Banco Santander
Bank of Tokyo Mitsubishi-UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JP Morgan Chase
Societe Generale
UBS

Wolfsberg Anti-Corruption Guidance

This Guidance replaces the Wolfsberg Statement against Corruption issued by the Wolfsberg Group[1] in 2007. Transparency International and the Basel Institute on Governance have been closely involved in the development of this Guidance, which aims to:

- describe the role of the Wolfsberg Group, and financial institutions more generally, in support of international efforts to combat corruption
- identify some of the measures financial institutions may consider in order to prevent bribery in their own operations and protect themselves against the misuse of their operations in relation to corruption
- set out guidance for an internal framework against corruption appropriate for a global financial institution.

1. Introduction

Bribery is commonly described as involving the promise, offer/acceptance or transfer of an advantage either directly or indirectly, in order to induce or reward the improper performance of a function or an activity. It may occur in a commercial arrangement (so called commercial bribery) or involve the misuse of public office or public power for private gain in order to obtain, retain or direct business or to secure any other improper advantage in the conduct of business.

The fight against corruption requires a comprehensive, multi-stakeholder approach including supranational and national government agencies and law enforcement, assisted by civil society and the wider business community. The members of the Wolfsberg Group are committed to participating in this fight and are opposed to all forms of corruption, including commercial bribery and the bribery of public officials and commit to abide by laws designed to fight corruption.

The Wolfsberg Group members recognise that their institutions may be misused for the purpose of paying bribes or laundering their proceeds and, as such, recognise the need to take practicable measures to counteract such misuse. While members are legally obliged to report suspicious activity in accordance with applicable laws that may be related to corruption when detected in customers' financial operations, in many instances and without further information (for example, absent red

[1] The Wolfsberg Group consists of the following leading international banks: Banco Santander, Bank of Tokyo-Mitsubishi-UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale and UBS. This Statement was made in conjunction with Transparency International and Professor Mark Pieth of the Basel Institute on Governance.

flags), it may not be apparent from account activity that misuse is occurring and therefore it is hardly possible for financial institutions to detect whether customers' transactions involve, or are otherwise linked to, corruption.

2. Scope

This Guidance addresses the issue of corruption as follows:

- First, the internal measures to prevent corruption that financial institutions may themselves consider to ensure that their own employees adhere to high standards of integrity are outlined below and further developed in Appendix 1
- Secondly, it considers the misuse of financial institutions to further acts of corruption, together with some of the measures that financial institutions could implement to attempt to mitigate activity involving corruption, which are further developed in Appendix 2
- Thirdly, it highlights the importance of taking a multi-party approach to combating corruption which includes efforts by governments and other entities. Areas for cooperation relevant to the financial aspects of corruption are set out for further consideration in the last section of this Guidance, the aim of which is to promote further dialogue amongst the relevant parties.

3. Financial Institutions' Internal Measures/Anti-Corruption Programme

Financial institutions should risk assess their own activities, products and services as appropriate to develop and implement effective Anti-Corruption policies, procedures and measures, which are proportionate to the corruption risks identified. The following internal measures are important mitigants that a financial institution should consider implementing to prevent bribery and to protect employees, as well as the organisation itself, in the event that an allegation of direct or indirect bribery or corruption is raised:

- Senior Management Commitment

Senior management should establish a culture in which bribery is strictly prohibited and which requires employees and officers to adhere to high standards of integrity.

- Risk Assessment

Financial institutions should understand and assess the nature and extent of the risks relating to bribery to which they are exposed.

- Establishment of a Control Environment

Clear, practical and proportionate policies and procedures should be implemented to mitigate the risks of bribery. These are likely to include procedures relating to due diligence when engaging third parties and the inclusion of anti-bribery representations and warranties in contracts with third parties, where appropriate; due diligence in relation to corruption risks in M&A (where the financial institution is acting in a principal and not merely an advisory capacity) and other transactions that are potentially higher risk; gifts and entertainment; charitable and political donations, hiring and internship practices; and whistleblowing.

- Monitoring and Review

The institution should have mechanisms in place to ensure compliance with key policies and procedures and implement improvements where appropriate.

4. Misuse of the Financial System through Corruption

Financial institutions may be misused to further acts of corruption or to launder the proceeds of bribery. For example:

- a customer directing or collecting funds for the purpose of paying a bribe
- a recipient of a bribe placing proceeds of the illicit bribe payment into the financial system
- the deposit of misappropriated state assets
- the clearing of transactions in any of the above cases.

In many instances, and without further information (for example, absent red flags), it may not be apparent from account activity that misuse is occurring and, therefore, it is hardly possible for financial institutions to make a distinction between accounts and transactions associated with corruption and those accounts and transactions that have a legal and sound commercial basis. This is particularly, but by no means exclusively, the case when dealing with substantial companies with complex business operations. The primary responsibility to ensure that funds are neither collected nor used for illicit operations, including bribery, must rest with a financial institution's customer or that customer's representatives. This is particularly true since a financial institution will seldom have a complete overview of its customer's financial activity.

Transactions involving the proceeds of corruption often follow patterns of behaviour common to money laundering associated with other criminal activities. Adherence to existing anti-money laundering policies, procedures and controls is therefore important in the fight against corruption. By the same token, the standards and guidance set out in existing Wolfsberg papers are similarly relevant to determine and manage money laundering risks related to corruption.[2]

5. Risk Based Approach

The Anti-Corruption programme addressing internal bribery risks should be based upon the financial institution's wider risk management strategy which will encompass a risk based approach. How a financial institution's risk assessment methodology and its anti-money laundering measures may apply to customer related corruption is addressed in Appendix 2 and is based on the following criteria: Services Risk, Country Risk, Customer Risk, Industry Risk and Transaction Risk Indicators ('red flags').

