertain to the practical task of conducting a bribery risk assessment. In summary, these focus on the importance of:

- Board level and other senior management commitment and support, including the allocation of appropriate resource, for the risk assessment process and the broader anti-bribery programme;
- Appropriate levels of bribery risk awareness on the part of those charged with governance responsibilities;
- Clear accountability for the conduct of the risk assessment process and the proper use of the output derived from it.

¹⁰ This table is replicated in checklist form in Annex I.

The Board should have sufficient knowledge of bribery risk and monitor the effectiveness of the risk assessment process.

The importance of 'top level commitment' is central to standard anti-bribery guidance and to all risk management models. Board level management should give full backing to the risk assessment process and to the implementation of those policies and procedures which are considered necessary and proportionate to the risks identified. In most organisations the Board delegates the conduct of the risk assessment to someone in a suitably qualified and authoritative position below Board level. However the Board should recognise that its members need to have a sufficient knowledge of bribery risk and the effectiveness of the organisation's anti-bribery programme – including the effectiveness of the risk assessment process – to fulfil their governance obligations. Accordingly, the Board will want to be briefed both on the process and on its results. It will also wish to satisfy itself that risk assessment is established as a regular process to ensure that the organisation's risk profile is kept up to date and reflects changes and developments in the business over time. Consideration of bribery risk and the anti-bribery programme should feature with appropriate regularity, perhaps as part of the wider discussion of risk generally, on the Board's agenda.

A vital aspect of the Board's commitment is the allocation of the necessary, appropriately trained resources to conduct an effective risk assessment. This is more than a matter of simply appointing the right person to carry out the task. The risk assessment process requires the allocation of time, potentially from a number of people. In a large, multi-national organisation, this may be a substantial number of people, who are called upon to provide information and generally contribute to the process. As the MoJ Guidance puts it:

Appropriate resourcing... should reflect the scale of the organisation's business and the need to identify all relevant risks.¹¹

The Board should leave no doubt as to the importance and priority of the risk assessment process to those called upon to contribute to it.

The Board should leave the organisation in no doubt that the risk assessment process is important and that those called upon to contribute to it in any way should give it appropriate priority and attention.

The effectiveness of the risk assessment process depends, amongst other things, on clarity of accountability for the process. Roles, responsibilities and reporting lines all need to be defined. In small organisations, this may be kept very simple, as much of the work may fall to one person. In a larger, multi-entity, multi-national organisation, this becomes a significant task in its own right.

Aside from their governance role, the Board and other members of senior management should not be overlooked as valuable sources of knowledge and insight as an input to the risk assessment process. They very often draw on years of experience within the organisation and in other organisations and industries. Their active involvement in the process not only helps them be better informed about the nature of the exercise, but also reinforces the message to others about its importance to the organisation.

2.4 Seeking multiple perspectives

A comprehensive bribery risk assessment needs to look at the business and activities of the organisation in the round. Those charged with the conduct of the risk assessment must ask themselves where they will obtain the necessary information and insight to identify all relevant risks. The extent of the answer, as ever, depends on the size and complexity of the organisation and its business.

¹¹ MoJ Guidance, p.25.

In general, valuable input is likely to be obtained from:

- Those in **line roles** familiar with particular businesses and/or markets; involvement of people in key line roles provides access to direct information about the business and the environment in which it operates. This need not be restricted to those in management roles. Some input from people 'at the coal face' – those in direct daily contact with customers, suppliers, government agencies and so on – are also potentially valuable, as they may have the most immediate experience of how things work in practice;
- Those who have a **functional role** which in some way involves them in the prevention of bribery and/or in dealing with the aftermath of an ethical breach as part of a wider role; people with relevant functional roles also have useful perspectives. These might include those in internal audit, finance, legal, human resources, risk, compliance and procurement, amongst others. These may not exist as separate functions in smaller organisations and they may bear different names, but they are all examples of functions which include responsibility for some aspect of an organisation's anti-bribery programme or who might expect to take part in the organisation's response to a bribery incident. They therefore have potentially relevant knowledge or experience to contribute;
- Those, if any, who have **specific anti-bribery roles** and/or expertise.

The risk assessment should take account of a broad range of perspectives to tap into the organisation's collective knowledge.

Some individuals fit more than one of the above profiles. Particularly in larger organisations, the level of focus and specialisation tend to separate them.

There are also a number of potential external sources that might be tapped. These include:

- Opinion releases and similar sources from the DoJ and SEC;
- Past legal cases relevant to the business;
- Guidance from industry bodies;
- Professional advisers;
- Independent experts such as non-governmental organisations.

2.5 Documentation

The MoJ Guidance is very clear about the need for the risk assessment to be documented.

Those responsible for bribery risk management in organisations falling within the jurisdiction of the UK Bribery Act should note that, while the MoJ Guidance is scrupulously non-prescriptive on most things, it is very clear about the need for a bribery risk assessment to be documented. In addition to the summary passage already quoted, it refers to one of the 'basic characteristics' of a risk assessment as:

Accurate and appropriate documentation of the risk assessment and its conclusions¹²

The risk assessment should be documented so that it can be used as an input to the further stages of the risk management process.

It is good practice for a risk assessment to be captured in writing, so as to enable it to be communicated, discussed and used – as it is intended to be – as an input to the overall anti-bribery programme. In extremis, it is a great deal harder for an organisation to demonstrate, if necessary, that it has taken appropriate steps to identify and consider bribery risk, if it has no written record of such a process.

There is no one 'right' way to document the risk assessment. Annex 2 to this guide provides an example of a possible approach. Many organisations will choose to adopt and, as necessary, adapt existing documentation formats. As long as these are capable of accommodating the specific characteristics of bribery risk, then there should be no problem with this. However it is worth pausing to consider the extent to which an existing format is in reality better than using a format specifically designed to capture bribery risk. The discussion of risk identification and risk evaluation in the next two sections also provides guidance, implicit or explicit, about what elements might usefully be documented.

¹² MoJ Guidance, p.25.

3. RISK IDENTIFICATION

3.1 Planning the risk identification

The risk identification phase aims to catalogue all key inherent bribery risks.

The risk identification phase creates a comprehensive catalogue of inherent bribery risks to which the relevant organisation could plausibly be exposed by virtue of the nature and location of its activities. To be useful, this catalogue should capture each risk with sufficient precision (a) for it to be properly and consistently understood by all concerned and (b) to enable it ultimately to be matched to one or more appropriately designed and implemented mitigating controls. The formulation of policies and procedures will also be assisted by a clear and specific understanding of the relevant risks. A helpful approach is to step back and take a fresh look at the business.

Deciding whether to assess passive bribery risk

Where the commercial organisation and/or persons connected with it pay a bribe, this is generally referred to as active bribery. Where an individual receives a bribe, it is known as passive bribery. Active and passive bribery are distinct risks. Both are of concern to any commercial organisation and both are outlawed in many countries.

In the commercial sector, the attention of policy makers and law enforcers has been focused on active bribery and the damage it causes to fair competition and economic development around the world. Active bribery also brings with it correspondingly greater legal, financial and reputational consequences for commercial organisations that engage in it. This is evident in the new corporate offence of 'failure to prevent bribery' under section 7 of the UK Bribery Act, which is confined to offences of active bribery. Accordingly, the emphasis in this guide is primarily on the risks relating to active bribery.

However, passive bribery (the soliciting or receipt of bribes) is also a significant threat for many commercial organisations and is equally damaging to the countries in which it takes place. Passive bribery is strongly associated with procurement fraud, where employees of the organisation accept bribes to subvert purchasing and tendering processes in favour of the bribe payer. The consequences can be very serious and include: financial loss through overpaying for goods or services; purchase of sub-standard, counterfeit or otherwise technically non-compliant goods; reputational and brand damage; and damage to customer and other relationships.

Passive bribery may also occur on the sales side, for example where goods or raw materials are in high demand and short supply. In such a case, an employee might accept a bribe to prefer one customer over another, again with potentially damaging consequences for relationships with other customers as well as the legal consequences.

Passive bribery is also a threat where the commercial organisation provides a service involving the provision of some form of certification, which a third party customer organisation needs for its own business. Examples might include legal certifications, notarisation, audit, attestation of product quality and specification, and so on. In these cases, the acceptance of a bribe by an employee of the provider of the certification could subvert the certification process.

While this guide focuses primarily on active bribery, a good practice organisation will combat all forms of bribery. Many of the principles outlined in this guide concerning the identification and evaluation of active bribery risk could be equally well applied to the risk of passive bribery.

Asking the right questions

An effective bribery risk assessment starts with some very basic questions along the following lines (the questions are by no means exhaustive):

- What do we do as a business?
- Do we operate in a range of businesses or markets which are sufficiently different from each other to have wholly or partially distinct risk profiles?
- What interactions with the outside world do our business activities involve?
- Who do we interact with?
- In particular, what interactions do we have with central or local government and public officials generally?
- What do we need from third parties that is particularly critical to our business?
- Are we able to interact directly with such third parties, or do we rely on intermediaries to help us?
- How many such intermediaries do we engage and what do they do for us?
- Where do we do business and are customs or practices in those places likely to expose us to risk?

Organisations need to take a fresh look at their business activities and relationships through an anti-bribery lens.

These questions are all very general in nature and most of them are deliberately open in style – demanding a full, factual answer, not just a yes or no. The questions are easily put, but answering them may take some effort. Given that most organisations have historically not carried out bribery risk assessments, it is probable that many will not have looked at their business activities in quite this way before. The point is not to ask the questions for the sake of it, but to use this as a means to tease out potential risks in sufficient detail to address them effectively.

Example – government interaction

Simply having 'government interactions; or similar in a risk matrix may just about suffice for the purposes of drafting a basic policy, but it is unlikely to be adequate for designing or implementing specific controls for application to real-life situations. For example, compiling a full list of interactions with government agencies in just one country could potentially take time and input from a number of people, depending on the size of the organisation and the nature of its business. In addition, such a list is likely to lead to further questions, such as:

- Is a government interaction direct or through an intermediary?
- What is the purpose of the interaction?
- If it is to obtain a permit or something else that may be important to our business, what is it and how important is it?
- How difficult is it rightfully to obtain the said permit?
- Are there conditions which we may or may not have fulfilled and, if so, what are they?

Gathering and validating information from the right people

Collectively, those who contribute to the risk assessment should be capable of providing a reasonably comprehensive overview of the business and its bribery risk profile. There is no 'right' number of people. For a small and simple business, it is quite possible that the number may be one. The larger and more heterogeneous the business, the more people and perspectives are likely to be needed to achieve the same overview.

Assuming, as in most cases, that more than one person is involved, there is a wide range of possibilities for how information might be gathered. In smaller organisations, one or more meetings might suffice. Larger organisations might opt for a combination of approaches including:

- workshops;
- interviews;
- questionnaires sent out to business units and functions requiring answers to standard questions;
- alternatively asking those participants directly to complete a risk assessment template of some description.

Ultimately, the right answer for a given organisation is what is effective, practical and proportionate given its scale and circumstances.

SIGNPOST

The use of questionnaires without additional personal interaction and follow-up is unlikely, on its own, to provide risk information that can be relied upon with confidence.

The right questions need to be asked and the answers appropriately validated.

