

***Anti-bribery and  
corruption systems  
and controls in  
investment banks***

## CONSULTATION

*This report contains a reminder of existing guidance where appropriate and adds new examples of good and poor practice we have identified. To make it as simple as possible, we have consolidated the existing guidance, and proposed new guidance, in Section 4 of this report. We have highlighted the proposed new guidance in that section in bold italics.*

*Please see GC12/5 for our consultation on the proposed new guidance, to which we are inviting you to respond. Please note that we are not consulting on our findings.*

# Contents

<b>1 Executive Summary</b>	<b>5</b>
1.1. Introduction	5
1.2. Findings	5
1.3. Conclusions	6
<b>2 Introduction</b>	<b>8</b>
2.1 Objectives	8
2.2 Background	8
2.3 Methodology	8
2.4 Firms' legal and regulatory responsibilities	10
2.4.1 Legal obligations under the Bribery Act	10
2.4.2 FSA rules and principles	10
<b>3 Findings</b>	<b>12</b>
3.1 Governance and management information	12
3.1.1 The use of MI	13
3.1.2 Governance and management information – examples of good and poor practice	14
3.2 Assessing bribery and corruption risk	14
3.2.1 Triggers for risk assessment	15
3.2.2 Creating a risk assessment	16
3.2.3 Updating the risk assessment	18
3.2.4 Apportionment of responsibilities	18
3.2.5 Risk assessment – examples of good and poor practice	19
3.3 Policies and procedures	20
3.3.1 Reviews of existing ABC policies and procedures	20
3.3.2 Code of conduct	21
3.3.3 Monitoring and review of ABC policies and procedures	22
3.3.4 Responsibility for policy and dealing with breaches	23
3.3.5 Policies and procedures – examples of good and poor practice	24
3.4 Third-party relationships and due diligence	25
3.4.1 Categorisation and business use of third parties	25
3.4.2 Establishing a definitive list of third parties	26
3.4.3 Risk-sensitive approach to due diligence	27
3.4.4 Risk factors and red flags	27

3.4.5	Approving third parties	28
3.4.6	Monitoring and review of third-party relationships	29
3.4.7	Our testing of the quality of due diligence	30
3.4.8	Third-party due diligence – examples of good and poor practice	31
3.5	Payment controls	32
3.5.1	Payment controls – examples of good and poor practice	33
3.6	Gifts and hospitality	33
3.6.1	Risk assessment	34
3.6.2	Culture and senior management oversight	35
3.6.3	Limits	36
3.6.4	Approvals	36
3.6.5	Monitoring	36
3.6.6	Political and charitable donations	38
3.6.7	Gifts and hospitality policy – examples of good and poor practice	39
3.7	Staff recruitment and vetting	40
3.7.1	Staff recruitment and vetting – examples of good and poor practice	42
3.8	Training and awareness	43
3.8.1	Training and awareness – examples of good and poor practice	45
3.9	Remuneration structures	45
3.9.1	Remuneration structures – examples of good and poor practice	46
3.10	Incident reporting	47
3.10.1	Whistleblowing	47
3.10.2	Incident reporting and management – examples of good and poor practice	48
4	Consolidated examples of good and poor practice	49

# 1 Executive Summary

## 1.1 Introduction

- 1 This report describes how investment banks and firms carrying on investment banking or similar activities in the UK (collectively referred to here as ‘firms’) are managing bribery and corruption risk in their businesses and sets out the findings of our recent thematic review. We expect regulated firms in all sectors to consider our findings and examples of good and poor practice, as they may also be relevant to firms in other sectors which are subject to our financial crime rules in SYSC 3.2.6R or SYSC 6.1.1R.<sup>1</sup>
- 2 We require regulated firms to establish and maintain effective systems and controls to mitigate financial crime risk. Financial crime risk includes the risk of bribery and corruption. (We summarise regulated firms’ regulatory responsibilities in this area in Section 2.4.) In addition to these regulatory requirements, bribery, whether committed in the UK or abroad, is a criminal offence under the Bribery Act 2010, which has consolidated and replaced previous anti-bribery and corruption legislation in the UK. We do not enforce, or give guidance on, the Bribery Act.

## 1.2 Findings

- 3 We found that, although some investment banks had completed a great deal of work to implement effective anti-bribery and corruption (ABC) controls, most had more work to do. Our key findings are set out below:
  - a) Most firms had not properly taken account of our rules covering bribery and corruption, either before the Bribery Act or after. There are fundamental differences between the two described in this report. For example, our rules require firms to put in place systems and controls to mitigate bribery and corruption risk and we do not need to find evidence of bribery taking place to take action against firms that fail to meet our requirements.
  - b) Nearly half the firms in our sample still did not have an adequate ABC risk assessment, although progress has been made since the implementation of the Bribery Act.
  - c) Management information (MI) on ABC provided to senior management was poor, making it difficult for us to see how firms’ senior management could carry out their oversight functions effectively.

---

<sup>1</sup> The findings and good practice will also be of interest to electronic money institutions and payment institutions within our supervisory scope.

- d) The majority of firms had not yet thought about how to monitor the effectiveness of their ABC controls. Only two firms had either started or carried out specific anti-bribery and corruption internal audits.
- e) Firms' understanding of bribery and corruption was often very limited.
- f) There were significant weaknesses in firms' dealings with third parties used to win or retain business, including in relation to compliance approval; due diligence; politically exposed persons (PEP) screening; ensuring and documenting a clear business rationale; risk assessment; and regular review.
- g) Many firms had recently tightened up their gifts, hospitality and expenses policies by prohibiting facilitation payments, increasing senior management oversight of expenses and introducing or revising limits. But few had processes to produce adequate MI, for example, to ensure gifts and expenses in relation to particular clients/projects were reasonable on a cumulative basis.
- h) Firms had well-established vetting processes in place when staff were recruited, but bribery and corruption risk had not usually been a factor in identifying high-risk roles which should be subject to enhanced vetting.
- i) Since the implementation of the Bribery Act, firms had generally provided adequate basic training to staff. But most (i) were still developing training for staff in higher risk roles and (ii) had no processes in place to assess the effectiveness of existing training.

### **1.3 Conclusions**

- 4 We are concerned that the investment banking sector has been too slow and reactive in managing bribery and corruption risk. Although we were frequently told about high expected standards of ethics and 'zero tolerance' of bribery and corruption, most firms had historically failed to ensure adequate systems and controls to identify, manage and control the bribery and corruption risks to which they were exposed. In particular, the introduction of the Bribery Act, and our visits, were the main triggers for many firms in our sample to review, or consider for the first time, their approach to ABC. And none of them had taken action or considered taking action in response to our 2010 thematic review of commercial insurance brokers' ABC controls or our related enforcement actions against Aon Ltd and Willis Ltd.
- 5 As a result, we found that some firms still had significant work to do to get an adequate ABC control framework in place. Those firms fell short of our regulatory requirements and we have highlighted where they need to improve. In addition, we are considering whether further regulatory action is required in relation to certain firms in our review. However, many firms had recently made significant progress to identify or reassess bribery and corruption risks and factor them into their ABC controls, including policies, procedures, training and monitoring programmes.

- 6 The FSA and, from next year, the Financial Conduct Authority will continue to focus on ABC issues in this sector and beyond to ensure firms are meeting their legal and regulatory obligations.

## 2 Introduction

### 2.1 Objectives

- 7 This report is the result of a thematic review to examine how firms mitigate bribery and corruption risk. Bribery and corruption risk is the risk of the firm, or anyone acting on its behalf, engaging in bribery or corruption. The main purpose of the review was to assess how effectively the firms we visited address the risk of becoming involved in bribery and corruption.

### 2.2 Background

- 8 In January 2009, we fined Aon Ltd £5.25m for failing to take reasonable care to establish and maintain effective systems and controls to counter the risks of bribery and corruption associated with making payments to overseas third parties. We subsequently carried out our thematic review of ABC controls in commercial insurance broking, published in 2010. In July 2011, we fined Willis Ltd £6.9m for similar regulatory failures to those of Aon Ltd. Both the Aon and Willis fines reflected a 30% discount for early settlement of the case.
- 9 Our 2010/11 Business Plan stated our intention to extend the scope of our anti-bribery and corruption work to investment banks.
- 10 We consolidated our expectations of firms' ABC systems and controls in our regulatory guide, *Financial Crime; a guide for firms* (the Guide), which came into force in December 2011. The Guide includes good and poor practice identified in our 2010 report on ABC systems and controls in commercial insurance brokers.
- 11 This report summarises the findings of our review. It contains a reminder of existing guidance where appropriate and adds new examples of good and poor practice identified in this review. The existing guidance, and proposed new guidance, is consolidated for ease of reference in Section 4 of this report and the proposed new guidance is highlighted in that section in bold italics. Please see GC12/5<sup>2</sup> for details of our consultation on the proposed new guidance, to which you are invited to respond. This guidance will be reflected in the Guide. We are not consulting on our findings.

### 2.3 Methodology

- 12 Our visits began in August 2011 and were completed in January 2012. We visited 15 firms, including eight major, global investment banks and a number of smaller operations which carry on niche investment banking or similar activities. Our sample firms were chosen mainly to ensure a good spread of

---

<sup>2</sup> See [www.fsa.gov.uk/static/pubs/guidance/gc12-05.pdf](http://www.fsa.gov.uk/static/pubs/guidance/gc12-05.pdf)



firms by size. The vast majority carried on business in countries and sectors, or with clients, which exposed them to higher levels of bribery and corruption risk. In addition, many of them used introducers or consultants to win some of this business, increasing the risk of bribery and corruption. None of the firms were selected because of pre-existing concerns about their ABC systems and controls. We therefore consider our sample to be broadly representative of investment banks and other firms carrying on investment banking-type activities.

- 13 Before we began our review, we consulted a range of stakeholders, including the Serious Fraud Office, the Serious Organised Crime Agency, the Ministry of Justice, the British Bankers' Association and Transparency International.
- 14 We then got information from all firms before visiting them, including: relevant policies and procedures; risk assessments; details of third-party relationships; relevant Board and Committee minutes; and relevant audit reports. In addition, we obtained details of countries in which the firms operated, lists of payments made to overseas third parties, gifts and hospitality registers, relevant suspicious activity reports (SARs), details of remuneration structures and training material.
- 15 We interviewed staff in key roles to understand how firms identified, assessed and managed bribery and corruption risks and at what level in the management structure it was considered. Where firms had identified an ABC 'champion', we met that person. We also met staff responsible for ABC at an operational level; the officer nominated to make SARs; business heads whose departments used third-party introducers; and staff from accounts, risk assessment, human resources, compliance and internal audit.
- 16 Where firms used third parties to win business, we discussed payments made to them. We also examined due diligence on third parties to ensure the business case for using them was fully understood, and the risk assessed and appropriately documented by the firm.
- 17 We assessed the following topics in relation to anti-bribery and corruption:
  - governance and management information (section 3.1);
  - assessing bribery and corruption risk (section 3.2);
  - policies and procedures (section 3.3);
  - third-party relationships and due diligence (section 3.4);
  - payment controls (section 3.5);
  - gifts and hospitality (section 3.6);
  - staff recruitment and vetting (section 3.7);
  - training and awareness (section 3.8);
  - remuneration structures (section 3.9); and
  - incident reporting (section 3.10).

We would like to thank the firms that participated in our review and for the information they supplied in relation to our visits. We would also like to thank the stakeholders for their advice and assistance.