Where risk factors are identified, an assessment should be made as to whether the customer should be the subject of enhanced due diligence, transaction monitoring, senior management approval and/or other measures, including review and oversight of their financial operations, as may be appropriate. In some circumstances the filing of a Suspicious Activity Report or other notification to the authorities may be required by local law or regulations.

6. A Multi-Stakeholder Approach

The International community recognises the need for States to cooperate with one another in order to prevent and eradicate corruption. Organisations like the OECD and the UN also recognise that if efforts are to be effective, the involvement and support of individuals and groups outside the public sector are required, including civil society, non-governmental organisations and community-based organisations. Private sector companies and their related industry organisations, Chambers of Commerce and other industry organisations also have an important role to play in this regard in

[2] See http://www.wolfsberg-prinicples.com

apprising financial institutions of developments to prevent corruption by industrial sectors or individual firms.

The Wolfsberg Group supports the publicly led multi-stakeholder approach to addressing the following important areas where further dialogue and co-operation may lead to improvements in preventing and deterring bribery and other corrupt activity as it affects the financial sector, in particular:

- Governments and international institutions (IMF, World Bank): where governments, through their diplomatic services or political analysts, have evidence of corruption in foreign countries or have evidence that foreign officials and their families have acquired assets through corruption, they should take appropriate action such as sharing this assessment with civil society and the private sector in an appropriate manner.
- Governments and their agencies: export credits agencies, development aid, lending and trade departments, should carry out co-ordinated due diligence and monitoring so that an appropriate audit trail in respect of money transfers and credits may be established by them.
- Governments and international bodies: in order that a more co-ordinated and harmonised approach may be developed between governments as to the recovery and repatriation of assets held by financial institutions and identified as connected to corruption.[3]
- Law enforcement and Financial Intelligence Units: should identify new techniques used by money launderers in relation to bribery and other corrupt activity, communicate typologies to the financial community and develop appropriate countermeasures.
- Regulators and supervisors: in relation to the development of policies and procedures that are consistent with regard to the definition and identification of Politically Exposed Persons as well as the initial and on-going management of relationships with customers who fall into this category.
- Civil society and non-governmental organisations: should identify trends, patterns and mechanisms used by bribe payers and recipients, thereby gaining a better understanding of the causes and effects of bribery and other corrupt activity, in order to prevent the misuse of financial institutions and support the development of appropriate standards and controls.

The Wolfsberg Group believes that constructive dialogue in this area will help to increase the knowledge and ability of such agencies and institutions to identify trends, patterns, money laundering techniques and mechanisms used in the furtherance of acts of bribery and corruption and, with an effective public private partnership, financial institutions will be better placed to assist in the fight to prevent and/or detect and disclose incidents of corruption.

[3] See for example the World Bank Stolen Asset Recovery (StAR) Program.

Wolfsberg Anti-Corruption Guidance Appendix 1
Guidance on an Internal Anti-Corruption Framework

This Appendix focuses on the internal bribery risks a financial institution might face and not those posed by client risk which is addressed in Appendix 2. This Appendix provides guidance only and may be taken into consideration by financial institutions when developing, implementing and enhancing their Anti-Corruption programmes.

1. Introduction

While no Anti-Corruption Programme ("programme") can comprehensively prevent or protect against corruption, and there is no one-size-fits-all programme, the following guidance on the components of such a programme and the minimum standards set out below will help financial institutions to prevent bribery.

The implementation of the programme will depend on the make-up of the financial institution but, wherever possible, should commence simultaneously throughout the institution to ensure the establishment of globally consistent minimum standards.

While the aim is to focus on areas of risk that are of particular relevance to global financial institutions, adherence to this guidance is not a substitute for legal advice. Financial institutions should therefore seek the assistance of their own internal legal advisers and external counsel for advice as may be relevant to their respective businesses.[4]

2. Summary of the Minimum Elements of an Anti-Corruption Program

- The financial institution's Anti-Corruption stance should be developed by senior management and endorsed by the Board or equivalent body.
- A written policy (or policies) with a general prohibition on all forms of corruption and its authorisation should address commercial bribery and the bribery of public officials including the promising, offering, giving or receiving of bribes directly or indirectly.
- Policies and procedures should delineate the risks associated with public officials. The definition of "Public Official" must meet international standards and should also define when the officers and employees of a State Owned Entity should be treated as "Public Officials" as a result of government ownership or control.
- Internal communication of the Anti-Corruption principles through policies, procedures and guidance, with commensurate training of all appropriate employees and relevant third parties.
- Roles and responsibilities should be allocated to sufficiently senior management to ensure the programme and appropriate controls are implemented throughout the institution, its branches and subsidiaries (including those in the non-financial sector).
- An independent unit such as Compliance, Legal or Security must have the knowledge, expertise and responsibility to manage the programme and be appropriately resourced.
- The commitment to a firm Anti-Corruption policy should be publicly communicated (e.g. as part of a corporate social responsibility programme).

[4] While domestic law will be important, internationally active financial institutions should also consider the relevance of the US Foreign Corrupt Practices Act, the UK Bribery Act and Guidance Note, other national laws passed under the OECD Convention Against Bribery in International Business Transactions; Annex II to the OECD Recommendations for Further Combating Foreign Bribery in International Business Transactions, as well as relevant publications by civil society such as Transparency International and the International Chamber of Commerce.

3. Governance

The most senior management of the financial institution should ensure that the Anti-Corruption standards become part of the institution's cultural fabric and are applied consistently throughout the organisation and in all jurisdictions where business is conducted.

3.1 Roles and Responsibilities

To ensure the effective functioning of the programme, the following roles and responsibilities should be allocated:

Senior Programme Management (Executive Board or equivalent body and the Board of Directors): a member of the firm's Executive Board or equivalent body should have responsibility for the bank's Anti-Corruption programme. Periodic reporting about the programme should be made to both the Executive Board or equivalent body and the Board of Directors.