However information is sought from contributors, it is important that the right questions are asked in the right way and the answers appropriately validated. The value of the information provided will be proportional to the degree to which the informant understands the purpose of the exercise and the nature of bribery risk itself. Those whose 'day job' revolves around anti-bribery and compliance issues can over-estimate the level of awareness of, or engagement with, the topic by those receiving their enquiries. Appropriate messages from the top will undoubtedly boost engagement. Appropriate anti-bribery awareness training as well as briefing on the specifics of the risk assessment process also helps to enhance the quality of information fed into that process.

Validation of information gathered does not mean full verification which is impractical given the nature of the exercise. However, those gathering the information should consider whether it is both complete and reasonable based on their own understanding of the business. Those responsible for the conduct of the risk assessment process will therefore need an appropriate set of expectations about likely areas of risk so enabling them to evaluate and challenge the input they are receiving.

Case Study 3

Company C, a global business, carried out a 'risk survey' by asking its business units to complete a standard template. The initial results showed a high degree of inconsistency in the coverage of risks and level of detail. Some business units which were expected to have similar risk profiles in fact returned very different information. During validation it became clear that business units had not been adequately briefed and that there was a widespread lack of understanding of bribery risk. The company took a number of steps, including:

- Targeted anti-bribery training to raise bribery risk awareness;
- Improvements to the bribery risk template, including more detailed briefing notes on how to complete it;
- Regular validation and challenge of business unit risk assessments, including incorporation of this within the internal audit programme;
- Evaluation of business unit management on compliance performance, including the quality of business unit risk assessments.

As regular risk assessment becomes embedded into the routines of the business, appropriate enquiries by the internal audit or equivalent function could become a further source of validation. Whether on a targeted basis, or alongside other audit activities, internal audit could be asked to review and report on the approach taken to bribery risk assessment by line or functional management.

Using what you've got

In addition to active engagement with the relevant people, most organisations are in possession of a range of internal sources of information which they can use as input to the risk assessment process. These might include:

- Past experience of bribery issues (including experience brought by board members and employees from other organisations);
- Findings from internal audit reports, internal investigation reports, etc;
- Country and market insights from management and employees in different countries. Market insights include knowledge about local culture and business practices, customer and competitor behaviour, etc;
- Knowledge of local laws and regulations from the in-house legal team or local management;
- Whistle blower or similar reports.

Any such sources are part of the 'corporate memory' and should be harnessed to maximise the breadth of information available to those carrying out the risk assessment.

Considerable amounts of information will also be available in the public domain, as briefly discussed in section 2.4 above.

Risks and risk factors

As part of a structured approach, it is also helpful to distinguish between the terms 'risk' and 'risk factor'. 'Risk' has already been defined using the COSO Framework definition. If a risk is "the possibility that an event will occur and adversely affect the achievement of objectives" then the identification of a risk involves formulating an appropriate description of the adverse event in question. A 'risk factor', on the other hand, is the description not of the adverse event itself but of a circumstance (internal or external to the organisation) which tends to increase the likelihood of the adverse event occurring. In essence, the difference between risks and risk factors can be broadly characterised as the difference between asking the question "What could go wrong and how might it happen?" and asking the question "Why might it happen and how likely is it to do so?" The following example illustrates the distinction:

- **Risk:** A bribe may be paid by a local business unit in order to win a substantial, long-term contract with a key customer in [country X];
- **Risk factors:** There is known to be a high level of corruption in [country X]; employees of the customer are known to have asked for bribes in the past; management of the business unit are under severe pressure to meet budget and this contract is of a scale that will make a material difference to achieving that goal; anti-bribery controls in the business unit are weak; there is a culture in the business unit (and in [country X] generally) of deference to senior management; etc.

In practice, many risk factors tend to apply to more than one risk. Some may actually apply to most if not all risks, for example the existence of generally weak anti-bribery controls. For this reason, it may be impractical and unwieldy to list all risk factors separately for all risks.

3.2 Key categories of risk

The objective of risk categorisation is to ensure that all facets of the business have been considered with regard to their propensity to expose the organisation to bribery risk. There is no universally agreed categorisation of bribery risk. However the categories are drawn, there will always be debate about what belongs where and whether there is overlap between one category and another. None of this should detract from the importance of a structured approach to the consideration of bribery risk in its many different guises. Businesses have a range of characteristics, and risks may potentially stem from any of these.

The UK's MoJ Guidance provides a useful set of risk categories as a starting point, identifying five such categories:

- 3.2.1 Country risk;
- 3.2.2 Sectoral risk;
- 3.2.3 Transactional risk;
- 3.2.4 Business opportunity risk;
- 3.2.5 Business partnership risk.

Each of these categories is associated to a varying degree with both risks and risk factors.

A proper consideration of country risk should ask why and how a country is risky.

3.2.1 Country risk

The country risk category covers risks derived from the location of business activities.

The starting point for many in considering country risk is an index such as TI's Corruption Perceptions Index (CPI).

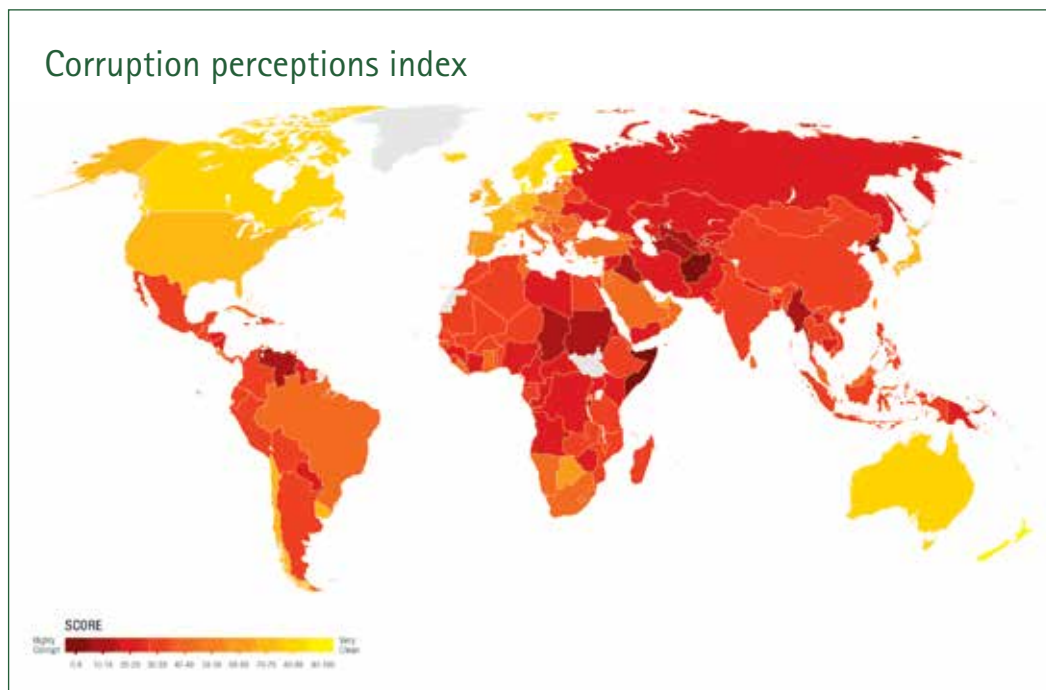
SIGNPOST

The risk score from an index such as the CPI is a good example of a risk factor – it tells you something about the level of risk, but nothing about the nature of the risk. Clearly, a proper consideration of country risk needs to go further. We may have a broad sense of the level of risk, but the risk score on its own doesn't explain why a particular country carries a higher risk, let alone how the risk might manifest itself.

The sorts of factors that might underpin a high corruption risk score for a country include:

- Lack of enforcement of anti-bribery legislation;
- Lack of transparency in business dealings;
- Impenetrable bureaucracies;
- The need to use well connected intermediaries to gain access to people in positions of power;
- Evidence of endemic corruption in everyday life;
- Lack of an established rule of law;
- Lack of a truly independent and impartial judiciary;
- Lack of effective democratic institutions;
- Lack of independent media;
- A culture that tends to encourage circumvention of rules, nepotism, cronyism and similar distortions to an open market;
- Pressure to conform to specific cultural norms and customs or unfamiliar business practices which may conflict with applicable anti-bribery laws;
- The prevalence of requests to make 'grease' or 'facilitation' payments to expedite processes.

Having established that there is a particular level of risk in a given country and the sorts of factors that give rise to that level of risk, how bribery might actually occur in the business in that country needs to be determined. It is possible that there may be some risky transaction that is unique to a particular country, in which case it will most likely be identified in the context of an effective analysis of country risk. However most specific bribery risks emerge to a large extent from consideration of the other risk categories.



Source: CPI map from: <http://cpi.transparency.org/cpi2012/press/>

The CPI is one of the most widely-used tools in corporate risk management. It provides a high-level view of the corruption in countries around the world. However, it is important to recognise that:

- Corruption happens in all countries, and so even a country that scores well on the CPI may present risks;
- There is regional variation within countries;
- Risks may vary significantly between sectors and business models;
- The CPI is a) based on perceptions and b) measures public sector corruption;
- TI recommends that the CPI scores should be used as an entry point to additional information such as the Global Corruption Barometer or more detailed country-level analysis.

Case Study 4

After assessing the bribery risks in its interactions with healthcare professionals, Company D, a pharmaceuticals company, found that in some markets healthcare professionals were actually more likely to be influenced through the offer of luxury travel and access to key opinion leader meetings than by the offer of cash. In other words, the prospect of enhanced profile and status was more attractive to such third parties than immediate financial gain. This enabled the company to focus its anti-bribery efforts on an area that might otherwise have been thought of as lower risk.

3.2.2 Sectoral risk

Certain sectors are typically associated with higher levels of bribery risk than others. The MoJ Guidance cites the extractive industries (oil, gas and mining) and large scale infrastructure as two such sectors. Other sources, including TI's Bribe Payers Index, add others to the list of higher risk sectors. As with country risk, the acknowledgement that a given sector is associated with higher bribery risk is of limited value in itself, as it says nothing specific about the nature of the risks involved or how they arise. Furthermore, there is a danger that too much focus on sector risk in the abstract will lead those not in sectors considered high risk to think of themselves as low risk without proper analysis of whether that is really true.

No sector is immune from bribery risk. It's not about the sector label, it's about what business in the sector actually entails.

No sector is immune from risk. Risk derives not from the industry label but from the concrete activities that businesses operating in that sector undertake. Nevertheless, looking at the sector dimension can provide a useful focus for identifying both risks and risk factors. Looking at a sector level may act as a short cut to the identification of at least some key risk areas, particularly where a relevant sector trade body has already published guidance on the topic.

SIGNPOST

Organisations should always beware of relying exclusively on generic material – even if designed for the right sector – which was not written for any specific organisation with its own unique risk profile and circumstances.

Sectoral risk factors, which may directly or indirectly elevate the level of bribery risk might include:

- Requirement to operate in countries associated with high levels of corruption;
- High degree of interaction with government;
- High levels of regulation;
- Prevalence of high value, complex and/or long term contracts;
- Business activities involving multiple business partners, stakeholders and/or complex contractual or corporate structures.