## 2.4 Firms' legal and regulatory responsibilities

### 2.4.1 Legal obligations under the Bribery Act

18 The Bribery Act came into force on 1 July 2011. It consolidated and replaced long-standing anti-corruption legislation. There are now four bribery offences: bribing another person; being bribed; bribing a foreign public official; and commercial organisations failing to prevent bribery.

19 Although not obligatory under the Bribery Act, it is a defence for firms charged with failing to prevent bribery to show that they had adequate anti-bribery procedures in place. The Ministry of Justice has published guidance (the MOJ Guidance) on what adequate anti-bribery procedures can be.

### 2.4.2 FSA rules and principles

20 We do not enforce the Bribery Act. But corrupt conduct in FSMA<sup>3</sup>-authorised firms affects at least two of our statutory objectives:

- *Reducing the extent to which it is possible for a financial business to be used for a purpose connected with financial crime* because bribery and corruption are financial crimes; and
- *Maintaining market confidence*, because bribery and corruption distorts competition and could affect the UK financial market's reputation.

21 The FSA therefore seeks to ensure that regulated firms adequately address the risk that they – or anyone acting on their behalf – act corruptly. The following rules and principles<sup>4</sup> are particularly relevant to bribery and corruption issues:

- *Principle 1*: A firm must conduct its business with integrity.
- *Principle 2*: A firm must conduct its business with due skill, care and diligence.
- *Principle 3*: A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
- *SYSC 6.1.1R*<sup>5</sup>: A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable,

---

3 The Financial Services and Markets Act 2000.

4 E-money institutions and payment institutions are not subject to our Rules and Principles but must satisfy us that they have robust governance, effective risk procedures and adequate internal control mechanisms. So the guidance in this report is also relevant to them.

5 For insurers, managing agents and Lloyd's, the equivalent provision is SYSC 3.2.6R.

tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime.

- 22 Other rules are also important in this context. For example, SYSC 5.1.1R requires firms to employ people with the skills, knowledge and expertise necessary for the discharge of the responsibilities allocated to them. SYSC 9.1.1R requires firms to keep records sufficient to enable us to monitor their compliance with our rules. And Principle 11 requires firms to disclose to the FSA appropriately anything relating to the firm of which we would reasonably expect notice. This is likely to include any instances of staff, or others acting on the firm's behalf, engaging in bribery and corruption.
- 23 We do not prescribe how firms should comply with our principles and rules. But they should be able to demonstrate that they can identify and assess bribery and corruption risk, and take reasonable steps to prevent bribery and corruption taking place.

# 3 Findings

## 3.1 Governance and management information

- 24 A firm's senior management is responsible for ensuring that the firm conducts its business with integrity and tackles the risk that the firm, or anyone acting on its behalf, engages in bribery and corruption. To this end, we expect senior management to understand the bribery and corruption risks faced by the firm, the materiality of the risks to its business, and the extent to which the firm's ABC systems and controls are adequate and effective. So it is important that firms' senior management is kept up to date with, and stays fully abreast of, bribery and corruption issues.
- 25 We assessed how firms' governance arrangements enabled senior management to fulfil their functions in relation to ABC. We considered how firms allocated responsibility for ABC, the degree of engagement and awareness on the part of firms' Boards and the quantity and quality of MI provided to those ultimately responsible for ABC systems and controls.
- 26 Most firms used senior committees which reported to their board of directors, to drive the ABC agenda. In addition, two firms had appointed senior managers to 'champion' their ABC approach. In both cases, these individuals worked in conjunction with compliance or relevant committees and were a point of focus for staff to discuss or raise questions about ABC issues.

*In one large firm, senior management was well engaged with the ABC framework. It was clear that various control areas, including compliance, could rely on senior management to reinforce ABC messages to the business and that well established governance committees were in place to discuss ABC-related issues.*

- 27 Most of the smaller firms we visited considered their size a benefit in promoting a good ABC culture and sharing information about key risks. While we acknowledge these potential benefits, formal governance controls should also be in place.

*In one small firm, the CEO said the firm's size made it easy to communicate with everybody throughout the organisation. He added that 'staff understand the A-Z of what is going on, as there are not many layers for getting access to information'.*

### 3.1.1 The use of MI

- 28 MI must be both accurate and informative to help firms' senior management take responsibility for the mitigation of bribery and corruption risk. What constitutes accurate and informative ABC MI will be different in each firm, depending on the types of bribery and corruption risk within their business. For example, firms may or may not use third-party business introducers.
- 29 Good quality MI should enable senior management and the Board to fulfil their functions by providing information, including an overview of the bribery and corruption risks faced by the business, systems and controls to mitigate those risks, information about the effectiveness of those systems and controls, and legal and regulatory developments.

*In one small firm, all three group business heads said that no ABC MI had been received by the Board. It became evident during our visit that cross-group information had never been presented to the Board and that there was no Board level oversight of the highest bribery and corruption risks in the firm's business.*

- 30 Given the number of recent significant developments in the ABC legal and regulatory guidance for firms, we were disappointed that none of the firms visited provided good quality ABC MI to their senior management or their Boards.

*Two large firms stated that the development of quantitative and qualitative MI was proving to be a real challenge, and many firms spoke of initiatives to produce ABC MI that were at different stages of development – some very early.*

- 31 Several firms' MI focused solely on the progress of projects to improve compliance with the Act and our rules, but did not consider the bribery and corruption risk inherent in their business. Progress reports on key projects may form an important part of MI, but this should not be at the expense of other relevant information such as the level of risk faced or the effectiveness of controls.

*In one firm, the Head of Compliance said he was unsure about what MI should be produced for bribery and corruption and needed to consider further how best to provide senior management with MI specific to ABC.*

#### **MI on third-party relationships**

- 32 We visited 11 firms that used third parties to introduce business leads. None produced sufficiently detailed MI on its third-party relationships.

*One large firm acknowledged that, overall, governance over third-party relationships required strengthening.*

- 33 As set out in our report on ABC in commercial insurance broking, we consider it to be good practice, where appropriate, for MI to cover information about third parties, including new third-party relationships; their risk classification; higher risk third-party payments for the preceding period; and unusually high commission or fees paid to third parties.

### **3.1.2 Governance and management information – examples of good and poor practice**

#### ***Good practice***

- Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate terms of reference and senior management membership, reporting ultimately to the Board.
- Regular and substantive MI to the Board and other relevant senior management forums including an overview of the bribery and corruption risks faced by the business, systems and controls to mitigate those risks, information about the effectiveness of those systems and controls and legal and regulatory developments.
- Where relevant, MI includes information about third parties including (but not limited to) new third-party accounts, their risk classification, higher risk third-party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties.
- MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption.
- Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.

#### ***Poor practice***

- Failing to establish an effective governance framework to address bribery and corruption risk.
- Failing to allocate responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee.
- Little or no MI sent to the Board about bribery and corruption issues, including legislative or regulatory developments, emerging risks and higher risk third-party relationships or payments.

## **3.2 Assessing bribery and corruption risk**

- 34 Identifying and assessing bribery and corruption risk is a prerequisite for an effective ABC control framework. It is also a regulatory requirement. Bribery

and corruption risk is the risk of the firm, or anyone acting on the firm's behalf, engaging in bribery or corruption. We expect firms to identify, assess and regularly review and update their bribery and corruption risk assessment. The risk assessment should be also used to inform the development of monitoring programmes; policies and procedures; training; and be embedded into operational processes.

- 35 When reviewing firms' approaches to assessing bribery and corruption risk, we considered the extent to which firms were aware of, and understood, their legal and regulatory obligations, and the extent to which the risk assessment took account of these obligations. We also considered the extent to which firms' processes enabled them to identify bribery and corruption risks specific to their business and to assess the extent to which these risks were materially relevant to the firm.

*One large firm told us it had conducted a gap analysis of the Aon Ltd and Willis Ltd anti-bribery and corruption cases in order to inform its risk assessment. However, they were unable to provide us with documentary evidence to support this.*

- 36 All firms claimed they adopted a 'zero tolerance' approach to bribery and corruption and we found they had all undertaken at least some level of risk assessment. However, the number and range of risk factors they used to inform their risk assessments varied considerably, even after taking into account expected variations due to different sizes and levels of exposure to ABC risk of the firms in our sample. And we were concerned that nearly half of the firms in our sample were significantly less well advanced in terms of their ABC risk assessment than we would have expected.
- 37 The risk factors considered by firms included: client/project type; country risk; sector risk; involvement with public bodies/PEPs; business activity; the use of third parties such as introducers, advisers and consultants; and certain activities or transactions (eg, charitable contributions, mergers and acquisitions, export finance, fund raising); and internal processes such as hospitality/gifts/hospitality, procurement, corporate hires and staff remuneration and training.

### **3.2.1 Triggers for risk assessment**

- 38 We were concerned to find that, despite a long-standing regulatory requirement to identify, manage and monitor the risks to which a firm is – or might be – exposed, around a third of firms carried out an assessment of their bribery and corruption risk for the first time in response to the introduction of the Bribery Act. Moreover, none of the firms in our sample had taken action in response to our 2010 thematic review of wholesale insurance brokers' ABC controls and our enforcement notices to Aon Ltd and Willis Ltd. One firm even dismissed the Aon case as 'irrelevant'.



*Two small firms had adopted different approaches, in that one had incorporated bribery and corruption risk in a more general financial crime risk assessment and the other had included it in an anti-money laundering risk assessment.*

- 39 Firms that had carried out an ABC risk assessment before the Bribery Act came into force gave two main reasons for revising that assessment. First, it needed to be extended to cover bribery in the private sector as well as bribery of public officials. Secondly, the assessment needed to take account of the Bribery Act's reach beyond the UK.

*Two firms specifically mentioned that compliance with US legislation (The Sarbanes Oxley Act 2002 and the Foreign Corrupt Practices Act 1977) had driven their ABC control framework prior to the Bribery Act.*

- 40 We were also concerned to find that a significant number of firms did not have a clear definition of bribery and corruption. As a result, not all firms had a clear understanding of what constitutes bribery and corruption. If firms are not aware of the full extent of their legal and regulatory obligations, or fail to understand the nature of the risk they are assessing, they risk failing to understand fully the bribery and corruption risks they are exposed to, and consequently fall short of their regulatory obligations.

### **3.2.2 Creating a risk assessment**

- 41 We found that all firms had identified a range of bribery and corruption risks. However, firms followed different approaches to identifying and assessing risk. Eight firms broadly adopted a 'collaborative' approach to creating their risk assessment, either by consulting staff from across the business or by using consultants or lawyers to help them identify their bribery and corruption risk. Where firms consulted staff from across the business, they generally carried out interviews in a sample of business units, circulated questionnaires about bribery and corruption risks to business unit heads or overseas offices, or relied on a combination of interviews and questionnaires.
- 42 Firms adopting a 'collaborative' approach should consider the potential conflicts of interest which might lead business units to downplay the level of bribery and corruption risk to which they are exposed.

*A senior individual at one large firm who had been interviewed as part of the firm's risk assessment process told us there was no bribery and corruption risk in his business unit. However, he then described what we considered higher risk business practices, including frequent interaction with public officials in higher risk countries, gifts to public officials to foster good relations, and his ability to influence the recruitment process in the firm.*



- 43 Seven firms did not consult staff or experts as part of their risk assessment. Of these, some relied instead on generic, publicly available information, including the MOJ Guidance. Others had created, or were in the process of creating, a risk assessment without input from either the business or other external sources or information.