Business Line Managers: carry primary responsibility for compliance with the established programme, which may include doing their own, (independent) assessment and identification of potential risks and responsibility for (all) efforts to mitigate those risks.

Programme Manager*:* an independent unit within the financial institution must have the knowledge, expertise and responsibility to manage the programme and be appropriately resourced. This unit should be part of a Control Function such as Compliance, Legal or Security, and not a purely advisory function. This unit should serve as the institution's centre of competence for all matters with respect to the Anti-Corruption programme.

3.2 Internal Reporting

Regular reporting to senior management on the programme is a means to maintain reliable and comprehensive escalation practices. The frequency of reporting should be sufficient so as to ensure the continued effectiveness of the programme. Relevant data should be collected from around the institution at regular intervals by the programme manager, to assist in proper programme maintenance.

Reports should contain action items/deliverables, as well as some or all of the following:

- Status update on programme implementation including Key Performance Indicators/metrics (e.g. in relation to training)
- Significant deviations by employees from internal rules on gifts and business entertainment
- Approvals of third party intermediaries identified as presenting increased risks
- Allegations of corruption against the institution or its employees
- Employee reports of any solicitation or offer of bribes or other corrupt proposals by third parties
- Whistleblowing reports raising bribery issues
- Relevant external legal & regulatory developments
- Any other significant issues such as regulatory reporting or filings in relation to internal bribery

3.3 External Auditing and Reporting

Consideration may be given to having the adequacy of the programme tested and or verified by external organisations or auditors as may be appropriate. A financial institution's Anti-Corruption commitment should be communicated externally.[5]

4. Policies and Programme Framework

4.1 Overall Policies

An Anti-Corruption policy which is applicable globally and group-wide to all staff should form the reference point for all related Anti-Corruption standards and policies. This policy should be visible, accessible and encapsulate the “tone from the top” from senior management and stipulate zero tolerance for all forms of bribery, including the prohibition of facilitation payments.[6] The Anti-Corruption policy may reference the institution’s Code of Conduct or other ethics statement, which, in turn, should contain specific reference to the prevention and avoidance of internal bribery and corruption.

Other areas of focus for the Anti-Corruption policy (or covered in separate documents/policies) are: gifts; hospitality; entertainment and expenses; political and charitable donations; sponsorship; marketing; due diligence procedures applicable to third parties and in the context of M&A transactions (where the financial institution is acting in a principal capacity) and other potentially higher risk transactions; inclusion of Anti-Corruption representations and warranties in contracts with appropriate third parties; hiring and internship practices; solicitation and extortion and conflicts of interest.

Financial institutions should ensure that a clear definition of a 'Public Official' is included in relevant policies. Anti-Corruption laws generally treat (foreign) public officials and their representatives/agents as presenting increased corruption risks for companies seeking to obtain or retain government business. Internal policies should, as a minimum, meet international standards that define ‘(foreign) public officials’ whereby the standards should also apply to domestic public officials. The public official definition should provide for a procedure to determine the degree of government ownership or influence that would require an entity to be treated as state owned or controlled and therefore its managers and employees as within the definition of a public official, particularly where such entities are treated under domestic law as government instrumentalities.

Appropriate due diligence and senior management approvals should be implemented as warranted by the risks, such as in certain situations where public officials are involved, for example if high value gifts or business entertainment are to be provided; or where interactions with third party intermediaries retained by a financial institution and public officials may occur, in which case enhanced due diligence may be required.

The programme must cover all parts of the front and back office, including any so-called middle-office functions such as Finance, Tax and Operations. Departments such as Corporate Affairs, Marketing, Sponsorships, Facilities, Business Development, Corporate Real Estate and Procurement should also be included, particularly given their close interaction with external vendors and service

[5] External communication could, for example, be in the context of a financial institution's annual social responsibility report. Guidance on reporting can be found in the UN Global Compact TI Reporting Guidance on the 10th Principle against Corruption at http://www.unglobalcompact.org/docs/issues_doc/Anti-Corruption/UNGC_AntiCorruptionReporting.pdf. The reference to this guidance paper is by way of example only.

[6] Some financial institutions may create exceptions to this prohibition where serious harm to the health or personal safety of an employee is at stake.

providers. Certain temporary staff, outsourced service providers, contractors and any other personnel by virtue of their role, location on premises and access to information should also be in scope.

For institutions that maintain Compliance Manuals/Employee Handbooks, there should be specific reference to each employee's personal responsibility to protect their respective institutions, its reputation and themselves from the risks arising from bribery and corruption.

4.2 Risk Assessments Inform the Programme Framework

The programme framework is informed by periodic risk assessments, which serve to determine the appropriateness of an institution's risk based approach. Some areas of business may be more susceptible to acts of bribery and may therefore need more frequent reviews.

Financial institutions must regularly re-assess their internal bribery risks quite apart and separately from any risk assessment conducted in connection with client risk (see Appendix 2). Defining which categories of third parties can create potential liability will be a key element in the risk assessment. Similarly, the risk rating of countries where the financial institution is active, where clients are based and where a financial institution might seek to engage finders or intermediaries to pursue business opportunities or new clients will inform the risk profile. Transactions, products or services may also pose increased bribery risks, particularly where state owned entities or public officials are involved. Activities undertaken by an institution’s branches, subsidiaries and service providers to those entities should also be subject to risk assessment.

The programme's scope will also be determined by assessing the conflicts of interest and corruption risks associated with gifts and entertainment, sponsored travel, hiring/internships, charitable donations and political contributions. Appropriate risk mitigants, controls and monitoring must be implemented to address the identified risks as appropriate.

Employees should understand where the governance and oversight responsibility lies for ensuring an effective Anti-Corruption programme and for monitoring the existing framework to ensure compliance with industry best practice and regulatory standards and requirements.