In practice, many organisations operate in more than one sector. For example, the risk profile of the 'upstream' business of an oil and gas company may look quite different from that of its 'downstream' operations. Even if a particular sector predominates, consideration needs to be given to ancillary or non-core activities, the risk profile of which may be quite different.

3.2.3 Transactional risk

Detailed consideration of concrete business activities is key to considering transactional risk. For the purposes of this guide, the term 'transaction' is used broadly to cover any activity involving some form of economic exchange between counterparties. Transactions may be more or less risky, depending on matters including:

- The subject matter of the transaction;
- The identity and nature of counterparties, for example whether they are connected to government in some way;
- The degree of transparency of the transaction or related dealings;
- How critical a particular service or supply is to the procuring party – for instance, its importance to the business and/or the level of urgency required.

Organisations need to think about bribery risk at the transactional level.

Examples of transactions typically seen as carrying heightened risk include:

- Sales to government customers, particularly in higher risk countries;
- Gifts, hospitality and travel expenditure, especially for government officials;
- Use of company assets for the benefit of third parties for non-business purposes;
- Charitable and political donations and other corporate relations activities;
- Sponsorships;
- Giving employment to persons connected with government officials;
- Obtaining licences, permits and regulatory clearances of any kind;
- Movement of goods across borders and related activities;
- Lobbying governments on policy, legislation and/or regulation;
- Others that affect a specific company or business circumstance.

In addition to the above examples, there are a range of issues to do with (a) transaction size and complexity and (b) business relationships, corporate structures and the like. These are highlighted under the business opportunity and partnership risk categories below.

High-risk transaction 1: Sales to government

Paying a bribe to achieve a sale is illegal under the UK Bribery Act regardless of whether the customer is connected to government or is a representative of a private sector concern. The focus on government sales does not mean that non-government sales are devoid of risk, but reflects the reality that in many countries any dealing with government officials is likely to carry a higher level of risk. Laws that comply with the OECD Anti Bribery Convention, such as the FCPA, are explicitly focused on the bribery of government officials. For example, there is a specific offence of bribing a foreign public official under section 6 of the UK Bribery Act. One of the challenges – which must be addressed as part of the risk assessment exercise – is to identify who is a government official. This may not be absolutely clear-cut in some countries where there is a degree of uncertainty about whether particular organisations belong in the public or private sectors.

The risk assessment should identify the extent of government business and where this is located to help determine the significance of this risk to the organisation. It should also be borne in mind that gaining access to opportunities to bid for government contracts may be as risky as the bidding process itself.

High-risk transaction 2: Gifts, hospitality and travel

The issue of gifts and hospitality has received disproportionate coverage since the advent of the UK Bribery Act. In some respects, the risks attached to these transactions can be exaggerated. As the MoJ Guidance states, while there is no doubt that, in certain circumstances, such expenditures can be used as a form of bribery:

Bona fide hospitality and promotional or other business expenditure which seeks to improve the image of a commercial organisation, better to present products or services, or establish cordial relations, is recognised as an established and important part of doing business and it is not the intention of the Act to criminalise such behaviour.¹³

In the US, legislators have taken a slightly different approach by including within the FCPA an explicit exemption for "Bona Fide Expenditures". For practical purposes, the UK Bribery Act and the FCPA arguably lead to similar conclusions about where the line is drawn, even if they do so via different routes.

¹³ MoJ Guidance, p.12.

Organisations need to be aware of the impact of local law, custom and practice on the implementation of policies and procedures.

Context is critical in determining whether gifts or entertainment are appropriate or not.

The challenge for commercial organisations is to formulate policies, design controls and deliver appropriate training and other communications which minimise the risk that such expenditures are incurred for purposes that do not meet the above test. It should also not be overlooked that, whatever the UK Bribery Act or the FCPA may say, locally applicable laws may be different. In some countries, strict quantitative limits (possibly as low as zero) may apply to the value of such expenditures, particularly those that benefit a public official. These limits also need to be factored into the local implementation of any policy. Without such clear-cut constraints, it is a matter of judgement as to what is appropriate. Context is critical: the circumstances, location, value and beneficiary all play a potential role in determining the right answer.

As far as the risk assessment is concerned, it is important to understand the sorts of situations in which such expenditures are incurred. A generic item 'gifts and hospitality' or similar is less helpful than a more detailed summary of the key categories of such items which are actually seen in the business. This may be quite culturally specific, with different types, amounts and frequency occurring in different countries, depending on local custom and practice.

Gifts and hospitality are also a prevalent concern in relation to passive bribery. Organisations should ensure that their employees are aware of what is and is not appropriate in terms of the receipt of gifts from third parties.

High-risk transaction 3: Use of company assets

An area often neglected is the risk that the organisation's assets might be made available to a third party as a quid pro quo for some benefit to be received from that third party. This might, for example, take the form of use of a corporate jet other than for bona fide business purposes; providing office space to house an essentially political campaign of some sort; and so on. There are endless possibilities and the task for those conducting a bribery risk assessment is to consider what exposure there might be to this sort of risk. A helpful start is to ask, as part of the information gathering process, whether there is any experience of requests received for this sort of support and how such requests were responded to.

High-risk transaction 4: Charitable and political donations, etc

Charitable and political donations are often grouped together, although – if genuine – they are different in nature. Many organisations have a policy of not making political donations, at least not in the form of funding.

Charitable donations at first sight appear to be a very different proposition. Commercial organisations typically do make such donations, sometimes as part of a wider corporate social responsibility or similar programme. As with any other business partner, however, it is important that a proper assessment is made of the bona fides of any charity and the background and context to a donation. Documented bribery cases from the past have shown that charities can be used as a conduit for payments that are in effect bribes, perhaps because they represent a back-door means of channelling funds to a government official's family, or because an apparently charitable undertaking is actually part of a local politician's campaign.

As with any of the key risk types, it is important not to interpret the definitions too narrowly and to think laterally about what sort of situations might arise which, whatever terms are used to label and describe them, have fundamentally the same sorts of characteristics. Thus, when thinking about political or charitable activity, consideration should also be given to the broader range of community programmes and other activities intended for the public good which many commercial organisations engage in. These may fall into either of two categories: voluntary and compulsory. Voluntary activities under this head are those which an organisation chooses on its own initiative to undertake. All of these should be subjected to the same scrutiny as described above as to the nature of the activity and the identity and nature of counterparties and beneficiaries, and whether some ulterior motive exists on either side of the relationship, or could be perceived to do so.

Good intentions can blind organisations to the risks. Charitable donations should be subject to appropriate scrutiny, notwithstanding their benevolent purpose.

In this context, compulsory activities are those entered into transparently as a condition of the award of some contract, concession or similar. This is a common feature of negotiations for exploration, drilling or mining rights in the extractive industries, or of the granting of permission for major infrastructure or property developments. For example, a mining company seeking rights to explore a green field site for its potential as a mine will almost invariably be required to provide various benefits to local communities affected by its operations. These might take the form of new roads, schools, hospitals as well as employment opportunities. Such compulsory quid pro quos are sometimes referred to as 'offsets' and are common to large scale capital projects. Assuming they are officially sanctioned, transparent, properly monitored, incorporate anti-corruption measures and would apply to any bidder, such expenditures should in and of themselves be unobjectionable. However, care must be taken to ensure that the scope of these activities does not extend to any which might improperly influence decision making. For instance, the risk could be examined in more depth by considering which groups or individuals would benefit most from offsets – in the mining case, the likely winners of supply contracts – and whether the bodies implementing offset activities have appropriate anti-bribery safeguards and controls.

A comprehensive risk assessment seeks to identify the full range of activities which might fall under this category. Having recognised the general risk and put in place suitable policies and procedures, each individual case must be considered in its own right and relevant third parties subjected to appropriate due diligence. Such case-by-case considerations, while likely to follow similar principles, are not within the scope of this guide.

SIGNPOST

Charitable donations are an area where good intentions can blind organisations to the risks.

High-risk transaction 5: Sponsorships

Certain sponsorships are closely allied to the sorts of community activities described above. An organisation might sponsor a local sports team, cultural event or similar in a location where it operates. The activity is in itself innocent enough; the risk to be considered is that there might be some expectation of a specific benefit in return.

Educational scholarships and other support for individuals where the organisation has control or influence over the selection of beneficiaries should also be considered an area of potential risk, since benefits could be conferred on persons connected to people in authority as a quid pro quo.

High-risk transaction 6: Employment of persons connected with government officials

A similar principle applies to the employment of persons connected with government officials or others in a position to make decisions in favour of the organisation. The fact of such a connection should not, of course, preclude a person from employment. However, care needs to be taken to ensure that employment is offered for the right reason (best candidate, suitably qualified, competitively selected on the basis of normal processes and criteria).

High-risk transaction 7: Licences, permits, regulatory clearances

This is a very broad area and the actual licences, permits, etc required by a business to operate vary greatly depending on the nature of the activity, the jurisdiction, and so on. A helpful step towards assessing risk in this area is to create as comprehensive as possible an inventory of such requirements, including their description, purpose, from whom, how and how often they are required to be obtained, key conditions to be fulfilled, and so on. Each of these generates a series of interactions with officialdom and potential exposures to bribery risk, the level of which may be influenced by factors such as general levels of corruption, the complexity of the conditions and processes associated with obtaining the licence, permit, etc and the extent to which it is critical rather than merely important to the business.

The risks in this area are not restricted to the legal and reputational damage that might result from obtaining licences, etc by corrupt means. Where a licence is obtained through bribery, this may not simply be a case of avoiding bureaucracy or placating a corrupt official; it may also involve the circumvention of rules that are there for a reason, perhaps compromising risk management in other areas such as health and safety, environmental compliance and so on.

Case Study 5

Company E, a mining company, carried out a detailed inventory of the numerous permits and licences required for it to carry on its business. These varied according to the location and status of a particular mining project: from green field site to early exploration to commissioning to full operation and finally to decommissioning. In all, it found that it needed more than 20 permits and licences, necessitating interactions with several different government agencies, both central and local, and different officials within those agencies. This knowledge enabled the company to target its anti-bribery efforts effectively in this key area of operational risk.

High-risk transaction 8: Movement of goods across borders

The movement of goods across borders is a fact of daily life for many businesses. It brings with it frequent interactions with customs and excise officials, directly or through agents. In countries with poor records on corruption, getting goods into port or through customs is often cited as a perennial headache for manufacturing and trading companies and the logistics businesses that support them. Demands for payments to speed things up or even move things at all are a regular occurrence.

The risk assessment should capture this risk, where it applies. It will be helpful to obtain views from those directly involved in this aspect of the business to get a sense of the reality 'on the ground'.

Case Study 6

Company F, a consumer goods company, discovered that customs officials in one of its markets were incentivised to collect more excise duty by sharing substantially in the incremental duty collected. The company was also using an intermediary in most of its day-to-day dealings with the customs authorities. The company recognised that there was a high risk that improper inducements might be offered or solicited on either side in order to resolve excise duty issues and took steps to mitigate this risk.

High-risk transaction 9: Lobbying

Commercial organisations may seek to convey their views on particular matters in order to influence government actions or broader policy. The openness of governments to dialogue with business varies greatly around the world, as does the ease of access to government ministers and officials. This is an area where the use of intermediaries is prevalent and, while this may be necessary to gain access to the right people, it tends to elevate the risk of such activities. There is clearly a wide ethical gulf between bona fide efforts to put forward an informed point of view on a particular aspect of government policy as part of a genuine dialogue and attempts to subvert government decision making by corrupt means.