*One large firm had created a very detailed risk assessment, using data from Transparency International and a commercially available intelligence database. However, the firm had not drawn on internal knowledge to tailor the assessment to its business. As a result, the risk assessment did not identify the specific risks to which the firm was exposed.*

- 44 We saw some merit in the adoption of a ‘collaborative’ approach in some cases, in particular where this involved internal sources. In general, this was conducive to raising awareness of anti-bribery and corruption among staff and often led to more tailored, and therefore useful, risk assessments. However, we were not always convinced that firms had satisfied themselves that staff they had selected to complete questionnaires or participate in interviews were sufficiently aware of, or sensitised to, bribery and corruption issues.

*One firm said that, where heads of business units had been asked to complete a questionnaire, in some cases business unit heads had sought assistance from their staff or from compliance, in order to provide more informed responses.*

- 45 It was also often unclear why firms had selected certain staff to consult. We also found that some firms had selected business units based on either a subjective perception of corruption risk or preference, rather than an informed decision based on objective criteria.

*Three large firms had not completed a full bribery and corruption risk assessment. Furthermore, two of them had determined that bribery and corruption was high risk for their business but had not identified where or what the highest risks were.*

- 46 Where firms used external sources, we were not always clear why a provider had been selected, in particular where it was not obvious that the chosen provider had sufficient anti-bribery and corruption expertise to add value to the firm’s own efforts. Where firms created a risk assessment based on generic, external guidance alone, we were often not convinced that this was enough to capture and assess the risks the firm was exposed to: a good risk assessment draws on the best information available from internal and external sources.

*One small firm had not completed a formal risk assessment, believing it to be unnecessary due to the firm's small size. Instead, the firm stated that its senior management had discussed and identified bribery and corruption risks across the business and also countries that were considered to be corrupt or involved in tax evasion.*

### **3.2.3 Updating the risk assessment**

- 47 As a key management tool, the ABC risk assessment must be regularly reviewed and, where appropriate, updated as external and internal bribery and corruption risks change.
- 48 Of the eight firms that had adopted a more 'collaborative' approach to creating their risk assessment by involving staff from across the business, four had not considered when or how it would be revised. Of these four firms, it was also unclear whether three of them, who had used questionnaires or interviews to create their risk assessments would repeat the exercise, at least in part due to resource constraints.

*One large firm had established an annual global review of bribery and corruption risk, supplemented by an independent review of the risk assessment by the firm's internal audit function.*

- 49 Those firms that had established a process to update their risk assessments had adopted a number of different approaches, broadly based on trigger events or periodic reviews. Trigger events included the approval of new products or new business; new bribery and corruption typologies by relevant national or international bodies such as industry working groups; and legal or regulatory developments. Different approaches to conducting regular reviews included undertaking twice-yearly reviews to assess the appropriateness of the risk assessment; involving risk committees to determine what the emerging ABC risks were; involving internal audit to review the ABC risk assessment; and engaging with previously-interviewed business heads to reassess or reaffirm ABC risk.

*Some firms referred to committees that were responsible for approving new business or but it was not always clear to what extent the committees would consider bribery and corruption risk.*

### **3.2.4 Apportionment of responsibilities**

- 50 We expect responsibility for carrying out a risk assessment and keeping it up to date to be clearly apportioned to an individual or a group of individuals with sufficient levels of expertise and seniority. We found that most firms had assigned

responsibility to the compliance function or a senior manager, a new business approval committee or, in some cases, the board.

*One large firm had not assigned specific responsibility for oversight of risk assessment to an individual or group of individuals; rather, it was left to individuals responsible for conducting due diligence, although where risks were identified, these would be referred to compliance. We were concerned that, while the level of risk involved in specific business transactions was assessed, the firm had an incomplete view of the extent of its bribery and corruption risk.*

### 3.2.5 Risk assessment – examples of good and poor practice

#### ***Good practice***

- Responsibility for carrying out a risk assessment and keeping it up to date is clearly apportioned to an individual or a group of individuals with sufficient levels of expertise and seniority.
- The firm takes adequate steps to identify the bribery and corruption risk, for example by using a range of expertise from both within and outside the business.
- Risk assessment is a continuous process based on qualitative and relevant information available from internal and external sources.
- Firms consider the potential conflicts of interest which might lead business units to downplay the level of bribery and corruption risk to which they are exposed.
- The risk assessment informs the development of monitoring programmes, policies and procedures, training,, and operational processes.
- The risk assessment demonstrates awareness and understanding of the firm's legal and regulatory obligations.
- The firm assesses where risks are greater and concentrates its resources accordingly.
- The firm considers financial crime risk when designing new products and services.

#### ***Poor practice***

- The risk assessment is a one-off exercise.
- Efforts to understand the risk assessment are piecemeal and lack coordination.
- Risk assessments are incomplete and too generic.

- Firms do not satisfy themselves that staff involved in risk assessment are sufficiently aware of, or sensitised to, bribery and corruption issues.

### 3.3 Policies and procedures

- 51 Firms must take adequate steps to prevent their bribery and corruption risks crystallising. So it is essential that firms have in place robust and effective ABC policies and procedures that are appropriate to their business, sufficient to counter bribery and corruption risk, implemented effectively, and clearly communicated to staff. Firms must regularly review and update policies and procedures, including when new risks are identified or when there are changes in relevant legislation or regulation.
- 52 ABC policies and procedures will vary depending on a firm's exposure to bribery and corruption risk. But in most cases, firms should have policies and procedures which cover expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms and disciplinary sanctions for breaches. These policies need not be in a single 'ABC policy' document and may be contained in separate policies.
- 53 During our review, we assessed whether firms had in place a policy, or policies, dealing specifically with bribery and corruption issues (including, where applicable, a code of conduct or a code of ethics); the process used to implement these policies; whether policies had been applied effectively; and the level of oversight and review of policies and procedures (including management of breaches).

#### 3.3.1 Reviews of existing ABC policies and procedures

- 54 Of the 15 firms we visited, 12 had used the implementation of the Bribery Act as an opportunity to review, or put in place, for the first time, their ABC policies and procedures. The introduction of an entirely new ABC policy was more common in smaller firms, while others had reviewed existing policies and procedures. Only two firms had no ABC policy in place at the time of our visit. In both cases, work was underway to introduce a policy by summer 2012.

*Each of the large firms in our sample had a global presence and used, or was developing, a globally consistent approach to their ABC policies, procedures and controls. Five firms had previously used an existing ABC framework to comply with the US Foreign Corrupt Practices Act ('FCPA') and adapted it to include additional controls to comply with the Bribery Act.*

- 55 Most firms that did not have an ABC policy in place before the Bribery Act told us that existing anti-money laundering systems and controls, together with the staff Code of Conduct, adequately covered their obligations in this area at the

time. However, very few firms were able to demonstrate that they had actively considered our requirements, or bribery and corruption in general, before the introduction of the Bribery Act. Firms should consider relevant FSA rules and publications when reviewing and amending their ABC policies and procedures, in order to avoid gaps in their systems and controls.

*One small firm told us that, prior to the Bribery Act, there were areas within existing policies and procedures that related to bribery and corruption, such as the gifts and expenses register and certain paragraphs in the code of conduct. The firm's response to the Bribery Act brought the relevant areas together.*

- 56 About half the firms in our sample had used the services of compliance consultants or legal firms when producing new or updated ABC policies. Other firms had drawn on external reports and publications when drafting their policies. These included our thematic report ‘*Anti-bribery and corruption in commercial insurance broking*’; the MOJ Guidance; and the FSA’s Final Notices issued in respect of Enforcement action against Willis Ltd and Aon Ltd. As with risk assessment, we expect firms to consider an appropriate range of relevant material when formulating or reviewing their ABC policies.

*One large firm had conducted a gap analysis between the FCPA and the Bribery Act. They had met a number of large law firms to elicit their views on the ABC risks inherent in dealing with non-public office holders; gifts and hospitality; facilitation payments; and jurisdictional issues.*

- 57 Thirteen firms in our sample had decided to introduce a global or firm-wide ABC policy. Most of their new policies now used the Bribery Act requirements as the minimum global standard required. This was because the Bribery Act’s provisions are wider ranging than the FCPA’s. These firms had also enhanced associated policies such as: gifts, hospitality and expenses; engaging with third parties (introducers, distributors and suppliers); and the amendment of wording in the employee code of conduct. More detailed information on these policy enhancements can be found in sections 3.4 and 3.6.

*One large firm explained that it had adopted a global approach to ensure consistency in the many countries in which it operated. This was particularly necessary, they said, for their gifts and hospitality policy. Prior to the Bribery Act, there had been a large number of different regional policies, now replaced with one global policy with set approval thresholds.*

### **3.3.2 Code of conduct**

- 58 Codes of conduct set out the standards of behaviour expected of staff and often cover issues relevant to ABC, such as conflicts of interest, gifts and corporate

hospitality, and a zero tolerance approach to bribery and corruption. There is no requirement on firms to have a code of conduct; but a code can help to add visibility and emphasis to issues the firm deems important.

*A large firm had a separate anti-corruption policy and code of conduct in place for its suppliers.*

- 59 Six firms had had recently reviewed and amended their codes of conduct to reflect the Bribery Act.
- 60 However, two firms in our sample admitted that their code of conduct had been in place for a number of years and did not adequately take account of ABC issues, while the senior management in one small firm did not know whether the firm had a code of conduct.

### **3.3.3 Monitoring and review of ABC policies and procedures**

- 61 Firms should monitor and regularly assess the adequacy and effectiveness of ABC policies and procedures to ensure they continue to comply with their regulatory obligations. Monitoring and review mechanisms should form an integral part of a firm's policies and procedures.
- 62 While we acknowledge that some firms were still finalising their ABC policies and procedures, we found that most firms had yet to devise mechanisms for reviewing or monitoring their ABC policies and procedures or their effectiveness. Where firms had considered this, they planned to conduct monitoring and testing in a variety of ways, including:
- regularly reviewing ABC policies and procedures in light of updated bribery and corruption risk assessments;
  - monitoring controls over payments to third parties, hospitality and expenses to detect breaches of policy (however, this was largely work in progress and had not yet led to any enhancements to policies and procedures);
  - gathering and analysing feedback from business units about the implementation of policies and procedures, breaches, practical difficulties or gaps encountered;
  - analysing complaints and whistleblowing reports to assess compliance with ABC policies and procedures and identify areas where policies might need to be strengthened;
  - analysing staff queries to identify where ABC policies and procedures lacked clarity; and
  - conducting testing, including internal audit reviews, to assess how well processes are being followed.



*At a large firm, monitoring compliance with the ABC policy appeared to be weak and there was no systematic effort to capture ABC related issues and questions raised by staff, as queries were logged but not analysed.*

*At a small firm, the risk of bribes being paid was monitored via the checking of expenses claims, which were all allocated to clients and projects. Any concerns in this area would be brought to the attention of compliance by the employee's line manager. Any breach of the ABC policy would be taken to HR and reported to senior management.*

### **Internal audit**

- 63 Internal audit is a key means of monitoring procedural effectiveness. We found that, among firms who had longer-standing, well-established ABC policies and procedures, only two had been the subject of ABC focused audits in the last two years. However, around half the firms visited stated that assessment of ABC policies and procedures would be included in internal audit reviews in the future.