5. Third Parties

Vendors and service providers, including real estate brokers, agents, lawyers, accountants, intermediaries, finders, lobbyists, marketing firms, advisors, technical specialists and so on, hereinafter referred to as 'third parties', are commonly used by financial institutions to develop, expand or maintain business. The Anti-Corruption policy should be made known to third parties as appropriate, and it should be made clear that all activities carried out on behalf of the financial institution must be compliant with applicable anti-bribery laws and (as appropriate) the policy. The due diligence and retention procedures associated with third parties should apply a risk based approach and be reflected in appropriate policies and procedures.

Payments to third parties should represent no more than appropriate remuneration for legitimate services rendered. The third party must explicitly agree not to pay bribes and contracts should address the possibility of termination of the agreement if a bribe is paid.

The monitoring of the third party's activities and expenses may be appropriate in some circumstances, particularly if any red flags emerge during the relationship. Monitoring could comprise reviewing the services actually rendered before payments are made; reviewing any unusual or excessive expenses; auditing the third party on a risk based, periodic basis and promptly if any suspicions arise; certifications of compliance by the third party with applicable anti-bribery laws and (as appropriate) the financial institution's Anti-Corruption standards.

5.1 Agents/Intermediaries Obtaining/Retaining Business for the Financial Institution

Third parties that are engaged, directly or indirectly, by the financial institution to act on their behalf to find, introduce, obtain or maintain business, clients or licences for the financial institution, or who introduce the financial institution to government officials or government enterprises, irrespective of whether a transaction is completed, should be subject to an assessment that examines:

- the business necessity for their retention
- the third party's status (e.g. to determine whether they, their beneficial owners, or directors, managers of employees are themselves public officials), background and reputation (e.g. qualifications for the services to be provided)
- the likelihood of interactions with a public official where that official has discretionary authority over some matter impacting or involving the financial institution
- the country risk (reference may be made to countries perceived as having high levels of corruption)
- the type of client
- the reputation of the third party
- the proposed products and services and the amount and terms of compensation (inappropriate or unusually large 'success fees' would be a red flag).

This assessment will inform the risk categorisation of a third party and the consequent level of due diligence and escalation procedures.

Where red flags are uncovered, further due diligence and escalation procedures should be undertaken so that a fully informed decision as to whether to employ the third party can be taken. While a red flag on its own may not mean the relationship cannot go ahead, its significance may need to be examined in the context of all the facts, and what did not present itself as a serious issue at one stage of a relationship may pose significant risks of liability at a different stage. Similarly, where red flags arise in the context of a review, escalation procedures should take effect and consideration as to whether to continue the relationship should be undertaken and the outcome documented.

There are many red flags which would warrant further review, the following are a non-exhaustive selection.[7] The third party:

- has a flawed background or reputation
- is a recent senior public official of the same government department or business responsible for the award of the contract or matter at issue
- is suggested by a public official, particularly one connected to the business or matter at issue
- has a close business, personal or family relationship with a public official who has discretionary authority over the business or transaction at issue
- objects to Anti-Corruption representations or warranties being included in the agreement
- does not reside or have a significant business presence in the country where the customer or business is located
- is a shell company or has some other non-transparent corporate structure
- requires payment of a commission, or a significant portion thereof, before or immediately upon award of the contract
- requests unusual contract terms that raise local law issues
- requests payment in cash, advance payments, payment to an individual or entity that is not the contracting individual/entity, payment to a numbered bank account or a bank account

[7] See ICC Guidelines on Agents, Intermediaries and Other Third Parties, 19 November 2010.

not held by the contracting individual/entity, or payment into a country that is not the contracting individual/entity's principal place of business or the country where the services are performed.

Applicable risk mitigation for such third parties includes KYC and due diligence processes; background checks; obtaining external risk reports on the entity or individual; media searches and escalation procedures for material negative news related to bribery; inclusion of appropriate contractual terms with Anti-Corruption representations and warranties; and on-going monitoring and periodic reviews post appointment. Communication of the Anti-Corruption standards and appropriate training of third parties should also be carried out so as to mitigate liability risks, preferably in the local language and with periodic follow ups as may be necessary. Financial institutions should maintain a record of the names, terms of employment and payments to all third parties who are retained by them in connection with transactions with public officials, state or private entities.

Third parties that are classified as higher risk may require more robust acceptance practices, including, where appropriate, an independent review or the involvement and/or sign-off by senior management.

5.2 External Service Providers/Vendors & Procurement Processes

The procedures relating to the procurement of goods and services from external service providers, vendors and similar third parties should be set out in clear guidelines that address bidding processes; selection criteria; and the risks of conflicts of interest such as the receipt of gifts from such third parties by employees involved in the selection processes.

5.3 Joint Ventures / Principal Investments & Acquisitions

Successor liability relating to corruption could arise where a financial institution has merged, partnered with or acquired another company. Due diligence around such transactions should therefore aim to obtain reasonable assurance of identifying any past or current instances of bribery, over a reasonable period of time prior to the completion date of the transaction. The scope of the diligence to be conducted should involve person(s) separate from the proposed management team and employees in the proposed venture/merger. In certain instances (e.g. hostile acquisition), it may be necessary to conduct due diligence post acquisition, in which case it should be finalised within a reasonable period (such as three months) after completion of the transaction. Where post-transaction due diligence identifies an actual or suspected bribery incident, the institution should consider whether to request an opinion from outside counsel or appropriate law enforcement agencies regarding appropriate action to take.

6 Donations

Accurate books and records of political and charitable donations should be maintained. Internal policies should specify any requirements for pre-approval of donations or limitations on donations and the criteria for those limitations. Financial institutions should not seek to gain an economic advantage in relation to business giving and implement approvals and reviews of donations.