The risk assessment should incorporate significant lobbying activities, where they occur, in conjunction with the identification of any intermediaries who are used to facilitate or carry out such activities on the organisation's behalf.

High-risk transaction 10: Other

Individual companies may face other types of transaction risk. The nine transaction types listed above should be considered illustrative and not exhaustive.

3.2.4 Business opportunity risk

The MoJ Guidances defines this risk as follows:

Such risks might arise in high value projects or with projects involving many contractors or intermediaries; or with projects which are not apparently undertaken at market prices, or which do not have a clear legitimate objective.¹⁴

The business opportunity risk category relates to the basic characteristics of a transaction, such as:

- Value;
- Complexity;
- Commercial rationale.

SIGNPOST

What is business opportunity risk? As an example, a complex and high-value transaction with questionable commercial rationale is a business opportunity that may represent a bribery risk.

High value and complexity tend to elevate risk.

Transactions with high value may create greater incentives for one or more parties to the transaction to behave corruptly in order to ensure the transaction goes ahead and that they will benefit from it. What constitutes a high value is likely to vary from one organisation to another and from one situation to another. The definition of a high value transaction for a multi-billion pound turnover company may be orders of magnitude different from a transaction considered high value for a SME. Any transaction which is significant in relation to the organisation in question or even to individuals involved in the transaction (such that its success would, for example, have a significant impact on their remuneration), may be deemed high value.

Complexity will often go hand in hand with higher transaction value. Complexity may arise because of the number of parties involved, such as consortium partners, sub-contractors, intermediaries or similar. The more third parties involved, the higher the risk that one or more of them could act in a manner which creates legal – or at least reputational – exposure for the organisation. Alternatively, it may relate more to the duration and/or number of phases of the project in question. The more complex the project itself in terms of inputs, interactions, phases and/or outputs, the greater the potential for breakdowns in accountability and control over expenditures at some point.

Transactions with no clear, legitimate commercial rationale are a significant red flag.

Transactions for which the commercial rationale is difficult to explain are of particular concern. There may be a legitimate reason for a transaction to be structured, routed, priced, etc in a particular way – for tax efficiency, for example, – but questions need to be asked where transactions have characteristics, elements or parties for which the purpose is not readily apparent. Examples might include:

- Costs of goods or services which seem out of proportion to what is being provided;
- The involvement of intermediaries or other third parties whose contribution to the transaction is unclear;
- The procurement of goods or services the purpose of which is uncertain.

¹⁴ MoJ Guidance, p.26.

Bribery risk cannot be outsourced. Outsourcing an activity will tend to compound the risks because third parties are more difficult to control.

3.2.5 Business partnership risk

Under many anti-bribery laws around the world, including the UK Bribery Act and FCPA, an organisation may be held liable for the acts or omissions of a third party operating on its behalf. The extent to which the organisation may be held liable depends on the facts of each case, such as whether the organisation is aware of a particular party in the supply chain and, if so, the degree of control the organisation has over the conduct of that party.

The knowledge, influence and intentions of the organisation in the establishment of a given chain of supply are important. Organisations cannot simply hide behind an opaque structure or seek deliberately to distance themselves from the acts of other parties by interposing yet others between them. There is therefore no specific number of links in a supply chain beyond which liability cannot extend. On the other hand, where an organisation participates in good faith at one end of an extended supply chain it could legitimately claim that it is less likely to have knowledge of other parties further along the chain, let alone be in a position to control their actions.

All of this raises a host of questions and challenges for those carrying out the bribery risk assessment. It is critical that business relationships are properly analysed and understood. These fall into a number of categories, including:

- Intermediaries;
- Joint ventures;
- Consortia.

The overarching questions in all cases revolve around the true nature of the relationship and the degree to which an involved third party might be considered to be acting on behalf of the organisation, along with the identification of other risk factors connected to the underlying activities involved. There are in effect two different dimensions of risk related to third parties:

1. the level of risk associated with the activities undertaken by the third party; this is the subject of the risk assessment process.
2. the risk associated with the third party itself by virtue of its identity, ownership, activities, track record, reputation, and so on. This is addressed through risk-based due diligence, which is a separate topic not discussed in any detail in this guide, although as a general rule the level of due diligence – like all other risk management responses – should be risk-based and proportionate.

Third party risk comprises: 1) the inherent risk of the outsourced activity; and 2) the risk associated with the third party which carries it out.

SIGNPOST

Due diligence on third parties may range from very limited, high level procedures for low risk cases to much more in-depth fact gathering ('enhanced due diligence') for third parties carrying out higher risk activities. At the higher risk end of the spectrum, it may be necessary to involve third party specialists to assist with open source research of the kind not readily available to non-specialists.

Intermediaries

Intermediaries come in many forms. They may include (without limitation):

- Sales agents;
- Distributors;
- Contractors and sub-contractors;
- Customs agents and freight forwarders;
- Lobbyists;
- Lawyers;
- Tax advisers;
- Advertising agents;
- Event organisers;
- Visa agents;
- Introducers;
- Consultants;
- Others not listed here.

Organisations should look at the substance of third party relationships, not just their legal form or the terminology used to describe them.

It is important to think broadly about the sort of interactions the organisation has with third parties and to look for the characteristics indicating the existence of an intermediary relationship. Those conducting the risk assessment should not be distracted by terminology. The label given to a particular third party is not the determining factor; what matters is the substance of the relationship and the nature of what the third party is, or might be, doing on behalf of the organisation.

What is the risk from suppliers?

One type of third party not included in the above list is the straightforward supplier (or vendor). The MoJ Guidance suggests that:

...where a supplier can properly be said to be performing services for a commercial organisation rather than simply acting as the seller of goods, it may also be an "associated" person.¹⁵

This appears to draw a distinction between a) suppliers simply selling goods or services and b) suppliers whose activities involve interactions with a third party on behalf of the organisation. An example of the latter might be an oil services company operating an oil rig as a contractor on behalf of a large energy company. The important point here is that not all third parties need to be treated in the same way and many 'normal suppliers' can be legitimately regarded as relatively low risk. However, as always, it comes down to the true substance of the relationship and the level and nature of involvement of the customer organisation in the supply process.

¹⁵ MoJ Guidance, p.16. An "associated person" is one capable of creating liability for the organisation for failing to prevent bribery pursuant to section 7 of the UK Bribery Act.

Joint ventures

Joint ventures are a common feature of business. In some developing markets, they may be the most practical – perhaps even the only possible – way of gaining access to that market. Countries where this is the case tend to be countries which also have poor corruption reputations. Joint ventures take a number of forms. They may involve the establishment of a separate joint venture entity jointly owned by a number of joint venture partners. The day-to-day control of such an entity may or may not be in proportion to the share of equity owned by each joint venture partner. There may be management agreements or similar in place which determine that a particular partner will have control, even if their equity stake would not of itself confer such control. Alternatively, joint ventures may be established by purely contractual arrangements, where the partners agree to collaborate in some way.

There is a risk that an organisation could be held liable for acts of bribery of the joint venture entity or any joint venture partner. The legal position on this is very case specific and may depend on a wide variety of factors. In any event, there is a commercial risk to the value of any investment and prosecutors and courts are likely to look through the legal form of any joint venture arrangement to the underlying substance of the relationships. Countering bribery risk in this area again involves a combination of effective risk assessment and mitigation, including appropriate due diligence on all parties involved.

Consortia

Consortia, where commercial organisations agree to collaborate in bidding for and executing a project of some kind, are for the practical purposes of bribery risk assessment similar to joint venture arrangements. They may be specific to one project and accordingly of a shorter term nature than joint ventures.

Critical to the risk assessment process in relation to any third party relationships is the recognition that the analysis of purely legal liabilities is not the be all and end all. The damage to reputation and business relationships arising from guilt by association can be immense.

3.2.6 Other risk considerations

One risk issue that arguably does not fit neatly under the previous headings relates to the legal and regulatory framework in which commercial organisations are required to operate around the world. This has already been touched on in the discussion of how local laws might affect policy around issues such as gifts and hospitality. However, the impact of local laws and regulations goes much wider than that and can cover a wide range of topics, including:

- The definition of bribery;
- The scope of bribery offences in terms of who is covered, public versus private, active versus passive, and so on;
- Limits on the value of gifts, hospitality, etc that can legally be given or received;
- The jurisdictional reach of the law;
- Whether certain payments are explicitly permitted that might be outlawed elsewhere, for example:
 - Facilitation payments (e.g. partially permissible under the FCPA)
 - Bona fide business expenditures (ditto)
 - Payments otherwise permitted under local written law (relevant, for example, in the context of the UK Bribery Act);

Organisations should analyse how different anti-bribery laws around the world impact their risk profile.

One aspect of inherent risk may be the laws and regulations of the organisation's home country.

- Whether there are other offences that might be brought alongside or instead of bribery offences, such as the accounting and record keeping offences under the FCPA or similar offences under the UK Companies Acts;
- What relevant laws say about the degree of responsibility an organisation has for the acts of subsidiaries and third parties.

In many cases, laws and regulations simply codify what are widely seen to be appropriate standards of governance and conduct. However there may also be matters of detail which are specific to a particular jurisdiction and which require central and/or local tailoring of policies and procedures.

4. RISK EVALUATION

4.1 Purpose of risk evaluation

Risk evaluation helps to focus finite resources on priority risks.

Any commercial organisation faces a range of risks. Key areas include: financial, operational, legal and regulatory risks as well as risks to reputation and brand, each of which may itself encompass a host of individual risks. Given finite resources, organisations must decide how best to assess and mitigate risk. This means targeting risk management efforts at those particular risks which are capable of the most significant adverse impact on the achievement of business objectives.

Any risk evaluation will seek to determine which risks are of most significance to the business. A basic objective is to evaluate and prioritise different risks. With regard to bribery risk, this can be done at different levels:

- **Bribery risk v. other risks:** At the most basic level, bribery risk can be compared with other business risks to assess the relative significance of each risk area. Historically, this is as far as most organisations have gone in assessing bribery risk. This is useful to the extent that it provides a high level overview of all key risks, assuming that a comprehensive bribery risk assessment has been carried out to inform the correct positioning of bribery within this wider risk matrix. However, it provides no detail on the nature of individual bribery risks and is not sufficient of itself to provide a basis for effective bribery risk mitigation;
- **One bribery risk v. another bribery risk:** Assuming that an appropriate risk identification exercise has been carried out, an attempt can be made to differentiate between individual bribery risks. This is useful to the extent that such risks can be meaningfully differentiated. An approach to this is discussed in more detail below;
- **Business unit or market risk:** As well as comparing individual bribery risks, an organisation might seek to compare levels of bribery risk associated with different defined business units. This might be a comparison of risk levels in different legal entities or divisions, markets, product or service lines, countries or regions, etc, depending on what makes most sense in the context of the organisation and its business. This is also examined further below.

4.2 Evaluation parameters

Established risk management models generally identify two key variables which play a role in the evaluation of risk:

- Likelihood (or probability) of occurrence;
- Impact.