*Issues identified in the audits that had been conducted related to insufficient staffing levels to ensure compliance with ABC standards and breaches of pre-approvals processes for expenses.*

- 64 Three large firms had planned internal audit reviews of ABC systems and controls for early 2012, although there were different approaches to this work. Two firms planned to review the implementation of processes and procedures for ABC across all business lines – this type of internal audit review is often referred to as a ‘thematic’ internal audit. The remaining firm intended to assess ABC policies and procedures when reviewing individual departments, focusing on the six principles of the Bribery Act.<sup>6</sup> The latter approach seemed to be favoured among other firms we visited as thematic ABC audits were regarded as too costly. Consequently, ABC elements would be included in wider audit coverage.

#### **3.3.4 Responsibility for policy and dealing with breaches**

- 65 In all firms visited, responsibility for the ABC policy had been allocated to a senior member of staff or compliance team, or to a dedicated ABC committee or team.

*In one small firm, compliance was responsible for ensuring policies and procedures were kept up to date with legal and regulatory responsibilities via a process of regular review.*

- 66 In larger firms, policy implementation and monitoring had sometimes been delegated to regional compliance teams or staff working within the business, overseen by local management. In these situations, the staff these functions are

---

<sup>6</sup> Proportionate procedures, top-level commitment, risk assessment, due diligence, communication and training, monitoring and review.

delegated to should have adequate expertise on ABC and there should be an effective mechanism for reporting issues to the ABC committee or compliance.

*In one large firm, the Group Bribery Committee oversaw the implementation of ABC policies and procedures and enhancements. Business units were required to review the high level policy taking into account the particular risks they faced in order to identify what controls were required. Following this, compliance officers within each business unit were responsible for devising suitable monitoring programmes. Progress regarding the development and implementation of policies was reported to the Group Bribery Committee. Below that committee, each region had its own bribery committee, as did each global business unit.*

- 67 With one exception, firms' ABC policies included an escalation procedure for reporting breaches to senior management. However, we were surprised that there appeared to be no instances of major breaches of ABC policy (such as a bribe being paid to a third party) reported by any of the firms that we visited, even in firms with well-established ABC policies and procedures.

*At one small firm, there had been no breaches of the bribery and corruption policy identified to date. There was also no defined process for dealing with any breach. The firm believed that any breach would be identified through approval controls over payments exceeding a certain threshold which was set at a low level.*

- 68 Minor breaches of policy (such as mistakes on expense forms) were usually dealt with on a case-by-case basis and staff could then be required to undertake enhanced training.

*At another small firm, breaches of policy were considered as part of the annual performance review. Cutting corners in relation to the firm's ABC policy would be regarded as a serious issue.*

### **3.3.5 Policies and procedures – examples of good and poor practice**

#### ***Good practice***

- The firm clearly sets out the behaviour expected of those acting on its behalf.
- Firms have conducted a gap analysis of existing ABC procedures against applicable legislation, regulations and guidance and made necessary enhancements.
- The firm has a defined process in place for dealing with breaches of policy.
- The financial crime/compliance team engage with the business units about the development and implementation of ABC systems and controls.



- ABC policies and procedures will vary depending on a firm's exposure to bribery and corruption risk. But in most cases, firms should have policies and procedures which cover expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms and disciplinary sanctions for breaches. These policies need not be in a single 'ABC policy' document and may be contained in separate policies.
- There should be an effective mechanism for reporting issues to the ABC committee or compliance.

#### **Poor practice**

- The firm has no method in place to monitor and assess staff compliance with ABC policies and procedures.
- Staff responsible for the implementation and monitoring of ABC policies and procedures have inadequate expertise on ABC.

### **3.4 Third-party relationships and due diligence**

69 The Bribery Act defines an 'associated person' very broadly, as a person who performs services for, or on behalf of, an organisation. This broad definition may therefore cover a variety of service providers, such as consultants, introducers, agents, intermediaries of any kind, lawyers and contractors. A firm may be considered responsible for corrupt payments made to, or by, an associated person retained by that firm, whether or not it knew that the associated person intended to pay, offer or accept a bribe.

70 In addition to these legal obligations, we expect regulated firms to have in place policies and procedures to assess the risk that third parties acting on their behalf engage in corruption and to take adequate, risk sensitive, measures to mitigate that risk. Consequently, for both legal and regulatory reasons, it is essential that appropriate due diligence is undertaken, and full records kept, on any associated person with whom the firm has dealings.

#### **3.4.1 Categorisation and business use of third parties**

71 We expect firms' ABC policies and procedures to define clearly what constitutes a 'third party' to identify the level of risk the firm is exposed to. We also expect firms to set out specific criteria for selecting third parties that include a clear commercial rationale for using the services of a third party.

72 In practice, we found that several large firms formally categorised their existing third-party relationships into various broad groups, laid down in their policies and procedures or related manuals and guidance.

*One major firm split its third-party relationships into three categories: vendors (including suppliers of goods, materials, software, operations processing, etc); sources (eg entities such as lawyers and accountants from whom the firm sourced work); and introducers/consultants (parties actively engaged by the firm to gain work for the firm or assist it with projects). Where it was not entirely clear whether a particular entity qualified as a third party, a specialist unit within the firm was responsible for making a decision.*

- 73 For two major firms, however, appropriate categorisation of third parties was much less of an issue, because they engaged only a few third-party consultants.

*In one case, a number of the consultants were former employees of the firm who had left to pursue their own ventures. The relationships were advisory only, did not involve business introductions and existed mainly in countries where the firm already had a presence.*

*Similarly, in the other case, the firm had no real need to use traditional third parties, such as business finders and introducers, as it already had wide geographical reach. Nevertheless, the firm did have a number of senior advisers on its books, who were hired to give specialist advice in areas such as tax liability.*

- 74 Smaller firms typically made no, or little, use of third parties to introduce business. These firms sourced most of their business both from recommendations or referrals from clients and from service providers such as lawyers, accountants or other UK regulated firms. Smaller firms were not in the habit of paying for introductions, partly because they competed for new business with other firms and also because, in at least one case, they referred work to lawyers and accountants. Smaller firms sometimes employed senior advisers on an ad hoc basis, for example to help complete a deal.

### **3.4.2 Establishing a definitive list of third parties**

- 75 We found that the advent of the Bribery Act had prompted several large firms to review their categorisation of third parties and establish a definitive list of third parties who could be deemed ‘associated persons’ under the Bribery Act:
- One large firm, which had previously had a relatively small list of third-party relationships, found their list had expanded as a result of the firm amending its definition of third parties beyond those dealing with government officials. However, this firm had also pruned its list in order to omit certain senior advisers and consultants who had no involvement in providing business leads. It also maintained an ‘exempt entities’ list, comprising the many law firms, accountants, and banks and other authorised firms with which it regularly

transacted business. A number of third parties on the list were awaiting a full review by compliance of their status.

- Another large firm was actively engaged in a major exercise to compile a definitive list of its ‘consultants’ world-wide. The aim of the exercise, due for completion by end-2011, was for all individual lines of business to flush out their consultant agreements and place them in a new single central repository. Responses received from across the group had soon shown that the number of consultants was greater than expected and prompted intra-group discussions about who should be considered a consultant. The exercise was co-ordinated by a working group of the firm’s senior level anti-corruption committee, which ensured a consistent approach. While the process was not yet complete, it had already produced some useful results: some business units had decided they no longer needed certain consultants’ services; others had incorrectly included certain names; and some consultants identified gave advice to the bank but were not actively soliciting business on the bank’s behalf.
- A third major firm, with only a small number of introducers and consultants, sourced work from many thousands of entities, some of whom could well be high risk third parties. This firm recognised that it needed to conduct an exercise to identify active third-party relationships. However, the work – which was to be outsourced – had not yet started and had no estimated date for completion. Following our visit, the firm started this work.

76 No smaller firms had found it necessary to compile a definitive list of third parties, given their limited, ad hoc use of them.

### **3.4.3 Risk-sensitive approach to due diligence**

77 We expect firms to determine the extent of appropriate due diligence on third parties on a risk-sensitive basis. They should seek to identify possible bribery and corruption issues as part of their due diligence work, taking account of risk factors such as negative press allegations against the third party or any known (or discoverable) political connections. This is particularly important where third parties are used to generate new business.

78 Where higher risk relationships are concerned, we expect firms to undertake enhanced due diligence measures. This should include an appropriate degree of compliance and senior management oversight and sign-off.

### **3.4.4 Risk factors and red flags**

79 We found that firms cited a number of risk factors and ‘red flags’ that they would consider in deciding whether to take on a new consultant or similar third-party relationship.

80 These included: activity type; location of activity; industry sector; and any connections with government officials. Other relevant considerations were: the

third party's own operating history; any adverse judicial or regulatory findings; media searches that revealed evidence or allegations of fraud, bribery, sanctions breaches or similar illegalities; the business rationale for hiring the third party; and where, when, how and how much the firm was paying the third party. Some of these factors could combine to prevent the hiring, for example if the work was being undertaken in a high-risk jurisdiction for payment to an offshore account elsewhere.

### 3.4.5 Approving third parties

- 81 We found that all but three firms in our sample had clear and documented procedures for taking on new third-party relationships.
- 82 The approval process generally began with the front office initiating a written, standardised proposal covering specified areas of pre-hire or pre-transaction due diligence. The extent of the due diligence varied according to the assessed risk of hiring the third party. The initiator was usually responsible for gathering basic identity and verification information, whereas compliance often searched various commercially-available intelligence databases and the 'open source' internet for adverse information on the third party. Where these searches indicated the need for enhanced due diligence, several firms commissioned specialist intelligence reports for a better informed view of, for example, whether negative press reports were likely to be politically motivated or whether the consultant's corporate structure showed connections to high levels of government.

*Most firms were very focused on the reputational risk of doing business with suspect third parties and on establishing a solid business case for engaging the services of a third party. But a number of firms went a step further, by reviewing the third party's own anti-bribery and corruption controls and, in one case, requiring the consultant to participate in relevant pre-hire and post-hire training.*

- 83 We were, however, concerned to find that in three large firms there was no prescribed third party take-on process. Two of the firms justified the lack of settled process by referring to the need to retain flexibility where, for example, needs could vary according to the transaction. In the other case, the firm intended to introduce a standard take-on approach by the end of 2011.

*One major firm used a bespoke automated system for third-party due diligence. The system asked a series of detailed questions of the employee wishing to employ a third party, on the basis of which the proposed relationship received a scored risk rating. That risk rating determined the level of due diligence required. The system's functionality ensured not only that appropriate sign-offs were obtained from compliance and the relevant anti-corruption committee but also that contracts, with signatures, were uploaded onto the system. Compliance was able to use the system to produce a range of regular management information.*

- 84 In general, we were pleased to find an appropriate level of senior management involvement in decision making about new third-party relationships or transactions. In high-risk situations, in addition to sign-off from a business head, new engagements generally required the approval of a 'New Business Committee' (or similar body) of senior executive management. That committee would consider not only the potential reputational risk and business rationale but also whether the third party would provide a valuable service on commercial terms and not merely 'open a door'. Some firms emphasised that, if there were any doubts, the engagement or transaction would not proceed. They also made clear that committee approval was in no sense a 'rubber stamp' on proposals put forward.

#### ***Contractual arrangements***

- 85 Four large firms had certain specific ABC requirements (so-called 'reps and warranties') routinely incorporated into contracts with consultants and other third parties.