6.1 Charitable Donations / Sponsorship

Organisations should have a clear and transparent approach to charitable donations, a process for selecting suitable recipients and conducting appropriate levels of due diligence, employing a risk based approach. Certain donations which may appear legitimate on their face could in fact serve as a subterfuge for bribery. For example, if a charitable donation is solicited from a financial institution by a Public Official for a charity connected to her/his family and there is pending business with the government department where the public official is employed, such a donation should be strongly discouraged or require approval from the Executive Board or equivalent body.

6.2 Political Contributions

The laws on donations to political parties vary widely around the world. In some countries they are extensively regulated and in others they are not. In any event, it is advisable for financial institutions to adopt minimum standards to control political donations. In so doing, the institution will mitigate the risks of creating a conflict of interest in respect of future business. Heightened scrutiny should be applied where the donation is solicited by the client or a Public Official, regulator, lobbying company or trade organisation (a financial institution should ensure it is not used to channel a bribe to a Public Official on behalf of third party).

7. Gifts and Business Entertainment

Financial institutions provide gifts and business hospitality to a wide range of stakeholders including clients, prospective clients, shareholders, employees and, where laws permit, also to public officials. Such entertaining is undertaken to improve the image of the financial institution, present products and services or establish cordial business relations and is a normal and acceptable part of business relationships. In addition, many financial institutions seek to enhance their brand image or status in the communities where they operate through sponsorships of events and institutions. Such sponsorships or donations may support the arts, sporting or cultural events, conferences, seminars, educational establishments, academic endeavours or otherwise be of a philanthropic or charitable nature. Business entertainment may also comprise invitations to stakeholders and clients in connection with a unique or one-off event such as celebrating a corporate milestone or anniversary.

Global financial institutions serve a wide variety of clients many of whom are offered business entertainment in one form or another. Business hospitality should be proportionate and take account of the recipient’s role or position as appropriate.

The offering of exclusive or relatively large entertainment or gifts to prospective or existing private clients to whom such entertainment or gifts would not be of significant value relative to their personal wealth is acceptable. If the person acts on behalf of others, the financial institution's exposure to that individual in that capacity should be considered when extending gifts or entertainment.

Business entertainment of a public official must be reasonable and proportionate and take account of all applicable laws and regulations to which the public official is subject, both domestically and by laws that have an extra-territorial reach. Where public officials are subject to internal regulations or codes of conduct, which are not publicly available, it may be advisable to obtain external counsel’s opinion on what would constitute reasonable business entertainment and/or take other steps to be transparent towards the recipient’s employer or organisation.

Where a financial institution has hosted or sponsored a conference, seminar or other business oriented event that has served to educate or inform employees or other clients, and public officials have been amongst the external speakers, it would typically be acceptable, absent other risk factors to bestow a reasonable gift as a token of appreciation to all the speakers, including any public officials, in recognition of their contributions and separate from any contractual fee arrangements.

Business entertainment may also be an intrinsic part of a business deal such as where deal or non-deal road-shows are organised and which involve an itinerary over several days. In such cases the client and/or the financial institution may cover the costs of the travel, hotels and entertainment. In all cases, and whatever the permutations of the arrangements, it behoves financial institutions to ensure they have clear contractual arrangements with their clients and any third parties participating in the road-shows. Where entertainment arises on an ad-hoc basis, such as where a road-show extends over a weekend where no business meetings are planned, institutions should make provision for such eventualities in their policies and procedures so that a reasonable approach is taken to such situations and transparency is maintained vis-à-vis all parties.

Financial institutions will need to have escalation procedures to address the risks presented in certain circumstances that will require particular care before gifts or entertainment can be offered. For example: when seeking to entertain individual public officials from government entities that have commercial operations, but which are also in a position to regulate or supervise the financial institution, these will need to be reviewed and any risks mitigated appropriately before any invitations are issued. Similarly, potential conflicts of interest will need to be addressed where, for example, a public official is the CEO of a state owned entity that conducts business with the investment banking arm of the institution, but is also a private client with substantial assets with the wealth management division of the bank and is proposed as a guest to an exclusive function sponsored by the bank. Risk mitigants will depend on all the circumstances and what is permissible according to applicable laws, but could include obtaining external counsel's advice, issuing transparency letters to the government agency or entity where the public official works, extending the invitation to the public entity more generally and not targeting any specific individual; as well as the inclusion of disclaimers on invitations that place the onus on the recipient to be transparent to his/her employer or organisation and placing threshold limits on entertainment within a given timeframe.

A financial institution's policy on gifts and entertainment should set forth general principles for providing gifts and entertainment including, for example, any circumstances requiring outright prohibitions; triggers or threshold levels (where these are used) above which consultation and approval by the front office from Legal & Compliance should be sought; statements as to appropriate frequency and amount for clients and separately for public officials; considerations to be undertaken by business and Compliance approvers when acting on requests for provision; books and records requirements and items that may be excluded from consideration as proper gifts or entertainment (for example deal road-shows).

Policies should also include guidance for the following:

- Distinct treatment of public officials such as prior approvals before extending any invitations, exclusion or reduced thresholds (where these are used)
- The treatment of cash payments or their equivalent (generally prohibited absent exceptional approvals from senior management in the front office business and Legal & Compliance)
- The provision of gifts and entertainment to a client's spouse, children and other family members (generally not acceptable but permissible where usual and customary to do so)
- The treatment of cultural events within certain jurisdictions that may require waivers from standards or policies
- The treatment of other items of value provided by the institution, which are not technically classed as gifts and entertainment,[8] but do involve the provision of items of value to the recipient such as organizing a road-show, internships and speaker fees

[8] This definition should distinguish between items that are services provided to clients and traditional gifts and entertainment expenses.