Depending on the nature of the risk in question, these variables may be expressed in either quantitative or qualitative terms, or a combination of both.

This guide takes a pragmatic line on the differentiation and prioritisation of individual bribery risks. If bribery risks are difficult to quantify, then it may not be practical to attempt to stratify them into more than a limited number of categories or levels. Stratification of risks only makes sense to the extent that there is a real, practical difference in the way such risks will be addressed through mitigating controls.

Likelihood is driven by the presence of risk factors. The more numerous or significant the risk factors, the greater the likelihood that a risk event will occur.

4.2.1 Likelihood

The terms likelihood and probability are often viewed as interchangeable in discussions around risk evaluation. Probability has stronger quantitative connotations, given its use in the fields of mathematics and statistics. Accordingly, in light of the more qualitative approach outlined in this guide, the term likelihood is favoured here.

Quantitative and qualitative approaches to measuring likelihood

Whether or not likelihood is susceptible to quantitative measurement depends on the nature of the risk. An adverse event which is endemic in the business and expected to occur with a high and relatively predictable frequency (and with relatively predictable, homogeneous results) will generally lend itself better to a quantitative approach. Examples might include claims frauds in the insurance sector or pilferage in retail. These are a constant feature of the relevant business and the risk management process revolves around finding the right balance between the benefit of reducing their impact and the costs of doing so.

Conversely, risks which are not regular or predictable in terms of likelihood or impact cannot so easily be measured using a quantitative approach. Adverse events which are expected to occur infrequently and/or with no discernible pattern of occurrence and events which cannot be so easily quantified in terms of their full impact are suited to a more qualitative treatment.

Likelihood is essentially driven by the presence of risk factors. The more significant and/or numerous the risk factors associated with a particular activity, the higher the likelihood that an adverse event might occur in the context of that activity.

As discussed in section 3, risk factors are characteristics or circumstances which will tend to increase the risk that bribery might occur. Risk factors do not describe the risk itself (i.e. how bribery might occur), but rather they address the question of why bribery might occur and how likely it is to do so. Some risk factors may apply to more than one – and possibly all – areas of risk. For example, a general culture of corruption in a particular location is likely to elevate the risk associated with many, if not all, business activities carried out in that location.

A structured way of considering risk factors is outlined in the table below, which sets out how different risk factors might affect the evaluation of risk. The examples given are by no means exhaustive. They are intended as suggestions of the sorts of factors that might be considered in arriving at an evaluation of bribery risk associated with a particular activity or area. The illustrative documented risk assessment in Annex 2 does not explicitly list out all the risk factors considered, but rather they are subsumed into the "risk rating" assigned to each risk area (along with the evaluation of impact discussed later in this section). Risk factors, therefore, are an important input to the risk evaluation process rather than an output from it. The output is the risk rating, which should drive the level of mitigating response.

Using risk factors to evaluate likelihood

Risk factor	Lower likelihood	Higher likelihood
Culture	- The location of the activity is not associated with significant levels of corruption - There is a strong anti-bribery culture within the organisation	- The location of the activity is associated with significant levels of corruption - There are prevalent local customs and practices which are incompatible with applicable anti-bribery laws - There is an absence of strong ethical leadership in the relevant business unit - There is evidence of past business ethics issues in the relevant business unit
Incentives (What's at stake?)	The individual transaction or activity is not significant in its financial or other consequences	- Individual transactions are large and/or significant in the context of the business - Individual transactions may not be large in value, but their consequences are potentially significant (e.g. procurement of a licence, permit, etc) - Success may drive significant rewards for individuals or organisations involved (e.g. commissions, success fees, bonuses, etc)
Opportunity	- Transactions or activities do not have higher risk characteristics - There is good evidence of effective anti-bribery controls	- The transaction has one or more of the following characteristics or features: - Interaction with government officials - Use of intermediaries - Typically higher risk (see examples considered in section 3 of this guide) - Complexity (multiple parties, phases, transactions) - There is evidence of absent or weak anti-bribery controls (aside from poor corporate culture dealt with above). These might include: - Poor governance generally and/or lack of oversight - Lack of clear policies - Lack of training and awareness - Weaknesses in financial controls - Lack of whistle blowing mechanisms or similar - Lack of monitoring and review

The well-known "fraud triangle" uses a similar categorisation of fraud risk factors to the approach used in the above table. It should be noted that, while the above factors include references to controls and examples of "control risk", the evaluation of likelihood is still fundamentally at the inherent level. The control related factors are generic and high-level and are likely to be based on general perception and experience, rather than specific to a particular risk area or to individual controls.

Aside from establishing a set of relevant risk factors, there is the question of how to 'score' a particular risk or business unit based on the extent of risk factors present. There is no single right answer as to how to measure the accumulation of risk factors and their impact on likelihood. Depending on the circumstances of each organisation and their existing approaches, possibilities might include:

- Taking the presence of any one or more specific risk factors as evidence of heightened risk;
- A simple count, with the greater number of risk factors indicating greater levels of risk;
- Giving each risk factor its own weighting such that some count for more than others.

Impact is a measure of the adverse effect of the defined risk event on the achievement of objectives. The impact of bribery risk is difficult to quantify.

4.2.2 Impact

The impact of a risk is a measure of the adverse effect of the defined event on the achievement of objectives. It follows that, however the objective itself is measured, the same basis of measurement needs to be assigned to the associated risks. As already indicated in the above discussion of likelihood, the more quantifiable the objective potentially impacted, the easier it is likely to be to quantify the risk itself in a meaningful way.

The sorts of objectives which are capable of being adversely effected by a bribery incident are very broad and potentially quite fundamental to the business as a whole. Many of them are inherently difficult, if not practically impossible, to quantify. If the objective is difficult to quantify, then so will be the risk.

The financial, legal/regulatory, commercial and reputational fallout from one or more bribery allegations will be difficult to predict. There is no easy equation to express the relationship between the characteristics of the offence and the scope of its consequences. Clearly, the scale of corrupt behaviour, its duration and prevalence, the identity and roles of those involved, the financial or other advantages sought or gained and the way the organisation responds to its discovery are all amongst the factors likely to influence the overall impact. As such, it will be noted that there is some degree of overlap between those factors that drive likelihood and those that drive impact.

SIGNPOST

Given the practical difficulties involved in assessing and distinguishing different bribery risks by reference to impact, organisations may choose to assume a default level of impact and focus their attention more on the risk factors that drive likelihood.

4.3 Differentiating individual bribery risks

Prioritisation of bribery risks is useful to the extent that individual risks can meaningfully be differentiated in terms of likelihood and impact. The key question is what difference the risk rating makes to how the risk is addressed.

To the extent that a series of different bribery risks can be differentiated meaningfully from each other in terms of likelihood and impact, this is clearly a helpful thing to do. It will assist one of the basic aims of risk management, which is to direct finite resources towards the mitigation of the most important risks. Conversely, where such risks cannot be usefully differentiated, then it may be less effective to attempt to do so. On a pragmatic note, some degree of differentiation is likely to enhance the credibility of the risk assessment with senior stakeholders in the organisation, who will be accustomed to the idea that business risks should be prioritised. They will want to understand how bribery risks rank between themselves and alongside other business risks.

There is always danger in trying to pin down too precisely which kinds of bribery are worse than others. No-one wants to be seen to condone any instance of bribery or downplay its seriousness. In certain circumstances even a small bribe can have big consequences. Furthermore, perceived tolerance of small bribes, facilitation payments and other examples which might seem somehow less egregious can send the wrong signal inside and outside the organisation and ultimately undermine efforts to mitigate the risk of more serious instances. To try to codify in advance and in the abstract which particular acts of bribery might be more or less likely, or have more or less impact, may seem – when looked at in this light – a somewhat hopeless task, not to mention one susceptible to endless debate.

The key question is what practical difference the categorisation of a particular risk makes to the nature and extent of efforts to mitigate it. Introducing too many risk levels adds complexity and the potential for confusion and inconsistency. Unless there is clarity about the distinction between the treatment of each level of risk, the value of greater differentiation is questionable. Examples of how different risk levels might drive different levels of mitigating response include:

- Different levels of authorisation of a relevant transaction or activity;
- Different scope of due diligence in relation to certain types of third party and/or outsourced activity;
- Different contractual requirements to be put in place in relation to certain types of third party and/or outsourced activity;
- Different levels of monitoring and review of certain transactions, activities or relationships.

In practice, a common solution is to define three different risk levels, and this is the approach adopted in the illustrative documented risk assessment matrix in Annex 2. This fits with a high/medium/low or red/amber/green schematic – two popular variants. Organisations that consider it useful to adopt more gradations than this should not feel discouraged from doing so. They should still find the general principles set out in this section of assistance. Equally, some organisations may only see benefit in defining two levels. If this is consistently followed through in terms of mitigating responses, there is no reason why this should not also be an appropriate approach. It should not be forgotten that risk evaluation is not an end in itself; its purpose is to help focus and prioritise.

The interaction of likelihood and impact

In conducting and documenting a bribery risk assessment, a practical decision has to be made about whether to record likelihood and impact separately, or as a combined rating, or both. Whether or not a combined rating is produced, there will in any event be a need to define a consistent basis for deciding how different combinations of likelihood rating and impact rating should be ranked. For example, is a low likelihood/high impact risk to be given greater or lesser priority than a high likelihood/low impact risk? Or are those two combinations equivalent on a net basis? Would they both be equivalent to a medium likelihood/medium impact risk?¹⁶

Is a low likelihood/high impact risk less or more significant than a high likelihood/low impact risk? In the context of bribery risk, there is an argument for giving more weight to impact.

These questions reinforce the qualitative nature of the exercise in which an exercise of judgement is necessary. They also prompt the further question of whether it is appropriate to give equal weight to likelihood and impact or whether one of these should be viewed as more important than the other. There is no single right answer to this question, either as to whether the two variables should be given different weighting at all, or what the appropriate relative weightings might be. But, given the potentially serious direct and collateral consequences of one or more bribery incidents – along with the challenges associated with evaluating likelihood – there is an intuitive argument for giving more weight to impact.

4.4 Business unit or market-level risk

An additional approach is to focus the risk evaluation on some meaningful and relevant type of unit within the business. This might be a business unit in the conventional sense of an operating company or a business division; or it might be a group of activities associated with a particular product or service, or with a business function (e.g. external affairs, government relations, sales and marketing, etc); or it might encompass all activities within a particular country or region.

The business unit or market risk approach is not an alternative to the basic bribery risk assessment described above; it is a possible addition to it. The business unit or market risk approach is based upon the assumption that the organisation has already identified and evaluated its key

¹⁶ The challenge of combination is increased further where quantitative measurement is attempted. Multiplying numerical ratings together to derive a kind of "expected value" in the statistical sense of the term risks creating a spurious numerical precision. (Such an "expected value" approach is really most appropriate to easily quantifiable, high volume risk events – characteristics not associated with bribery risk).

bribery risks, without which it will not be effective. The objective is to build on that foundation and to assess the relative level of risk present in different business units or markets.