*Two firms had similar contractual protections in place, including explicit reference to compliance with the FCPA and, in one case, a right of termination in relation to corruption related issues. Another told us it was considering whether to include ABC-specific clauses into third-party agreements.*

### **3.4.6 Monitoring and review of third-party relationships**

- 86 We consider it essential that firms regularly monitor and review their third-party relationships using a risk-based approach. This is necessary, both to check whether there is a solid business case for the relationship to continue and to ensure that changes to the nature and risk profile of the relationship are appropriately identified and signed off. We expect the frequency and depth of the reviews to match the assessed risk rating of the third-party relationship.
- 87 We were disappointed to discover only limited evidence of ongoing monitoring and review of third-party relationships by firms in our sample, though there were different reasons for this.

- 88 Two large firms had in place a regular monitoring and review cycle, determined by the risk rating of the relationship. The reviews would typically look at business activity and any other factor, such as adverse information received on the third party, which might require compliance or a senior management committee to decide whether the relationship should be allowed to continue.

*At the opposite extreme, another large firm had conducted no reviews of its third-party relationships. Compliance expected individual business units to make them aware of any negative news or of the expected work not being produced by the third party, rather than taking any proactive role themselves. However, it was unclear whether all business units knew what was expected of them.*

- 89 Two other large firms were in the throes of remediating and recertifying their third-party relationships, both to establish a definitive list of these relationships and to decide which were worth retaining.
- 90 Among smaller firms, we found that due diligence carried out on third parties was often deal-specific, so monitoring and review of relationships was not an issue. And in one case, because the firm considered its business low risk for bribery and corruption purposes, the firm did not consider it necessary to conduct regular reviews.

### **3.4.7 Our testing of the quality of due diligence**

- 91 Wherever possible, we reviewed firms' records of due diligence carried out on third-party relationships. This revealed that, although there were clear due diligence procedures in place at most firms, the relevant procedures were often not followed rigorously.

*One large firm's files showed that, as part of the recently revised on-boarding process, consultants were routinely interviewed by compliance and also received anti-corruption training from the firm.*

- 92 Two firms demonstrated clear and comprehensively documented due diligence on their third-party relationships. In contrast, however, we noted some common failings at many firms, including:
- an apparent lack of compliance involvement in the approval of potentially high risk introducer/consultant relationships;
  - no evidence of routine checks to ensure that introducers and consultants were not PEPs;
  - failure to document properly the business rationale for the relationship;



- no evidence of risk assessment of the third party and no specific reference or consideration of the risk of bribery and corruption; and
- the inclusion of due diligence documentation that had not been translated into English, with no evidence that the material had been considered by someone who understood the language used.

### **3.4.8 Third-party due diligence – examples of good and poor practice**

#### ***Good practice***

- Where third parties are used to generate business, these relationships are subject to thorough due diligence and management oversight.
- Third-party relationships are reviewed regularly, and in sufficient detail, to confirm that they are still necessary and appropriate to continue.
- There are higher, or extra, levels of due diligence and approval for high risk third-party relationships.
- There is appropriate scrutiny of, and approval for, relationships with third parties that introduce business to the firm.
- The firm's compliance function has oversight of all third-party relationships and monitors this list to identify risk indicators, eg a third party's political or public service connections.
- Evidence that a risk-based approach has been adopted to identify higher risk relationships in order to apply enhanced due diligence.
- Enhanced due diligence procedures include a review of the third party's own ABC controls.
- Consideration, where appropriate, of compliance involvement in interviewing consultants and the provision of anti-corruption training to consultants.
- Inclusion of ABC-specific clauses and appropriate protections in contracts with third parties.

#### ***Poor practice***

- A firm using intermediaries fails to satisfy itself that those businesses have adequate controls to detect and prevent staff using bribery to generate business.
- The firm fails to establish and record an adequate commercial rationale for using the services of third parties.
- The firm is unable to produce a list of approved third parties, associated due diligence and details of payments made to them.
- There is no checking of compliance's operational role in approving new third-party relationships and accounts.

- A firm assumes that long-standing third-party relationships present no bribery or corruption risk.
- A firm relies exclusively on informal means, such as staff's personal knowledge, to assess the bribery and corruption risk associated with third parties.
- No prescribed take-on process for new third-party relationships.
- A firm does not keep full records of due diligence on third parties and cannot evidence that it has considered the bribery and corruption risk associated with a third-party relationship.
- The firm cannot provide evidence of appropriate checks to identify whether introducers and consultants are PEPs.
- Failure to demonstrate that due diligence information in another language has been understood by the firm.

### 3.5 Payment controls

93 In addition to effective third-party due diligence, firms should have effective systems and controls in place to ensure payments to third parties are in line with what is both expected and approved. So we considered how effective the firms' payment controls were.

94 Firms adopted different approaches to preventing unauthorised payments to third parties including requiring a business rationale and associated due diligence before any third-party payment was made; prohibiting cash payments to third parties; requiring a valid invoice before payment was authorised; requiring proposed transactions to be reviewed/approved by staff or committees independent of the business before payments were made; and escalating significant payments – or linked payments – for appropriate approval.

*A relationship manager at one large firm had established a third-party relationship without seeking the usual approval. When an invoice was submitted by the third party, the firm's accounts staff could not process the payment because there was no payment code on their accounting system.*

95 Firms undertook varying levels of payments monitoring ranging from six monthly retrospective reviews to identify trends to daily reconciliations between general ledgers and released payments. One firm said that it had reviewed and analysed all third-party payments as a result of our visit.

*A small firm told us that a payment was rejected because a third party had requested a payment to be transferred to an alternative bank account than that which was recorded against the third party's due diligence.*



### 3.5.1 Payment controls – examples of good and poor practice

#### *Good practice*

- Ensuring adequate due diligence on and approval of third-party relationships before payments are made to the third party.
- Risk-based approval procedures for payments and a clear understanding of the reason for all payments.
- Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.
- Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.
- A healthily sceptical approach to approving third-party payments.
- Adequate due diligence on new suppliers being added to the Accounts Payable system.
- Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.
- Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable hospitality.
- Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved.
- The facility to produce accurate MI to assist effective payment monitoring.

#### *Poor practice*

- Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.
- Failing to produce regular third-party payment schedules for review.
- Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.
- No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.

## 3.6 Gifts and hospitality

- 96 The exchange or offering of gifts and hospitality (G&H) can serve a legitimate business purpose, such as cementing good relations with business partners. However, G&H can also be used, or appear to be used, as bribes. A firm's

G&H policy should therefore be proportionate, unambiguous and effectively implemented.

- 97 Firms should seek to prevent the giving or receipt of gifts, hospitality or paying of expenses if it might influence, or be perceived to influence, a business decision. They should also ensure that their staff and other relevant stakeholders are made aware of, and understand, their policies on gifts and hospitality.

*At one firm, a TV was given as a present to an employee. However, the employee was not allowed to keep it and the TV was installed in the back office for general use by all staff.*

- 98 In general, we found that the Bribery Act had caused many firms to consider their existing G&H framework and enhance their policies and procedures. All firms had a single G&H policy, applicable across the organisation, which set out limits and the approval process. However some firms had more comprehensive policies on G&H than others. Examples observed in our review included:

- prohibiting cash, or cash equivalent, gifts;
- not issuing corporate credit cards and allowing expenses to be incurred and reclaimed only on personal cards – leaving employees at risk of unreasonable expenses not being reimbursed;
- prohibiting invitations to certain clients, such as public officials, to ‘premier events’ (eg Grand Prix, the football World Cup and Wimbledon finals); and
- prohibiting the flying of clients to major sporting events.

- 99 We found that some senior managers saw a benefit in developing G&H policies in conjunction with the business, to ensure that those policies were relevant to the firm’s business and supported by employees. However, firms should be alive to the potential conflicts of interest here.

### **3.6.1 Risk assessment**

- 100 Two firms had identified their highest bribery and corruption risk as corporate hospitality and most other firms considered it to be a main area of risk. In contrast, another firm saw no real concern as it ran no ‘big ticket’ events and gave no high-value gifts. All firms viewed G&H for public officials as high risk and imposed greater restrictions.

*At one firm, gifts to public officials were subject to due diligence checks against PEP, sanctions and country risk databases before approval was granted, in order to avoid any impression of bribery.*

### 3.6.2 Culture and senior management oversight

- 101 Management should foster a culture that promotes an ethical environment and requires employees to adhere to high standards of integrity. Appropriate standards should be set for giving and receiving hospitality, with senior management leading by example in adhering to those standards.

*One firm's CEO, in order to avoid any perception of impropriety, decided to distribute amongst staff the contents of an expensive hamper he had been given.*

- 102 Several firms spoke of a cultural change in the investment banking sector from bygone days of lavish hospitality. We also found that several firms had reduced their hospitality budget, mainly due to economic conditions and what they perceived to be a negative public perception of excess in banking. Client hospitality was much reduced and therefore excessive hospitality had become less of a problem for firms to tackle.

*One firm mentioned that most of its client hospitality involved fund managers. However, fund managers now had their own strict ABC policies in place, which prevented them, for example, from lunching with the same broker twice in one year.*

- 103 In general, we found that where firms had incurred significant expenditure, they were able to demonstrate an appropriate business case. However, we found some cases where hospitality received appeared inappropriate.

*At one firm, a three-day trip to the football World Cup in South Africa costing £10,000 for one employee and his wife was approved by a member of staff who was not listed as an approver in the firm's policy. Upon investigation, we discovered that the expense was signed off by an 'acting manager' in the absence of the designated manager. Subsequently, the firm decided to amend its policy to include names of individuals who could approve expense claims in the absence of the designated manager.*

#### **'Cultural necessity' and the law**

- 104 Some firms described difficulties when conducting business in some parts of the world where there was symbolic value in the exchange of gifts.

*At one firm, Eid festival gifts worth up to \$400 each were given to 29 sovereign wealth fund heads. The payments, which were channelled through compliance, were described as 'a cultural thing'.*

- 105 In such cases, we consider that firms should have appropriate policies in place to balance their desire to maintain good relations with clients with the mitigation

of the bribery and corruption risk inherent in business conducted with certain overseas jurisdictions. There is no exclusion in the Bribery Act covering what is 'expected' in other cultures.

### 3.6.3 Limits

- 106 We expect firms to define limits which are appropriate to the firm's business and proportionate to the bribery and corruption risk associated with certain clients or business relationships. While it is reasonable to allow staff to give or receive G&H of low value without pre-approval, firms should set a reasonable level at which G&H should be declared.
- 107 We were therefore encouraged to find that all firms' policies specified limits at which pre-approval was required. Limits were usually specified by type of hospitality and type of client and ranged from £100 to £400 for individual hospitality and, for corporate or sponsorship events, around £4,000 for smaller firms to £15,000 for larger firms.

### 3.6.4 Approvals

- 108 To control the risk of staff giving or receiving inappropriate G&H, it is important that G&H are approved by persons of sufficient seniority, using a risk-based approach. We expect to see an audit trail for the approval of expenses, together with an appropriate rationale for the hospitality.
- 109 We found different approaches to the approval of gifts. Some firms maintained lists of approvers in their G&H policies, whereas other firms did not specify approvers in their policies at all.

### 3.6.5 Monitoring

- 110 Robust G&H monitoring processes are essential for firms to ensure they are able to identify potentially corrupt behaviour by employees and/or clients. A good process should enable firms to categorise and assess expenses appropriately, for example by employee, client, project, type of hospitality and cost. So we were disappointed to find that seven firms were only now developing processes in this area.