- Specialised treatment of events that are sponsored by the financial institution, which provide a higher level of transparency, but may still require analysis
- Specificity around books and records requirements
- Requirements for any automated systems to be employed in connection with the giving/receipt of gifts and business entertainment.[9]

Financial institutions should also have policies and procedures that address the receipt of gifts and business hospitality from clients and third parties. Such policies and procedures should address risks related to conflicts of interest and bribery; the circumstances when gifts and entertainment should be declined and identify any gifts or business entertainment which the employee may not accept.

8. Whistleblowing

Institutions should establish a whistleblowing system that is an integral part of their programme. The system should aim to receive and entertain, in full confidentiality, all reasonable requests for advice and guidance on business conduct that appears to raise ethical concerns (including as they may be related to any acts associated with bribery including offers or solicitations), that are raised by its employees, subsidiaries and affiliates, and also to any extent possible by any third party acting on behalf of the institution or supplying goods and services thereto.

All whistleblowers' reports should be diligently acknowledged, recorded and screened. Bona fide reports should be investigated by the institution's whistleblowing unit and forwarded under strict confidentiality rules, to the appropriate person(s) or units within the institution. Financial institutions should have guidance in place for persons who are responsible for undertaking an investigation into the qualifying disclosures of malpractice. It should contain instruction on how to investigate instances of reported malpractice, who should be contacted regarding a particular disclosure (internally and externally) and it should align to applicable local regulation and the internal Code of Conduct procedures.

Financial institutions should maintain, to the fullest extent possible and at all times, the confidentiality of the data revealed through whistleblowing, as well as the identity of the whistleblower, subject to overriding legal requirements and should protect such data with the most appropriate means.

Confidentiality should be maintained throughout the process, with information transferred purely on a need to know basis, and employees should be provided with reporting hotline information.

9. Communication, Training & Education

Anti-bribery policies, procedures and standards have to be communicated effectively both internally and to appropriate third parties. The training should have at its foundation a 'tone from the top' message from senior management and should apply to persons at all levels of the institution including Members of the Board. Training should commence on joining the institution (during induction training) and thereafter be provided to all appropriate employees and third parties on a regular basis, with the frequency determined by the bribery risk assessment.

Substantively, training should include explanations of relevant definitions (bribery, public officials, etc.), references to applicable internal policies, procedures, laws and regulations, case studies and/or practical examples which present potential scenarios that employees may encounter in their line of

[9] The development and implementation of suitable automated technology, capable of capturing and monitoring data related to the providers and recipients of gifts and entertainment, as well as aggregating values globally and across all business units, presents significant challenges to most financial institutions.

business and/or within the financial institution. A clear explanation of individual employees' duties and responsibilities under applicable laws, regulations and policies should include information on when and how to seek advice, escalation and whistleblowing procedures and how to report any concerns or suspicions of bribery.

Post-training assessments or attestations of understanding should be completed by trainees (where it is appropriate to do so, such as in internal computer based learning courses) with completion records maintained for review by the senior programme managers. Detailed records should be kept of all training delivered to facilitate tracking and reporting of training sessions delivered. Specialist training should be provided as necessary to identified employees, which may include holders of Group delegated authority, business unit heads with responsibility for conducting due diligence on, and contracting with, third party intermediaries engaged to obtain new business or to retain existing business, as well as individuals who deal with public officials. Special awareness raising or training should also be considered to those who regularly extend gifts and business entertainment to clients or prospective clients above a certain amount, or to those who have authority over sponsorship and donation budgets. Employees should be given the chance to provide feedback on the training they have received at an early opportunity after its conclusion.

10. Controls

It is important that the appropriate control environment be established to support the on-going programme and ensure its continued robustness.

10.1 Monitoring & Surveillance

The leveraging of anti-money laundering monitoring processes to address bribery risks should be considered when developing an effective approach to monitoring for bribery. As businesses and circumstances change, monitoring should be on-going and institutions should ensure that they have sufficient resources to monitor, assess and mitigate bribery risks that emerge. Attention should be paid to public media to ensure that risks are identified early on. This is particularly relevant for firms which are expanding into new jurisdictions (where there may be a lack of transparency) and establishing new business relationships.

The output from monitoring and surveillance activities should be part of the overall control framework placed around bribery. Post transaction monitoring for expense reimbursement/receipt of gifts or business entertainment, sponsorship, corporate events and vendor retention should be conducted to assess adherence to internal process and procedures.

The four eyes principle should be included as an independent control verification measure particularly for activities or contracts that present increased bribery risks and which may require senior management review.

Breaches of a financial institution's Anti-Corruption policies by an employee, or an agent working on the institution's behalf, may involve unusual or suspicious activity warranting investigation by a control function such as the internal Financial Intelligence Unit or equivalent. In some situations, it may be advisable to retain outside counsel to assist in conducting the investigation. If suspicious activity is confirmed or suspected, or if there is no plausible explanation for the activity, the procedures relating to the filing of a Suspicious Activity Report should be followed, as required by local laws and regulations.

10.2 Risk Assessment & Review Function

In contrast to the Audit function, firms should also employ an internal risk assessment process to analyse holistically the risks across business areas and to identify any existing gaps or control failures and associated remediation recommendations. As part of their considerations, those involved in the Risk Assessment process should be conscious of the existence of bribery and corruption related risk as applicable to the areas that they propose to review.

10.3 Contractual Arrangements

The scope of anti-bribery terms in contractual arrangements with third parties will necessarily depend on factors such as the level of potential bribery risk posed by a given counterparty, the transaction in question and all the circumstances of the relevant contractual negotiation. Depending on the risk profile of the particular counterparty and the transaction in question, due consideration should be given to what is proportionate in the circumstances. Possible provisions for inclusion may include a prohibition on all types of bribery, an acknowledgement that appropriate anti-bribery policies and procedures are in place, and (if appropriate) termination, audit and books/records provisions. Third parties should not be contracted with unless key stakeholders are satisfied that the risks associated with third parties are within the risk appetite of the financial institution and/or have been properly mitigated and controlled. In cases of enhanced risk, it may be advisable to obtain an independent assessment from Compliance or other independent control function.