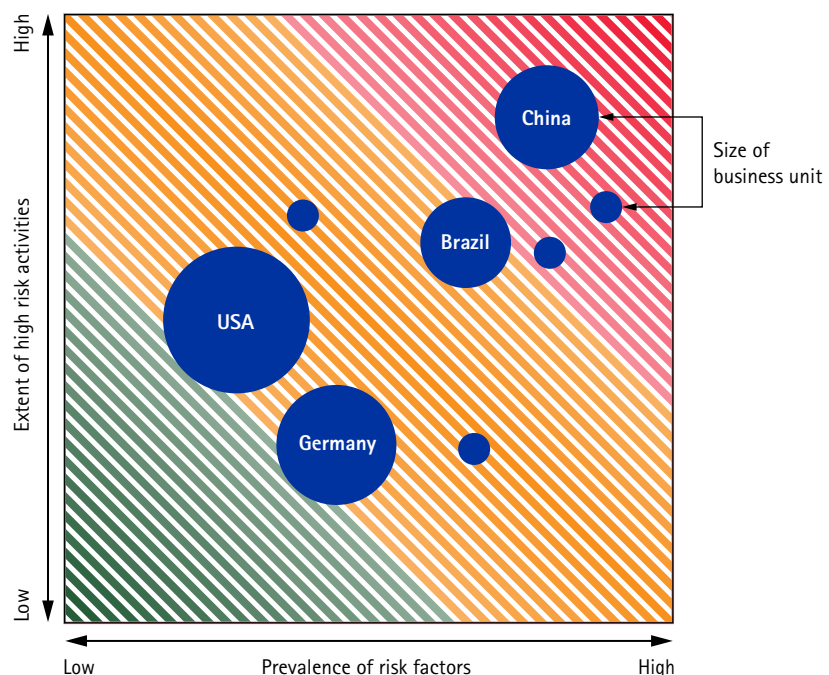
The benefit of a business unit evaluation of this kind is that it provides a potentially useful overview of which units or functions may need particular management focus, monitoring and review. This might be helpful in targeting efforts in areas such as internal audit, training and/or identifying the need for specific additional policies and procedures to counter localised risks. Larger and/or more complex organisations often have a number of quite distinct business streams, each of which has its own risk profile. Alternatively, the risks of doing the same business in different places may be assessed very differently depending on local culture, custom and practice.

As with all other aspects of the risk assessment process, there is no single right way of doing things, either in terms of inputs or outputs. Different variations have different numbers of dimensions. For example:

A business unit evaluation can help focus management attention, controls and monitoring and review efforts.

- At its simplest, a **one-dimensional** approach could be adopted simply by ranking business units according to the extent to which they are associated with risky activities;
- A **two-dimensional** approach could involve a second variable, such as the degree to which the business unit is associated with certain risk factors of the kind highlighted in the discussion of likelihood. A variation on this would be to capture whether a business unit has in place certain key controls. This would enable business units to be plotted on a two-dimensional diagram of some sort to distinguish them graphically;
- A **three-dimensional** approach might add a third variable, for example, some measure of the size of the unit (headcount, turnover, assets, or whatever measure is most pertinent to the nature, role and significance of the unit in question). This could be represented by the size of the business unit as depicted on the sort of diagram described under the two-dimensional approach above.

An example of what the three-dimensional approach might look like when represented graphically is shown in the diagram below.¹⁷



¹⁷ It should be noted that creation of such a diagram is most efficiently achieved by ascribing numerical values to the different variables and therefore to the individual risks and risk factors that underlie them so that scores for individual business units can be calculated by whatever formula is deemed appropriate and business units can then be placed in the correct relative position. What is important here is the relative ranking or positioning of different business units rather than their absolute score, which is entirely arbitrary.

SIGNPOST

Differentiating business units by size requires some caution. While size may assist in assessing the level of resource required to manage risk appropriately in relation to a business unit, it may not be the most reliable indicator of risk as such. History is littered with examples of bribery cases where the offence has occurred in relatively small business units or markets but has led to consequences far beyond the confines of those places.

Organisations carrying out business unit or market risk assessments will often gather much of the relevant input data from the business units themselves, perhaps by way of questionnaires or similar. This may be an efficient way of doing so, however care needs to be taken to ensure that there is appropriate quality control over the completeness, accuracy and consistency of the information provided.

5. NEXT STEPS: USING THE OUTPUT OF THE RISK ASSESSMENT

A detailed description of the steps that might be taken beyond the risk assessment process towards the full implementation of a proportionate, risk based anti-bribery programme falls outside the scope of this guide. This section provides a high-level overview and some general pointers to those next steps (each of which is a big subject in its own right), giving a wider perspective on how the risk assessment might be taken forward.

Following the process outlined in Section 1, the key next steps are:

- Planning and putting into action an appropriate response to the risk assessment, which involves:
 - Mapping risks on to existing controls;
 - Identifying gaps in existing controls in terms of risks not adequately addressed;
 - Designing and implementing appropriate remedial actions;
- Follow-up, monitoring and enforcement;
- Reporting.

5.1 Mapping risks on to controls

The controls mapping process should challenge whether existing controls are truly focused on the identified bribery risks.

The risk identification stage focuses on inherent risk and excludes consideration of controls. The risk evaluation stage, on the other hand, takes account of controls in a general sense in that evidence of weaknesses or gaps in control may constitute one of a number of risk factors (see Section 4).

Only once the risk assessment steps described in Sections 3 and 4 have been carried out, can the issue of what specific controls exist to mitigate each identified risk be considered and documented. In undertaking this exercise, the following points are worth noting:

- Some controls which exist for other purposes may also be co-opted as anti-bribery controls. These may need to be adapted to some extent. Controls over payment transactions would be an obvious example;
- When considering controls, it is important to be disciplined in analysing how a particular control is designed to mitigate the risk to which it is mapped. It is all too easy to assume, for example, that an existing approval process will prevent a corrupt payment. If such controls are focused merely on ensuring that certain documentation is in place, the more fundamental question of why a transaction is happening at all and whether it makes sense or looks right may not be picked up;
- Certain controls will cover more than one bribery risk; indeed, some may cover many or all bribery risks. Effective management communication, training and awareness raising programmes and similar over-arching anti-bribery procedures might fall into this category. These are not sufficient in themselves to prevent acts of bribery but they are an important element of the overall programme.

The output from the risk mapping process will be some form of risk matrix with relevant mitigating controls documented alongside the corresponding risks. Annex 3 provides an illustrative extract of how such documentation might look.

5.2 Gap analysis

An important by-product of the risk mapping process is the identification of risks for which there are no, or inadequate, controls. The identification of such issues is often referred to as a 'gap analysis'.

Gap analysis considers both specific unmitigated risks and general good practice guidance on effective anti-bribery programmes.

There are potentially two ways in which gaps in the anti-bribery programme may be identified. First, the absence of adequate controls to address a particular risk clearly constitutes a gap that needs to be filled. Secondly, certain controls may be identified not from consideration of individual risks, but from a wider consideration of established good practice in relation to the anti-bribery programme as a whole. For example, the absence of an effective whistle blower or equivalent mechanism might not naturally emerge from looking at specific bribery risks. On the other hand, looking at any of the main sources of general guidance on anti-bribery or compliance programmes would quickly reveal that some form of whistle blower or other secure reporting mechanism for employees (amongst others) is nowadays universally recommended (and in some cases required) for organisations other than the very smallest.

5.3 Remediation

An appropriate plan should be developed to address any identified gaps and to help mitigate the risk in a proportionate manner. Where significant remediation is required, then it will make sense to prioritise remedial actions to deal with the most critical gaps and/or those that can most easily be remedied first. The key phases of a remediation programme include:

- **Design:** Engaging with the business to share relevant parts of the assessment (and gaps), identifying resource and formulating policy and/or designing procedures that are specifically tailored to address a risk, or group of risks. The precise steps will depend on the nature the risk and of the control gap. For example, designing a suitable training programme will entail quite different steps, inputs and outputs from designing a new third party due diligence procedure;
- **Build:** Creating the necessary documentation, guidance and other necessary materials; putting appropriate organisational structures in place; drafting tailored communications, etc.;
- **Roll-out:** Launching new policies and procedures. This can be a phased process rather than launching everything at once. Crucially, those charged with implementation need to be equipped with the relevant knowledge and materials to do so, and have the knowledge that senior management support the changes;
- **Implementation:** Many organisations mistakenly believe that roll-out and implementation are one and the same thing – they are not. Implementation is an ongoing process and is the responsibility of those who run and work in the business. Implementation means working and doing business in accordance with the new policies and procedures on an ongoing basis.

It is a key management responsibility to monitor the effectiveness of the anti-bribery programme.

5.4 Follow-up, monitoring and enforcement

Ultimately, an effective anti-bribery programme must operate in practice, not just in theory. It is a key management responsibility to monitor the effectiveness of the programme in mitigating the risk of bribery. This might encompass, amongst other things:

- Ensuring effective implementation of policies and procedures;
- Monitoring the promulgation and understanding of training and other awareness raising communications;
- Appropriate real-time monitoring of high risk activities and relationships;
- Review and audit of high risk transactions;
- Obtaining appropriate periodic confirmations from employees and/or third parties of compliance with required standards;
- Robust responses to allegations of bribery or other non-compliant behaviour.

Effective enforcement must extend to third parties acting for, and on behalf of, the organisation. While there are practical limits to the extent to which an organisation can control the conduct of third parties, setting the right framework through the imposition of appropriate contract clauses will facilitate this. Such clauses might cover: acknowledgement of the organisation's code of conduct and policies; confirmation that the third party has equivalent policies and the necessary procedures to implement them; provision for periodic self-certification of the third party; provision in appropriate circumstances for the organisation to have some form of audit rights over the third party; and rights of termination for cause in cases of breach by the third party.

5.5 Reporting

An appropriate reporting regime should be established to ensure effective communication of the results of monitoring and enforcement, both internally and externally. The format and frequency of any reporting will depend on a range of factors, including the size and complexity of the organisation, the nature of the subject matter to be reported, the needs or requirements of the target audience and the purpose of a particular report.

Internally, reporting might include:

- Periodic updates for the Board on evolving risks and the status of implementation of the anti-bribery programme;
- Reports summarising internal audit and/or compliance monitoring findings;
- Reports of any alleged or actual breaches and the scope and findings of any investigation;
- A report or 'dashboard' highlighting activity in specific risk areas as part of a proactive monitoring regime.

Externally, reporting might include:

- Reporting on the organisation's risk assessment;
- Reporting on the organisation's anti-bribery programme;
- Reporting any alleged or actual breaches to relevant authorities.

ANNEX 1: BRIBERY RISK ASSESSMENT PROCESS CHECK LIST

The check list set out below is intended as an aide memoire for those charged with organising and carrying out a bribery risk assessment in their organisation. It is not exhaustive list but aims to cover the key elements outlined in this guide.