*At one firm, we were told G&H was reviewed on a 'best efforts' basis by the compliance team. Compliance did not look at every pre-approval and served as a point of escalation for issues that could not be resolved at business level.*

*At another firm, monitoring of G&H given and received was ad hoc, and the firm could not produce or, therefore, evaluate important information, such as the concentration of gifts given to individuals or organisations.*

*A third firm's compliance team undertook no analysis of its own gifts register or of the sponsorship and events register.*

111 Monitoring of G&H is not only necessary to ensure that staff are complying with the firm's policy but may also provide useful MI for the business more generally. (The use of MI is covered in greater depth in Section 3.1.1.) Examples of how some firms were using, or intended to use, G&H monitoring processes to bolster MI included:

- Developing a system to record all interactions the business had with each client. This would enable the firm to assess the concentration of gifts for each client and whether the hospitality provided was appropriate, as well as to analyse client activity, produce regular MI and decide whether resources should be targeted differently towards certain relationships.
- Using a database as a central repository for different types of anti-corruption related data, including G&H and contributions to charity (see section 3.6.6 for more on charitable donations). An enhancement was being made to this system to enable more efficient tracking of G&H, especially if requested for more than five people.
- Using a system enabling them to filter expenses according to employee, client and type of hospitality. The relevant MI was circulated to the chief executive officer (CEO) and chief operating officer (COO) monthly, allowing them to query certain expenses. The MI highlighted the top ten employees and top ten clients on which the hospitality budget was being spent. This enabled senior management to have clear and detailed oversight of expenses incurred by the firm.

***Ensuring the accuracy and completeness of G&H registers***

112 Requiring employees to declare G&H ensures that firms are dealing with business relationships in an open and transparent way, thereby reducing the risk of bribery and corruption. So it is important that firms accurately record G&H given or received, as this can form the basis for useful MI to assess, monitor and mitigate bribery and corruption risks (see paragraph 111 above).

*Typically, most firms' G&H registers recorded: employee name; gift value; date; gift description; the giver or receiver of the gift; the approver; date; and a comments box to provide additional information on the reason for the gift.*

113 Most firms maintained firm-wide logs of gifts given and received. However, it was clear from our review that there were issues in relation to the completeness of G&H registers. One firm believed that not all G&H given or received was being recorded by staff, resulting in a shorter than expected gift log. This firm, and some others, said the verification and reconciliation exercises they did to prepare for our visits had prompted them to consider what further work might be necessary. Other examples of issues with G&H logs included:

- a G&H register at one firm which appeared short;

- a G&H register which one firm felt did not accurately report the ‘whole story’ – as a result they were unable to confirm that all gifts received or given had been recorded; and
- at one firm, information prepared before our visit showed that there were inconsistencies in its G&H register, eg two items appeared in the finance expenses system that should have been recorded in the G&H register.

*At one firm, the only control over gifts received was the requirement for staff to self-certify compliance with policy.*

114 While there are undoubtedly challenges for firms in ensuring that gifts are declared in line with their policies, they might wish to consider the following measures to reduce the risk of gifts going undeclared:

- issuing regular reminders to staff about reporting gifts received or given – one firm did this during periods when staff were more likely to receive gifts, such as Christmas;
- providing examples in training and internal communications of employees who have/have not declared G&H appropriately;
- reconciling the gift register with actual gifts given or received;
- monitoring or auditing employees’ G&H compliance on a random basis; and
- setting out, and applying, appropriate sanctions for breaches of G&H policies and procedures.

### **3.6.6 Political and charitable donations**

115 Firms should consider carefully whether and how to make political and charitable donations, as they could, in some circumstances, amount to – or give the impression of – bribery. So it is good practice for political and charitable donations to be approved at an appropriate level, with compliance input.

#### ***Charitable donations***

116 All firms in our sample had a policy on charitable donations and most believed they could pose a bribery and corruption risk to their business. It is important for firms to ensure that they are giving to legitimate charities which are not involved in financial crime or other corruption.

117 Appropriate due diligence should therefore be carried out to assess whether charities are authentic; have any connections, associations or links to political causes; operate in, or send funds to, high-risk jurisdictions; or have been the subject of negative media reports indicating financial crime or other irregularities.



*One firm was expanding its due diligence processes to include a specific section on charities. The charities would be asked to complete a questionnaire that covered: adverse information on the charity or board member; whether the charity was operating in a high risk jurisdiction; and if funds could be destined for high risk countries. The firm would carry out additional research to check if the firm had links to political causes and if there was a risk of the firm making covert political contributions.*

*Another firm had a stand-alone committee independent of the business which was responsible for approval of charitable donations. This committee analysed the soundness of donations and focused on the reputation of the charity. Firms should consider mitigating the risk of bribery through additional controls such as public disclosure of charitable contributions and sponsorships.*

- 118 Some firms had experienced practical difficulties in implementing their policies on charitable donation. For example, one firm had lifted a blanket ban on supporting charities, as this had made it awkward for the firm to sponsor individuals participating in charity events. Instead of a blanket ban, the firm reviewed charitable donations on a case-by-case basis, in order to ensure that the donations were not bribes and could not create the impression of bribery.

#### ***Political donations***

- 119 Firms should consider the risk that employees might seek to obtain an advantage in business transactions by making direct or indirect contributions to political parties, organisations or individuals involved in politics. It is good practice for firms to ensure political donations are approved at an appropriate level, with compliance input, and subject to appropriate due diligence.
- 120 We found no examples of firms making political donations, although some had policies and procedures in place for employees wishing to make political donations. Two firms required employees to receive clearance prior to making political donations, even in a personal capacity, and also if they wanted to sit on a national political party committee. At one firm, the policy extended to contributions made by spouses, minors and other family dependants.

### **3.6.7 Gifts and hospitality policy – examples of good and poor practice**

#### ***Good practice***

- Policies and procedures clearly define the approval process and the limits applicable to G&H.
- Processes for filtering G&H by employee, client and type of hospitality for analysis.

- Processes for identifying unusual or unauthorised G&H and deviations from approval limits for G&H.
- Staff are trained on G&H policies to an extent appropriate to their role, in terms of both content and frequency, and regularly reminded to disclose G&H in line with policy.
- Cash or cash-equivalent gifts are prohibited.
- Political and charitable donations are approved at an appropriate level, with compliance input, and subject to appropriate due diligence.

#### **Poor practice**

- Senior management do not set a good example to staff on G&H policies.
- Acceptable limits and the approval process are not defined.
- The G&H policy is not kept up to date.
- G&H and levels of staff compliance with related policies are not monitored.
- No steps are taken to minimise the risk of gifts going unrecorded.
- Failure to record a clear rationale for approving gifts that fall outside set thresholds.
- Failure to check whether charities being donated to are linked to political causes.

### **3.7 Staff recruitment and vetting**

121 Robust recruitment and vetting processes, which take into account bribery and corruption risks associated with individual roles, are important if firms are to reduce the risk of employing staff who may be vulnerable to engaging in corrupt practices. This means that staff in higher risk roles, including from a bribery and corruption perspective, should be subject to more thorough vetting.

122 All firms in our sample had formal processes in place to recruit and vet staff. The background checks on prospective candidates generally included previous employment checks, credit checks to assess individuals' financial soundness and basic criminal record checks.

*One small firm said that references from previous employers were unreliable and revealed nothing about the candidate's previous performance. This underlines the importance of other checks in the vetting process.*

123 In many firms, vetting was outsourced to recruitment agencies. Firms who rely on such agencies to recruit and vet staff should be able to demonstrate a good understanding and awareness of the vetting checks conducted by these agencies



as they are ultimately responsible for anything these agencies do on their behalf. Firms should also consider conducting periodic checks to ensure that agencies are complying with agreed vetting standards.

*Two firms did not appear to have a sound knowledge of the checks the vetting agency had carried out on their behalf.*

- 124 Some large firms had introduced enhanced vetting procedures for staff in higher risk positions. However, we were concerned that most firms failed to take account of the bribery and corruption risk associated with certain roles; enhanced vetting often applied only to senior roles, however defined, and FSA controlled functions without any consideration of the function's exposure to bribery and corruption. In addition, although reputational considerations were taken into account in determining whether to undertake additional checks on an individual, it was sometimes unclear whether bribery and corruption risk was specifically taken into account.

*One large firm could not identify which roles involved high bribery and corruption risks. Nor did it know which vetting checks had been undertaken for candidates recruited from abroad, as the firm seemed to place total reliance on its outsourced recruiters.*

- 125 Enhanced vetting included Criminal Records Bureau (CRB) checks, sanctions screening, and checks for adverse information in the media and on staff fraud databases (eg CIFAS). Only one large firm carried out proactive staff screening against a PEP database as part of the vetting process, but some other large firms required employees to declare any relationships or affiliations to public officials as part of their recruitment process.

*One large firm was screening the firm's thousands of employees against a PEP database as part of its ABC framework enhancement programme.*

*One firm had in the past required referred new recruits to declare whether they had been referred by a 'government official' in order to identify PEP connections. However, the firm was now looking to extend the scope of this declaration and required staff to identify anyone who might have referred them in an attempt to capture other high-profile connections.*

- 126 Some firms did not apply equivalent checks to overseas candidates. Four firms said that recruiting international staff could be challenging, mainly because of legal restrictions in several countries regarding pre-employment checks. Two firms explained that certain countries did not release credit reference information for international applicants. Another said it was confident that its overseas recruitment agencies had access to equivalent sources of information in different jurisdictions but was unable to demonstrate this.

*One large firm said that recruitment and vetting was the most complex area of its ABC implementation work, mainly because of the need to consider ABC issues in candidates' countries of origin.*

127 We were pleased to find that temporary members of staff were not subject to less rigorous vetting than permanent staff in the same or similar roles. Since the risk of bribery and corruption does not decrease when a temporary member of staff or contractor handles higher risk business, the standard of vetting should not be relaxed.

*In one firm, temporary staff and contractors were subject to stringent checks, unless the duration of the assignment was less than four weeks. The firm explained that, given the length of time taken by vetting checks, it was not practicable to carry out vetting, as these hires usually took place at short notice. However, the firm emphasised that all necessary checks would be undertaken if the assignment over-ran or was extended.*

128 We found no evidence of repeat vetting for existing employees in higher risk roles, over and above the continuous conflict of interest staff disclosure requirements. For most firms we visited, staff vetting was therefore a one-off exercise. We consider this may leave firms exposed to bribery and corruption risk, as they may not be able to identify changes in an existing employee's circumstances which might make that person more vulnerable to becoming engaged in corrupt practices. However, two large firms were already looking to close this potential loophole by introducing a formal process to re-screen existing employees.

*One firm was considering re-vetting checks for existing members of staff who returned to work after a period of absence longer than thirty days. These checks would be similar to those on recruitment.*

### **3.7.1 Staff recruitment and vetting – examples of good and poor practice**

#### ***Good practice***

- Vetting staff on a risk-based approach, taking into account financial crime risk.
- Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially-available intelligence databases – for staff in roles with higher bribery and corruption risk.
- Where employment agencies are used, the firm periodically satisfies itself that the agency is adhering to agreed vetting standards.

### **Poor practice**

- Failing to carry out repeat checks to identify changes that could affect an individual's integrity and suitability.
- No risk based processes for identifying staff who are PEPs or connected to PEPs.
- Where employment agencies are used to recruit staff, failing to demonstrate a clear understanding of the checks these agencies carry out on prospective staff.
- Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.