10.4 Cash and Payment Controls

All payments must be made for legitimate business reasons. Invoices, receipts and substantiating documentation should be provided with an appropriate level of detail in order to support authorisation for re-payment of fees, travel and expenses and gifts and entertainment expenditures, which should be subject to a "four eyes" approval process and in accordance with the financial institution's internal gift and entertainment procedures. General principles such as a prohibition on cash payments should also be included in the financial institution's relevant policies and procedures.

10.5 Books and Records

Accurate books and records must be maintained in accordance with applicable regulatory and legislative requirements. Front and back office employees share responsibility for accurately documenting the provision of any items of value to clients, as well as payments to third parties and any approvals mandated by other internal policies and procedures.

10.6 Standards for Human Resources (including merit based hiring and internships)

Guidance regarding the offer of employment or internships, and the associated bribery risks, should be developed by key stakeholders including Human Resources (HR) to ensure that all offers of employment are merit based. Offers of employment or internships (or the opportunity to be considered for such) as an inducement or quid pro quo to obtain or retain business, to gain an unfair business advantage or to influence a government or regulatory action should be prohibited. HR should maintain records which conclusively prove the bona fides of internships. Instances of hiring practices that appear to violate these principles should be investigated by an independent internal function or, where appropriate, with the assistance of outside counsel.

Incentives and bonuses are a common and acceptable part of compensation within the financial services industry. When designing remuneration systems, however, management should be sensitive to the possibility that managers and employees may misunderstand incentives based upon specific sales and performance goals especially where tied to commissions, advancement, bonuses, or other 'one-off' payments related to a specific deal or transaction, in that they may encourage personnel to resort to improper practices to achieve such goals.

10.7. Third Parties and Procurement

Depending on the risk assessment, financial institutions should decide to what extent the procurement process and third party relationships should be managed or reviewed by a unit that is independent of the contracting party within the financial institution.

Wolfsberg Anti-Corruption Guidance Appendix 2
Guidance on Client Related Corruption Risks

This Appendix provides guidance only and is based upon existing Wolfsberg papers.[10]

Bribery has long been identified with the public sector and with certain industrial sectors which are widely regarded as being more prone to the risk of corruption than others.[11] In addition to those areas, however, financial institutions may also be at risk of being misused by persons paying and receiving bribes, including the laundering of the proceeds of bribes. This Appendix describes in more detail how financial institutions may mitigate the risks of such misuse.

Many of the measures put in place by financial institutions to mitigate money laundering risk are relevant to the prevention and detection of client related corruption. For example, adequate customer due diligence procedures, including enhanced due diligence for Politically Exposed Persons, support the mitigation of corruption risk. In addition, measures implemented by financial institutions to ensure that wire payments contain complete and accurate information also assist in the prevention and detection of corruption.

1. Services Risk

The payment and receipt of bribes may be effected through a variety of services provided by financial institutions. However, in considering and assessing exposure to this risk, there are certain services that may be considered more vulnerable to abuse than others. The risks and possible mitigating measures are highlighted below together (where appropriate) with any particularly relevant red flags.[12]

1.1 Private Banking

Risks – Private Banking, particularly international private banking services, are vulnerable for a variety of reasons including the high net worth characteristics of the customer base, the offshore nature of the facilities offered and the type of products and services available (e.g. asset protection and investment vehicles such as trusts, foundations, personal investment companies, cross border wire transfers, etc.). In particular, recipients of bribes may seek international private banking services to launder the proceeds of the bribe.

Mitigating Measures – Important mitigating measures include acceptance procedures for customers including the identification of beneficial ownership, the verification of identity and due diligence, notably establishing the source of wealth and source of funds deposited. These measures should also take into account risk indicators such as countries identified as representing higher risk for corruption, whether the customer is categorized as a PEP, whether the customer is involved in a higher risk industry, for example, arms dealing or acting as an agent or intermediary for the arms trade or other industry sector identified as

[10] See http://www.wolfsberg-prinicples.com

[11] See the Transparency International Global Corruption Barometer, published annually.

[12] In most cases, a financial institution will not necessarily be aware that corruption is involved in a particular transaction, 'red flags' may, however, be identified in the course of anti-money laundering transaction monitoring and financial institutions should take measures to address such 'red flags.' None of the transactions types or patterns mentioned as 'red flags' in this Appendix should automatically be considered suspicious without further investigation. Where such transaction types or patterns are identified, there may often be acceptable explanations for such activity. The 'red flags' mentioned in this Appendix do not comprise a comprehensive list nor are they intended to be used by financial institutions as a mandatory set of rules that must be applied. Each financial institution should take its own view on how best to configure its monitoring, based on its own circumstances.

posing increased corruption risks. Various risk attributes and red flags should be taken into account by an institution's policies to identify when enhanced due diligence should be applied to a prospective or existing client relationship. Adherence to the Wolfsberg AML Principles on Private Banking should constitute effective risk management in this area.

Red Flags - Substantial cash or wire transfers to or from an account of a private banking customer where such activity is not consistent with legitimate or expected activity. Particularly substantial activity over a relatively short time period and/or the improper use of corporate vehicles to obscure ownership and/or the involvement of industries and/or countries posing increased corruption risk may also raise suspicions that require further due diligence and investigation.