No.	Task	By whom	Completed (date)	Doc ref.
Planning, scoping and mobilisation				
1	Obtain Board level support for the risk assessment process including commitment to: a. Investment of appropriate time and resources b. Board communication of the importance of the exercise c. Personal participation of Board members as appropriate in the process			
2	Appoint project lead			
3	Define stakeholders, team, responsibilities and reporting lines			
4	Identify potential sources: a. People: Line and function b. Internal and external documents and data			
5	Establish risk assessment framework: a. Analyse business structure to determine how many distinct risk profiles there might be b. Determine the relevant business unit(s) to be covered c. Define appropriate information gathering procedures given extent and nature of information available d. Agree time frame for the exercise e. Define output(s)			
6	Draft risk assessment plan and time table			
7	Design any information capture templates required, for example: a. Pro forma risk matrices or similar b. Questionnaires			
8	Obtain any necessary approvals for the risk assessment process prior to commencement			
9	Formulate and communicate instructions to those contributing to the process, including: a. Context and importance b. General briefing on bribery risk and its potential impact c. Specific briefing on tasks to be undertaken d. Explanation of templates to be completed (if applicable) e. How to prepare for a risk assessment workshop (if applicable)			
10	Schedule any workshops or other interactive information gathering exercises			

No.	Task	By whom	Completed (date)	Doc ref.
-----	------	---------	------------------	----------

Information gathering and analysis

11	Review internally available documents and data for information relevant to the risk assessment. Such sources might include: a. Past experience of bribery issues (including experience brought by board members and employees from other organisations) b. Findings from internal audit reports, internal investigation reports, etc c. Country and market insights from management and employees in different countries. "Market insights" will include knowledge about local culture and business practices, customer and competitor behaviour, etc. d. Knowledge of local laws and regulations from the in-house legal team or local management e. Whistle blower or similar reports			
12	Conduct workshops and/or interviews with appropriate employees to gather insights about likely risk areas. Such employees might include those representing, where appropriate: a. The Board b. Line management for key businesses/markets c. Sales d. Procurement e. Internal audit f. Finance g. Legal h. Human resources i. Risk j. Compliance			
13	Gather information from business units and functions via questionnaires, risk assessment templates, or similar.			
14	Review relevant externally available documents and data, such as: a. MoJ Guidance b. Opinion releases and similar sources from the DoJ and SEC c. Guidance from industry bodies d. Published advice from professional advisers e. TI or other independent publications			
15	Collate and review information gathered from the above sources			
16	Follow up and challenge incomplete, inaccurate or inconsistent information (where applicable)			

No.	Task	By whom	Completed (date)	Doc ref.
Risk identification				
17	Has the risk assessment taken appropriate account of Country risk, considering, for example: a. Relevant cultural factors b. Local customs and business practices?			
18	Has the risk assessment taken appropriate account of Sectoral risk, considering, for example, such factors as: a. Requirement to operate in countries associated with high levels of corruption b. High degree of interaction with government c. High levels of regulation d. Prevalence of high value, complex and/or long term contracts e. Business activities involving multiple business partners, stakeholders and/or complex contractual or corporate structures?			
19	Does the risk assessment include (where applicable) typically heightened risk transactions, such as: a. Sales to government customers, particularly in higher risk countries b. Gifts, hospitality and travel expenditure, especially for government officials c. Use of company assets for the benefit of third parties for non-business purposes d. Charitable and political donations and other corporate relations activities e. Sponsorships f. Giving employment to persons connected with government officials g. Obtaining licences, permits and regulatory clearances of any kind h. Movement of goods across borders and related activities i. Lobbying governments on policy, legislation and/or regulation j. Other (specify)?			
20	Has the risk assessment taken appropriate account of Business Opportunity risk, considering, for example, the value, complexity or commercial rationale of transactions?			
21	Has the risk assessment taken appropriate account of Business Partnership risk, considering, for example: a. Use of intermediaries b. Joint ventures c. Consortia d. Other (specify)?			
22	Has the risk assessment taken appropriate account of other risk considerations, such as legal or regulatory risks?			

No.	Task	By whom	Completed (date)	Doc ref.
-----	------	---------	------------------	----------

Risk evaluation

23	Does the evaluation of risks identified take appropriate account of cultural risk factors (internal and external)?			
24	Does the evaluation of risks identified take appropriate account of factors that might create incentives for bribery?			
25	Does the evaluation of risks identified take appropriate account of factors that might create opportunities for bribery?			
26	Have the bribery risks identified been meaningfully evaluated and prioritised?			

Documentation

27	Have the results of the risk assessment been appropriately documented?			
28	Have the results of the risk assessment been communicated as appropriate to relevant stakeholders?			

ANNEX 2: RISK ASSESSMENT TEMPLATE

ILLUSTRATIVE DOCUMENTED EXAMPLE

This Annex contains an extract of an illustrative bribery risk assessment document. The format and content are consistent with the general principles set out in this guide, but they are not prescriptive and there are, of course, other possible formats which would be equally capable of fulfilling the objectives of an effective bribery risk assessment. Key points to note include the following:

- The illustrative risk assessment is generic and not tailored to any particular size of organisation, industry sector or geographical location.
- This same format might serve for a whole organisation, or for an individual business unit, market or function;
- The risk areas illustrated are by no means exhaustive of all risks that might be present in a business;
- The risk ratings ascribed to each risk area are illustrative only. Different circumstances might warrant different ratings in respect of the risk areas included.

The risk assessment pertains to a fictional commercial organisation, which manufactures and distributes a range of unspecified products. The organisation is a group with a head office and a number of production operations in various parts of the world. It currently exports its products to over 40 countries, where it operates through local sales and marketing subsidiaries and/or third party agents and distributors.

The format used in this Annex categorises bribery risks under two headings:

1. **Heightened risk transactions** – Identifies the sorts of transactions by which a bribe might be effected; and
2. **Activities** – Identifies business activities and/or relationships which might give rise to risk.

The rationale for this two-category approach is that:

- It avoids laborious repetition of the different ways in which a bribe might be paid in connection with each of the different risk areas; and
- It facilitates later controls mapping, as heightened risk transactions will generally be controlled in a similar way across different business areas and also for the same reason as above, namely that there is less repetition of risks against which controls need to be mapped.

The table below provides an explanation of the headings used in the illustrative bribery risk assessment document.

Heading	Explanation
Risk ID	A unique risk identifier for ease of reference.
Risk area	The transaction type or activity giving rise to the risk. This can be useful as a filter, enabling risks to be sorted by risk area.
Description	A reasonably detailed and specific description of the risk such as to enable any reader of the document to understand the nature of the risk and its relevance to the organisation (or relevant part thereof), highlighting where appropriate specific activities giving rise to the risk.
Active/Passive	Whether the risk is one of active or passive bribery, or both. This may be helpful in identifying the need for different responses to active and passive variants.
Public/Private	Whether the risk relates to bribery of public officials, employees of private enterprises or both. Again, a potentially useful filter, for example in highlighting all government interactions.
Risk rating	An indication of the assessed inherent risk level using a high/medium/low scale. Note that this is a composite risk rating of the kind discussed in section 4.3 of this guide, incorporating both likelihood and impact.
Business area/function	The business area of function subject to the risk. This may be a useful filter in analysing risks by the business area or function responsible for managing those risks.
Associated parties	Any third parties involved in a transaction or activity.

ILLUSTRATIVE RISK ASSESSMENT

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
1	Cash payments	Our policy is to avoid cash payments where possible. However, petty cash facilities are available for certain purposes in all locations. In addition, in some locations cash payments are necessary because of limited alternative means of money transfer. The risk therefore exists that cash payments could be used for improper purposes.	Active/ Passive	Both	High 	All	All
2	Gifts	Gifts are customary in many of our markets. There is a risk that an individual gift or a number of gifts in combination over time might improperly influence a recipient, or be seen to do so. This applies equally to third parties with whom we do business and to our own people in their dealings with others. There are some specific local customs and practices in our individual markets. These are captured in local market risk assessments and need to be managed and addressed locally.	Active/ Passive	Both	Medium 	All	All
3	Travel, hospitality and entertainment	We engage in a number of activities involving the provision to third parties of hospitality and entertainment. The majority of these expenditures are charged through our staff expenses system. We have on occasions also funded flights and other travel for certain government officials to view our facilities, which may also involve hospitality and entertainment as part of the package. There is a risk that such expenditures could be or be seen to be excessive or otherwise improper in the context of the activity to which they relate. There is also a risk that certain of our own staff might receive such benefits in a manner which compromises them in their role.	Active/ Passive	Both	Medium 	All	All
4	Sponsorships and grants	Historically, we have not engaged in sponsorships or grants. However, as we have grown the business in certain territories, we have increasingly received requests for such support. Accordingly, a decision has been taken that we will now do so on a strategic basis. The area of focus for sponsorships will be to support local cultural initiatives as an adjunct to our other community development activities. In doing so, we need to take account of the risk that such financial support might be or be seen to be linked to some specific commercial reward.	Active	Both	High 	All	All

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
5	Charitable donations	We make donations both in money and in kind to charitable organisations in the countries in which we have a presence. The causes to which such donations are made are a matter for local management to determine. While bona fide charitable donations are to be encouraged in line with the organisation's values, there is a risk that such contributions could be or be seen to be linked in some way to some specific commercial reward, and/or that an organisation we have understood to be a charity might transpire to be something else.	Active	Both	Medium 	All	All
6	Political donations	The organisation does not as a matter of strict policy make donations to any political party in any country. Nonetheless, care needs to be taken that transactions labelled under other categories are not in substance disguised political donations in return for some advantage. In certain countries, provision is made for individual employees to make personal political contributions on a voluntary basis as a deduction from payroll. There is a risk that the systems used to administer these deductions could be manipulated to hide a more substantial corporate donation that would breach policy.	Active	Public	Medium 	All	All
7	Discounts and rebates	In the normal course of business, discounts and rebates are offered to customers in both the private and public sectors. While this is common in our industry, the wide variety of arrangements and the relative complexity of some of them creates a degree of risk that such arrangements could be used to disguise improper inducements to individual customer representatives, for example by disguising the fact that free products have been provided to those persons as part of the overall deal.	Active	Both	High 	All	All, especially sales agents
8	Employment	Responsibility for the management of human resources, including hiring new staff, rests with individual business units. We operate in certain countries where family connections and personal relationships and allegiances may play a greater role in hiring decisions than we are used to in the UK. There is therefore a degree of risk that employment may be offered to an individual as an inducement or reward for some advantage to us granted by someone connected to that individual.	Active	Both	Medium 	All	All

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
---------	-----------	-------------	----------------	----------------	-------------	----------------------------	--------------------

Activities

9	Sales	We sell our products to a wide variety of customers in both the public and private sectors. We sell directly to customers and through a combination of sales agents and distributors. Although most of our products are not of very high value individually, we do have a significant number of high volume and long-term (multi-year) supply contracts with certain customers, such that the closing of these deals is of significant aggregate value to the business. There is a risk that either an employee or an intermediary might offer an inducement in order to make a sale.	Active	Both	High 	Sales & Marketing	Sales agents, distributors
10	Customs	Our products are manufactured in a limited number of regional centres, from which they are exported to other countries in that region. Key manufacturing centres are the UK, USA, Brazil, China and South Africa. Products are exported to over 40 other countries around the world, covering Europe, Americas (North and South), CIS, South East Asia and sub-Saharan Africa. We principally use two international logistics and freight forwarding companies, who manage both shipment and customs arrangements. In some countries, those companies employ other local agents to assist with local customs and excise authorities. We are billed for transport services as well as disbursements including local customs and excise charges. Our products are not perishable as such, but our customers will often order on a just-in-time basis. There is a risk that improper payments or other inducements might be offered by one of the above third parties in order to secure passage of our goods through customs within a specific time frame, or at all.	Active	Public	High 	Distribution	Logistics service providers, customs agents