## **3.8 Training and awareness**

- 129 Firms must employ staff who possess the skills, knowledge and expertise to carry out their functions effectively. Firms should review their staff's competence and take appropriate action, such as targeted training and awareness-raising, to ensure they remain competent for their role. Maintaining a good standard of staff training and awareness in a firm is also essential to ensuring staff compliance with policies and procedures. In particular, effective training should not only help prevent staff committing corrupt practices but also promote ethical behaviours in firms. Staff must therefore clearly understand their own ABC obligations and their employer's overall ABC approach.
- 130 Overall, we found that firms provided adequate basic training on ABC. Most firms required all staff, irrespective of seniority and position, to take ABC training. Our visits confirmed a good understanding of bribery and corruption risk among senior managers and other relevant staff in most firms. Many firms emphasised during the visits that bribery and corruption posed a serious risk to their reputation and could be costly.
- 131 Firms took different approaches to delivering staff training. Some large firms had dedicated trainers responsible for ABC training within the compliance function. However, most firms needed to do more to develop tailored risk-based training to promote understanding and awareness among staff with greater exposure to bribery and corruption risk. That said, we found that many firms had identified the need for enhanced training modules for staff in high-risk areas and were working to introduce such training.

*One large firm had appointed a training strategy specialist to develop tailored face-to-face training for staff with greater exposure to bribery and corruption risk.*

- 132 We found that the vast majority of firms had launched ABC training in response to the Bribery Act. This indicated a reactive approach to ABC training which meant

that, before the Bribery Act, many firms had not trained their staff on bribery and corruption risk and therefore had not met their regulatory obligations.

*One large firm provided training not only to its staff but also to associated third parties, such as consultants and introducers, to ensure that they clearly understood the firm's ABC policies, procedures and expectations.*

- 133 Some firms delivered stand-alone ABC training modules, while in others ABC formed part of more general financial crime training. Most firms relied on computer-based training or a presentation from the compliance department to deliver training. In many firms, training focused equally on legal and regulatory requirements, policies and procedures, and practical, real-life examples.
- 134 We found no evidence to suggest that firms intended to treat ABC training as a one-off event. Most firms had processes in place to update the training package and provide refresher or follow-up training to reinforce initial training.
- 135 We were disappointed that most firms did not test staff's understanding of training received. Instead, staff were merely required to confirm that they had read and understood relevant policies.

*One firm, which did test staff understanding, said it would follow up with employees who had failed a number of times, in order to understand the reason for them failing the test repeatedly.*

- 136 It is important for firms to be able to assess the quality and adequacy of their training. Some firms suggested that staff feedback or quality of internal reporting and whistle blowing might be indicative of greater awareness brought about by training. We expect firms to take appropriate steps to satisfy themselves that training has achieved the desired objectives.

*A large firm said that multiple test failures were very rare domestically but not uncommon in foreign branches and subsidiaries, due to language barriers. This suggests their training for overseas staff was ineffective.*

- 137 Relevant indicators, over and above staff test results and pass rates, may include – but are not limited to – internal reporting and whistleblowing and levels of compliance with firm's policies. Relevant data should be systematically collected, reviewed and assessed in order to evaluate and improve training.

*At one firm, some staff were unclear about both ABC risks generally and specific risks in their own role. This was particularly apparent among staff working in process areas, such as payment control, events management and recruitment, who seemed more focused on following established procedures than thinking about risks.*

*One large firm believed that training effectiveness could not be measured empirically. This firm therefore placed great emphasis on raising staff awareness. Targeted awareness training had prompted intelligent questioning by staff and also resulted in two potential bribery and corruption incidents being reported.*

138 In addition to formal training, we found that four firms had devoted resources to ABC compliance campaigns and events to promote staff understanding and awareness of the firm's ABC obligations.

### **3.8.1 Training and awareness – examples of good and poor practice**

#### ***Good practice***

- Providing good quality, standard training on anti-bribery and corruption for all staff.
- Ensuring training covers relevant and practical examples.
- Keeping training material and staff knowledge up to date.
- Awareness raising initiatives, such as special campaigns and events to support routine training, are organised.

#### ***Poor practice***

- Failing to provide training on ABC that is targeted at staff with greater exposure to bribery and corruption risks.
- Failing to monitor and measure the quality and effectiveness of training.

## **3.9 Remuneration structures**

139 We expect firms to manage the risk of remuneration structures that reward staff for taking unacceptable risks, including in relation to bribery and corruption. This expectation applies to all staff.

140 In addition, the FSA Remuneration Code (the Code) sets out the standards that banks, building societies and some investment firms have to meet when setting pay and bonus awards for certain groups of employees, known as 'Code Staff'. (These are any staff members who 'have a material impact on a firm's risk profile'.) We found that large firms had detailed Remuneration Policy Statements in place in

line with the Code, whereas small firms tended to adopt a less formal approach to remuneration.

- 141 Overall, the Bribery Act had not prompted a review of staff remuneration in the firms we visited, as against the revisions large firms had had to make to comply with the Code. This was disappointing, as it meant that firms had failed to assess the corruption risk associated with individual functions – not just Code Staff. Most firms took the view that, where a breach of ABC policy occurred and did not result in staff dismissal, it would affect an individual’s annual performance review to the same extent as any other policy breach.

*One small firm explained that, if there was any hint of an employee being involved in bribery and corruption, it would be a case of how quickly that employee could be dismissed, not how much their remuneration should be reduced.*

- 142 We found that staff appraisals generally took into account both the achievement of business targets and the quality of work, with regulatory compliance and adherence to firm ethics and values also forming part of the assessment. As a result, any breach of a firm’s policies and procedures could affect the amount of an individual’s remuneration. However, three firms explicitly stated that a good standard of compliance was expected and not cause for rewarding an employee.

*A large firm said that staff failures to comply with policies impacted on compensation but was unable to demonstrate how poor behaviour was taken into account in the compensation process.*

*Another firm said ‘good compliance is an expectation, the lowest common denominator’.*

### **3.9.1 Remuneration structures – examples of good and poor practice**

#### ***Good practice***

- Remuneration takes account of good compliance behaviour, not simply the amount of business generated.
- Identifying higher risk functions from a bribery and corruption perspective and reviewing remuneration structures to ensure they do not encourage risk taking.

#### ***Poor practice***

- Failing to reflect poor staff compliance with anti-bribery and corruption policy and procedures in staff appraisal and remuneration.



## 3.10 Incident reporting

- 143 Firms should have effective processes in place to ensure that they become aware of any bribery and corruption concerns and are able to take timely action to mitigate the risk. We assessed the effectiveness of firms' complaints, reporting and whistleblowing processes.
- 144 Overall, we found no serious weaknesses in internal reporting procedures. Firms generally relied on financial crime or ABC training to educate staff on how to raise concerns about bribery and corruption.

*One firm sent regular compliance alerts to remind staff of their responsibilities for reporting any kind of suspicious activity.*

### 3.10.1 Whistleblowing

- 145 Confidential whistleblowing procedures encourage employees to raise concerns internally about misconduct or perceived misconduct in their firm without fear of negative consequences for themselves. Access to whistleblowing may therefore be a useful component of a firm's ABC control framework.
- 146 We found that large firms generally had a formal written whistleblowing procedure with hotlines sometimes run by external service providers. Small firms failed to see the benefit of a whistleblowing hotline. Rather, employees were advised to raise any concerns directly with their line manager, a more senior manager or HR.
- 147 There is an important difference between raising a concern with the business and whistleblowing. Where firms chose not to provide staff with access to whistleblowing hotlines, they should consider what else they can do to allow staff to raise concerns anonymously, with adequate levels of protection and communicate this clearly to staff.

*Should firms' staff feel they cannot blow the whistle internally, for example because senior management might be involved in misconduct, we run an anonymous whistleblowing line for staff in regulated firms. Our whistleblowing line's telephone number is 020 7066 9200 or an email can be sent to [whistle@fsa.gov.uk](mailto:whistle@fsa.gov.uk). In addition, the UK charity, 'Public Concern at Work', offers free advice to people with whistleblowing dilemmas and professional support to organisations who need advice on how to set up whistleblowing facilities.*

- 148 We found some evidence that whistleblowing procedures had been updated in response to the Bribery Act and then communicated to staff. However, several firms' procedures made no direct reference to reporting bribery and corruption suspicions.

*One firm said that its long-established whistleblowing policy had been revised, following the Bribery Act, to make bribery and corruption an explicit part of the policy.*

- 149 Where firms had whistleblowing processes, guidance for staff on whistleblowing was generally adequate. Firms relied on training to make staff aware of their policy. Firms should ensure that the whistleblowing contact number, where applicable, is visible and accessible to all staff.

*One large firm had launched an 'ethics hotline'. This was an incident reporting facility separate from the whistleblowing line. The facility was available not only to employees but also, as was clearly advertised on the firm's website, any member of the public.*

*Another firm gave employees the option to report concerns to an 'integrity officer' who worked in parallel with the whistleblowing process.*

- 150 Firms should maintain proper records of incidents and concerns reported for future reference and possible trend analysis. Information gathered can also be a useful indicator to assess the effectiveness of the firm's ABC policies and procedures – either as a confirmation that these policies and processes are effective or to detect areas of vulnerability that need to be addressed.

### **3.10.2 Incident reporting and management – examples of good and poor practice**

#### ***Good practice***

- Clear procedures for whistleblowing and the reporting of suspicions which are communicated to staff.
- Details about whistleblowing hotlines are visible and accessible to staff.
- Where whistleblowing hotlines are not provided, firms should consider measures to allow staff to raise concerns anonymously, with adequate levels of protection and communicate this clearly to staff.
- Firms use information gathered from whistleblowing and internal complaints to assess the effectiveness of their ABC policies and procedures.

#### ***Poor practice***

- Failing to maintain proper records of incidents and complaints.