1.2 Project Finance / Export Credits

Risks – The provision of finance to customers of a financial institution and/or involvement in transactions linked to major project finance initiatives, such as those to support public sector infrastructure/construction projects or the exploitation of natural resources, are particularly vulnerable to the payment of bribes or other corrupt activity, not least because of the size and complexity of projects of this nature, in combination with the generally large number of participants involved, including government export credit agencies, private companies and banks. The responsibilities of financial institutions will generally be limited to their direct involvement in the financial advisory services, arranging or financing process such as with the borrower, exporter of record or sponsor and then only as regards disbursement of funds to, or for and on behalf of, the direct customer

Mitigating Measures – Where governments, international organisations or multilateral lending organisations are involved in loans, donations or other arrangements or in facilitating trade through export credits, financial institutions may have an involvement in these arrangements. In these circumstances, financial institutions can reasonably expect such governments or organisations to conduct appropriate assessments (diligence) on the parties involved and to take other appropriate measures to ensure that funds are not siphoned off to pay bribes. Financial institutions will, however, need to complete their own due diligence as appropriate to their customers.

Red Flags:
- Projects located in countries where corruption risks are regarded as being high
- A project structure involving legal entities in offshore jurisdictions where the ownership and role of the entity is not clear and purpose of the payment is not transparent
- A project involving the use of intermediaries
- Project payments to third parties, whose role in the transaction is unclear or who request unusually opaque methods of payment

Factors that could be considered by a financial institution whose customers are directly involved in project finance or related activities might include country, industry and political risk (see sections 2, and 3 below) as well as due diligence or enhanced due diligence on the customer. For example, it might be appropriate to consider a customer's record in relation to convictions or other sanctions for corruption, if known. It would not be reasonable to extend due diligence beyond the direct customer to sub-contractors, suppliers, agents, consultants or other intermediaries. However, if the financial institution discerns something sufficiently unusual about the transaction, it should seek clarification about the matter, so as to dispel concerns it may have with regard to the transaction.

1.3 Retail Banking

Risks - The diversity of products and services offered through a retail banking operation results in a huge variety of customers. This factor, together with the nature and scale of transactions executed through retail banks means that it is virtually impossible to identify specific transactions that may be linked to corrupt activities, particularly petty corruption, unless such transactions are sufficiently unusual and are identified in the course of monitoring designed to detect money laundering.

Mitigating Measures – In general a retail bank's AML policies and procedures should be applied adopting a risk based approach.

2. Country Risk

Countries having been identified by credible sources as having significant levels of corruption, for further information see the Wolfsberg Guidance on a Risk Based Approach.

3. Customer Risk

Certain customers identified during due diligence or enhanced due diligence (initial and on-going) may potentially represent a greater degree of risk. Such due diligence or enhanced due diligence may include identification of negative publicly available information from credible sources that calls into question a customer's activities regarding corruption, or, indeed, that indicates that prosecutions or actions have been taken by governmental authorities and/or law enforcement. The risks and possible mitigating measures are highlighted below, together with any particularly relevant red flags. Examples include:

3.1. Politically Exposed Persons - PEPs potentially represent higher risk because they either are in a position to exert undue influence on decisions regarding the conduct of business by private sector parties, or have access to state accounts and funds.[13]

Red Flags - Substantial cash or wire transfers into, or from, an account of a customer identified as a PEP, where such activity is not consistent with legitimate or expected activity. Particularly substantial activity over a relatively short time period and/or the improper use of corporate or other vehicles to obscure ownership may also raise suspicions.

3.2. Intermediaries/agents - In certain industries, the services of intermediaries or agents are used by companies to help secure or retain business abroad. Commissions paid to agents have sometimes been used to pay bribes to government officials on behalf of a company. Intermediaries and/or agents are often difficult to identify.

Mitigating Measures - If a financial institution is able to identify a private banking prospect or client as an intermediary and/or agent particularly in industries and/or sectors identified as posing increased corruption risk, it may determine that enhanced due diligence would be appropriate because, for example, the services (private banking), industry, country and/or transactional risk indicators are present which could increase the risks posed for the financial institution in dealing with the customer. Under these circumstances, the financial institution might consider one or more of the following as part of that enhanced due diligence exercise, for example whether the customer:

[13] Mitigating Measures: when PEPs are private banking clients, they should be subjected to greater scrutiny. See the Wolfsberg AML Principles on Private Banking and also the FAQs on PEPs on http://www.wolfsberg-principles.com/.

- has a family member in a government position, especially if the family member works in a procurement or decision-making position or is a high-ranking official in the department with which the intermediary is known to have dealings and that is the target of the intermediary's efforts
- has failed upon request (or has been suspiciously reluctant) to disclose owners, partners or principals; uses shell or holding companies or equivalent structures that obscure ownership without credible explanation
- has little or no expertise in the industry or the country in connection with which he acts as an intermediary
- anticipates substantial commission payments as an intermediary, either in absolute terms or as a percentage of the main contract sum, which cannot plausibly be verified vis-à-vis the role undertaken
- is retained by a company whose reputation in relation to the payments of such commissions is questionable by reference to prior convictions or governmental actions or that is reputed otherwise to engage in improper payments to governmental organisations.

Red Flags - Substantial cash or wire transfers into or from an account of a customer identified as an agent or intermediary where such activity is not consistent with legitimate or expected activity. Particularly substantial activity over a relatively short time period and/or the improper use of corporate vehicles to obscure ownership and/or the involvement of industries and/or countries posing increased corruption risk may also raise suspicions.

3.3 Correspondents – Correspondent customers potentially represent higher risks because the bank typically has no direct relationship with the customers of the correspondent bank. The bank is therefore unable as a matter of course to verify the identity of these underlying customers or understand the nature of the business and transactions (e.g. wire transfers, clearing cheques) it processes on their behalf.[14]

3.4 Industry Risk – Certain business sectors and industries have historically been identified with high perceived levels of corruption, financial institutions therefore need to assess, based on their own criteria, whether the activity of a customer in a particular industry poses a higher risk of corruption.

[14] See the Wolfsberg AML Principles for Correspondent Banking and also the Wolfsberg FAQs on Correspondent Banking on http://www.wolfsberg-principles.com/.