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
11	Lobbying	Lobbying activities are generally limited, however we have had a number of situations over time where we have sought dialogue with local or central authorities around areas of concern. These have included: • Dialogue at ministerial level in one country where local policy was unfairly discriminating against our products. • Dialogue with senior customs officials in a number of territories where we have been unhappy about the interpretation of local regulations concerning the treatment of our products for excise purposes. • Dialogue with the Finance Ministry in one country to help resolve a dispute with the tax authorities concerning transfer pricing. In some of the above cases we have engaged intermediaries to assist us in gaining access to the right people and in advising us how best to put our case. There is a risk that we or an intermediary on our behalf might offer or be seen to offer an improper inducement in the context of lobbying activities.	Active	Public	High 	Group CEO, Local General Managers, Group Tax	Lobbyists
12	Licences and permits	Our business is subject to the requirement to hold a range of permits and licences, the details of which vary from one jurisdiction to another. These include: • Factory operating licences • Building permits for new or extended facilities • Health and safety certificates • Licences to store and handle certain hazardous materials • Waste disposal licences • Export and/or import licences We have in the past encountered a few local difficulties in obtaining these in certain countries. We are also aware of cases where other companies have suffered severe disruption, including temporary forced closure of plants, as a result of failing to obtain or renew licences. There is a risk that we or a third party on our behalf might offer an improper inducement to obtain or retain a critical licence. We generally deal directly with the authorities on these matters.	Active	Public	High 	Manufacturing, Distribution	Planning consultants (building permits)

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
13	Tax	We operate sales and marketing companies in some of our key export markets. These import and on-sell our products locally and regionally. They pay corporation tax on profits and are subject to regular scrutiny in relation to transfer pricing. They also have to account for local sales taxes. Our manufacturing companies are also subject corporate and sales taxes. All operations are subject to periodic tax audits covering corporation, sales and employment tax compliance. We use tax advisers both to advise us on our tax position and also to negotiate on our behalf, where necessary, with the authorities. In certain countries the tax authorities are bureaucratic and unpredictable. There is a risk that we or a third party on our behalf might offer, or be seen to offer, an improper inducement to a tax official in order to resolve a tax issue.	Active	Public	Medium 	Group Tax	Tax advisers
14	Legal disputes	We have been involved in a number of patent disputes, both as claimant and as defendant. So far our experience has been relatively good in terms of the way those cases have been handled and resolved. However, as we increase production and/or sales in countries with less reliable justice systems and a lesser degree of respect for patents and intellectual property rights generally, we expect to see an increase in activity in this area. We need to be cognisant of the risk that we or a third party on our behalf might offer or be seen to offer an improper inducement in order to obtain a favourable resolution of a legal dispute.	Active	Public	Medium 	Group Legal	Legal advisers
15	Anti-counterfeiting	We have had problems in two markets in particular in relation to counterfeiting. Our response has been to work with the appropriate authorities in those countries to identify and close down counterfeiting operations. This has involved certain of our employees developing close working relationships with local law enforcement officers. We have also provided certain logistical and financial support to the relevant law enforcement agencies. There is risk that expenditures incurred in the context of anti-counterfeiting operations might extend, or be seen to extend, beyond what is appropriate.	Active	Public	Medium 	Group legal	–

Risk ID	Risk area	Description	Active/ Passive	Public/ Private	Risk rating	Business unit/ function	Associated parties
16	Joint ventures	Our Chinese manufacturing facility is operated by a joint venture between us and a local Chinese-owned company. Ownership of the JV is split 50:50, as is the board of the JV, albeit that we have the right to nominate the Chairman of the board, who has a casting vote. The JV sells our products within China and across the Asia-Pacific region. There is some risk that we could be exposed – reputationally, if not also legally – as a result of bribery by (a) the JV itself; and (b) the Chinese co-owner.	Active/ Passive	Both	High 	Group Board, local China Board	All
17	Acquisitions	As part of the strategic expansion of our product range, we will continue to make targeted acquisitions of companies that complement our current business. Many of the most exciting opportunities in this regard are in emerging markets. There is a risk that a company we acquire may have engaged or continue to engage in bribery for which we would be held responsible post completion.	Active/ Passive	Both	High 	Group Board, Group M&A	All
18	International mobility	We have relocated a number of our key people from the UK and other developed markets to help establish or build our business particularly in emerging markets. This requires obtaining work permits, dealing with personal tax matters, etc. We use visa and relocation agents to assist with this. We expect to see more such movements in the future. There is a degree of risk that we or a third party on our behalf might offer an improper inducement in order to obtain some item of documentation in relation to an international mobility matter.	Active	Public	Low 	Group HR	Visa agents, relocation agents
19	Security	In South Africa and Brazil in particular we have had a number of security issues around our manufacturing facilities. In both countries we have requested additional surveillance from local police forces. In return we have provided proportionate financial and logistical support to those forces, but not to individual police officers, except for the provision of basic refreshments while they are patrolling our facilities. There is risk that expenditures incurred in the context of our support for police operations might extend, or be seen to extend, beyond what is appropriate.	Active	Public	Medium 	Group Security, Local Security	–

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/ function	Associated parties
20	Corporate social responsibility ("CSR")	We engage in a number of activities aimed at benefiting the wider community in the places we operate. These include a number of activities dealt with and separately risk rated elsewhere in this document, namely: a. Charitable donations b. Sponsorships In addition to the above, we produce an annual report on our initiatives, which includes information not only about our community activities, but also our environmental impact, health and safety record, employee welfare and development and other matters important to our reputation and values. Some of the information is collated with the assistance of third parties and some of it is subject to external verification and "audit". There is some risk that we or a third party on our behalf might offer an improper inducement in order to procure the distortion or manipulation of information concerning our CSR key performance indicators. While considered remote, the impact of such a case would be significant in terms of loss of public trust or worse.	Active	Both	Medium 	Community relations	Third party information providers
21	Intermediaries	As indicated throughout this risk assessment document, we make use of intermediaries in connection with a number of key business interactions. The risks associated with the use of intermediaries will vary depending on the nature of the activity they undertake and the third parties with whom they interact on our behalf. Accordingly, such risks are considered in the context of those individual risk areas.	Active	Both	Various – see specific risk areas	All	All

ANNEX 3: RISK ASSESSMENT TEMPLATE INCLUDING CONTROLS MAPPING – ILLUSTRATIVE EXTRACT

This Annex sets out a template to illustrate how a controls mapping exercise might be built on to a documented risk assessment exemplified in Annex 2. As with Annex 2, this template is illustrative only and there are, of course, other ways in which the same objective might be achieved. The suggested format highlights three different forms of mitigating control, namely:

1. Policies and procedures;
2. Training and communication; and
3. Monitoring and review.

As stated in section 5, it is important that consideration is given to how a particular risk area is specifically addressed by the control in question. This will enable any gaps to be identified and appropriate remedial steps to be designed and implemented.

Risk ID	Risk area	Description	Active/Passive	Public/Private	Risk rating	Business unit/function	Associated parties	Mitigating controls		
								Policies and procedures	Training and communication	Monitoring and review

Heightened Risk Transactions

1	Cash payments	Our policy is to avoid cash payments where possible. However, petty cash facilities are available for certain purposes in all locations. In addition, in some locations cash payments are necessary because of limited alternative means of money transfer. The risk therefore exists that cash payments could be used for improper purposes.	Active/Passive	Both	High	All	All	Petty cash is operated on an imprest system. A petty cash ledger is maintained and regularly reconciled. All cash payments above [£ limit] require General Manager approval. Cash payments are being phased out where possible.	All employees receive e-learning. Targeted classroom training is provided for senior and front line staff. Training includes: – General bribery risk awareness – Risks related to cash transactions – Briefing on policies and procedures relating to cash.	Internal audit include petty cash in routine audit work. Special internal audit procedures are carried out in those operations where cash transactions are prevalent. Group Board monitoring of larger cash payments.
---	---------------	---	----------------	------	------	-----	-----	---	--	---

ANNEX 4: GLOSSARY OF TERMS

The table below contains brief definitions or explanations of some of the terms and abbreviations used in this guide.

Term	Definition/explanation
Bribery, active	The offering, promising or giving of an advantage as an inducement for an action which is illegal, unethical or a breach of trust.
Bribery, passive	The accepting or soliciting of an advantage as an inducement for an action which is illegal, unethical or a breach of trust.
Control risk	The risk that a control will fail to fulfil its preventative or detective function, whether as a result of poor design, inadequate operation or circumvention.
Corruption	The abuse of entrusted power for private gain.
DoJ	The US Department of Justice
FCPA	The US Foreign Corrupt Practices Act 1977
FSA	The Financial Services Authority in the UK , succeeded in its regulatory and enforcement functions in 2013 by the Financial Conduct Authority
Inherent (or gross) risk	An estimation of risk before taking account of the existence and effectiveness of controls or other mitigating factors.
Intermediary	A third party which intercedes or otherwise acts on behalf of a commercial organisation in relation to other third parties, such as customers, suppliers, government agencies and officials. Examples of intermediaries may include (without limitation): Sales agents, distributors, customs agents and freight forwarders, lobbyists, lawyers, tax advisers, advertising agents, event organisers, visa agents, introducers and "consultants".
MoJ	The UK Ministry of Justice
MoJ Guidance	The document entitled Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing issued by the MoJ in March 2011 pursuant to section 9 of the UK Bribery Act.
Residual (or net) risk	An estimation of risk after taking account of the existence and effectiveness of controls or other mitigating factors.
Risk	The possibility that an event will occur and adversely affect the achievement of objectives.
Risk evaluation	The exercise of estimating the potential significance of a given risk, and/or seeking to establish an indication of the relative importance of each risk to the organisation concerned.
Risk factor	A characteristic or circumstance tending to increase the level of risk.
Risk identification	The exercise of identifying, characterising and – where appropriate – quantifying a set of risks
Risk tolerance	(See also the definition of "Risk") The acceptable level of variation in performance relative to the achievement of objectives.
SEC	The US Securities and Exchange Commission
SME	Small and medium sized enterprise
UK Bribery Act	The Bribery Act 2010, which came into force in the UK on 1 July 2011.

This document is part of series of tools and indices published by Transparency International that can help companies reduce corruption.

Indices and corruption assessments

Bribe Payers Index

Corruption Perceptions Index

Global Corruption Barometer

National Integrity System assessments

Guidance

Adequate Procedures – Guidance to the UK Bribery Act

Anti-Bribery Due Diligence for Transactions

Business Principles for Countering Bribery

Doing Business Without Bribery

RESIST

All these documents are available free of charge from
www.transparency.org
www.transparency.org.uk

£25

This publication has been provided free of charge by Transparency International UK. We depend on donations to allow us to continue our work. A contribution of £25 per reader will enable us to do so. If you would like to make a donation of any size, please visit:
www.transparency.org.uk/donate



Transparency International UK
32-36 Loman Street
London SE1 0EH
Tel: 020 7922 7906
info@transparency.org.uk
www.transparency.org.uk