## 4 Consolidated examples of good and poor practice

<b>ABC systems and controls in investment banks – examples of good and poor practice</b> <i>(Proposed new guidance is highlighted in bold italics)</i>	
Examples of good practice	Examples of poor practice
<b>Governance and MI</b>	
<ul style="list-style-type: none"> <li>• Clear, documented responsibility for anti-bribery and corruption apportioned to either a single senior manager or a committee with appropriate terms of reference and senior management membership, reporting ultimately to the Board.</li> <li>• Regular and substantive MI to the Board and other relevant senior management forums including an overview of the bribery and corruption risks faced by the business, systems and controls to mitigate those risks, information about the effectiveness of those systems and controls and legal and regulatory developments.</li> <li>• Where relevant, MI includes information about third parties including (but not limited to) new third-party accounts, their risk classification, higher risk third-party payments for the preceding period, changes to third-party bank account details and unusually high commission paid to third parties.</li> <li>• MI submitted to the Board ensures they are adequately informed of any external developments relevant to bribery and corruption.</li> <li>• Actions taken or proposed in response to issues highlighted by MI are minuted and acted on appropriately.</li> </ul>	<ul style="list-style-type: none"> <li>• <b><i>Failing to establish an effective governance framework to address bribery and corruption risk.</i></b></li> <li>• Failing to allocate responsibility for anti-bribery and corruption to a single senior manager or an appropriately formed committee.</li> <li>• Little or no MI sent to the Board about bribery and corruption issues, including legislative or regulatory developments, emerging risks and higher risk third-party relationships or payments.</li> </ul>

## ***ABC systems and controls in investment banks – examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Assessing bribery and corruption risk</b>	
<ul style="list-style-type: none"> <li>• Responsibility for carrying out a risk assessment and keeping it up to date is clearly apportioned to an individual or a group of individuals with sufficient levels of expertise and seniority.</li> <li>• <b><i>The firm takes adequate steps to identify the bribery and corruption risk, for example by using a range of expertise from both within and outside the business.</i></b></li> <li>• Risk assessment is a continuous process based on qualitative and relevant information available from internal and external sources.</li> <li>• <b><i>Firms consider the potential conflicts of interest which might lead business units to downplay the level of bribery and corruption risk to which they are exposed.</i></b></li> <li>• <b><i>The ABC risk assessment informs the development of monitoring programmes; policies and procedures; training; and operational processes.</i></b></li> <li>• <b><i>The risk assessment demonstrates an awareness and understanding of firms' legal and regulatory obligations.</i></b></li> <li>• The firm assesses where risks are greater and concentrates its resources accordingly.</li> <li>• The firm considers financial crime risk when designing new products and services.</li> </ul>	<ul style="list-style-type: none"> <li>• The risk assessment is a one-off exercise.</li> <li>• Efforts to understand the risk assessment are piecemeal and lack coordination.</li> <li>• Risk assessments are incomplete and too generic.</li> <li>• <b><i>Firms do not satisfy themselves that staff involved in risk assessment are sufficiently aware of, or sensitised to, bribery and corruption issues.</i></b></li> </ul>

## ***ABC systems and controls in investment banks – examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Policies and procedures</b>	
<ul style="list-style-type: none"> <li>• The firm clearly sets out the behaviour expected of those acting on its behalf.</li> <li>• <b><i>Firms have conducted a gap analysis of existing ABC procedures against applicable legislation, regulations and guidance and made necessary enhancements.</i></b></li> <li>• <b><i>The firm has a defined process in place for dealing with breaches of policy.</i></b></li> <li>• <b><i>The financial crime/compliance team engage with the business units about the development and implementation of ABC systems and controls.</i></b></li> <li>• <b><i>ABC policies and procedures will vary depending on a firm’s exposure to bribery and corruption risk. But in most cases, firms should have policies and procedures which cover expected standards of behaviour; escalation processes; conflicts of interest; expenses, gifts and hospitality; the use of third parties to win business; whistleblowing; monitoring and review mechanisms and disciplinary sanctions for breaches. These policies need not be in a single ‘ABC policy’ document and may be contained in separate policies.</i></b></li> <li>• <b><i>There should be an effective mechanism for reporting issues to the ABC committee or compliance.</i></b></li> </ul>	<ul style="list-style-type: none"> <li>• The firm has no method in place to monitor and assess staff compliance with ABC policies and procedures.</li> <li>• Staff responsible for the implementation and monitoring of ABC policies and procedures have inadequate expertise on ABC.</li> </ul>

## ***ABC systems and controls in investment banks – examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Third-party relationships and due diligence</b>	
<ul style="list-style-type: none"> <li>• Where third parties are used to generate business, these relationships are subject to thorough due diligence and management oversight.</li> <li>• Third-party relationships are reviewed regularly, and in sufficient detail, to confirm that they are still necessary and appropriate to continue.</li> <li>• There are higher, or extra, levels of due diligence and approval for high risk third-party relationships.</li> <li>• There is appropriate scrutiny of, and approval for, relationships with third parties that introduce business to the firm.</li> <li>• The firm’s compliance function has oversight of all third-party relationships and monitors this list to identify risk indicators, eg a third party’s political or public service connections.</li> <li>• Evidence that a risk-based approach has been adopted to identify higher risk relationships in order to apply enhanced due diligence.</li> <li>• Enhanced due diligence procedures include a review of the third party’s own ABC controls.</li> <li>• <b><i>Consideration, where appropriate, of compliance involvement in interviewing consultants and the provision of anti-corruption training to consultants.</i></b></li> <li>• <b><i>Inclusion of ABC-specific clauses and appropriate protections in contracts with third parties.</i></b></li> </ul>	<ul style="list-style-type: none"> <li>• A firm using intermediaries fails to satisfy itself that those businesses have adequate controls to detect and prevent staff using bribery to generate business.</li> <li>• The firm fails to establish and record an adequate commercial rationale for using the services of third parties.</li> <li>• The firm is unable to produce a list of approved third parties, associated due diligence and details of payments made to them.</li> <li>• There is no checking of compliance’s operational role in approving new third-party relationships and accounts.</li> <li>• A firm assumes that long-standing third-party relationships present no bribery or corruption risk.</li> <li>• A firm relies exclusively on informal means, such as staff’s personal knowledge, to assess the bribery and corruption risk associated with third parties.</li> <li>• <b><i>No prescribed take-on process for new third-party relationships.</i></b></li> <li>• <b><i>A firm does not keep full records of due diligence on third parties and cannot evidence that it has considered the bribery and corruption risk associated with a third-party relationship.</i></b></li> <li>• The firm cannot provide evidence of appropriate checks to identify whether introducers and consultants are PEPs.</li> <li>• Failure to demonstrate that due diligence information in another language has been understood by the firm.</li> </ul>

***ABC systems and controls in investment banks –  
examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Payment controls</b>	
<ul style="list-style-type: none"> <li>• Ensuring adequate due diligence on and approval of third-party relationships before payments are made to the third party.</li> <li>• Risk-based approval procedures for payments and a clear understanding of the reason for all payments.</li> <li>• Checking third-party payments individually prior to approval, to ensure consistency with the business case for that account.</li> <li>• Regular and thorough monitoring of third-party payments to check, for example, whether a payment is unusual in the context of previous similar payments.</li> <li>• A healthily sceptical approach to approving third-party payments.</li> <li>• Adequate due diligence on new suppliers being added to the Accounts Payable system.</li> <li>• Clear limits on staff expenditure, which are fully documented, communicated to staff and enforced.</li> <li>• Limiting third-party payments from Accounts Payable to reimbursements of genuine business-related costs or reasonable hospitality.</li> <li>• Ensuring the reasons for third-party payments via Accounts Payable are clearly documented and appropriately approved.</li> <li>• The facility to produce accurate MI to assist effective payment monitoring.</li> </ul>	<ul style="list-style-type: none"> <li>• Failing to check whether third parties to whom payments are due have been subject to appropriate due diligence and approval.</li> <li>• Failing to produce regular third-party payment schedules for review.</li> <li>• Failing to check thoroughly the nature, reasonableness and appropriateness of gifts and hospitality.</li> <li>• No absolute limits on different types of expenditure, combined with inadequate scrutiny during the approvals process.</li> </ul>

## ***ABC systems and controls in investment banks – examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Gifts and hospitality</b>	
<ul style="list-style-type: none"> <li>• <i>Policies and procedures clearly define the approval process and the limits applicable to G&amp;H.</i></li> <li>• <i>Processes for filtering G&amp;H by employee, client and type of hospitality for analysis.</i></li> <li>• <i>Processes to identify unusual or unauthorised G&amp;H and deviations from approval limits for G&amp;H.</i></li> <li>• <i>Staff are trained on G&amp;H policies to an extent appropriate to their role, in terms of both content and frequency, and regularly reminded to disclose G&amp;H in line with policy.</i></li> <li>• <i>Cash or cash-equivalent gifts are prohibited.</i></li> <li>• <i>Political and charitable donations are approved at an appropriate level, with compliance input, and subject to appropriate due diligence.</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Senior management do not set a good example to staff on G&amp;H policies.</i></li> <li>• <i>Acceptable limits and the approval process are not defined.</i></li> <li>• <i>The G&amp;H policy is not kept up to date.</i></li> <li>• <i>G&amp;H and levels of staff compliance with related policies are not monitored.</i></li> <li>• <i>No steps are taken to minimise the risk of gifts going unrecorded.</i></li> <li>• <i>Failure to record a clear rationale for approving gifts that fall outside set thresholds.</i></li> <li>• <i>Failure to check whether charities being donated to are linked to political causes.</i></li> </ul>
<b>Staff recruitment and vetting</b>	
<ul style="list-style-type: none"> <li>• Vetting staff on a risk-based approach, taking into account financial crime risk.</li> <li>• <b><i>Enhanced vetting – including checks of credit records, criminal records, financial sanctions lists, commercially-available intelligence databases– for staff in roles with higher bribery and corruption risk.</i></b></li> <li>• Conducting periodic checks to ensure that agencies are complying with agreed vetting standards.</li> </ul>	<ul style="list-style-type: none"> <li>• <b><i>Failing to carry out repeat checks to identify changes that could affect an individual’s integrity and suitability.</i></b></li> <li>• <b><i>No risk based processes for identifying staff who are PEPs or connected to PEPs.</i></b></li> <li>• Where employment agencies are used to recruit staff, failing to demonstrate a clear understanding of the checks these agencies carry out on prospective staff.</li> <li>• Temporary or contract staff receiving less rigorous vetting than permanently employed colleagues carrying out similar roles.</li> </ul>
<b>Training and awareness</b>	
<ul style="list-style-type: none"> <li>• Providing good quality, standard training on anti-bribery and corruption for all staff.</li> <li>• Ensuring training covers relevant and practical examples.</li> <li>• Keeping training material and staff knowledge up to date.</li> <li>• <b><i>Awareness raising initiatives, such as special campaigns and events to support routine training, are organised.</i></b></li> </ul>	<ul style="list-style-type: none"> <li>• Failing to provide training on ABC that is targeted at staff with greater exposure to bribery and corruption risks.</li> <li>• <b><i>Failing to monitor and measure the quality and effectiveness of training.</i></b></li> </ul>

## ***ABC systems and controls in investment banks – examples of good and poor practice***

*(Proposed new guidance is highlighted in bold italics)*

Examples of good practice	Examples of poor practice
<b>Remuneration structures</b>	
<ul style="list-style-type: none"> <li>• Remuneration takes account of good compliance behaviour, not simply the amount of business generated.</li> <li>• <b><i>Identifying higher risk functions from a bribery and corruption perspective and reviewing remuneration structures to ensure they do not encourage risk taking.</i></b></li> </ul>	<ul style="list-style-type: none"> <li>• <b><i>Failing to reflect poor staff compliance with anti-bribery and corruption policy and procedures in staff appraisal and remuneration.</i></b></li> </ul>
<b>Incident reporting and management</b>	
<ul style="list-style-type: none"> <li>• Clear procedures for whistleblowing and the reporting of suspicions which are communicated to staff.</li> <li>• <b><i>Details about whistleblowing hotlines are visible and accessible to staff.</i></b></li> <li>• <b><i>Where whistleblowing hotlines are not provided, firms should consider measures to allow staff to raise concerns anonymously, with adequate levels of protection and communicate this clearly to staff.</i></b></li> <li>• <b><i>Firms use information gathered from whistleblowing and internal complaints to assess the effectiveness of their ABC policies and procedures.</i></b></li> </ul>	<ul style="list-style-type: none"> <li>• <b><i>Failing to maintain proper records of incidents and complaints.</i></b></li> </ul>



The Financial Services Authority  
25 The North Colonnade Canary Wharf London E14 5HS  
Telephone: +44 (0)20 7066 1000  
Website: [www.fsa.gov.uk](http://www.fsa.gov.uk)

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.

