



Banco Santander
Bank of America
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
JPMorgan Chase
MUFG Bank
Société Générale
Standard Chartered Bank
UBS

the Wolfsberg Group

Wolfsberg Anti-Bribery and Corruption Compliance Programme Guidance

Introduction

This publication from the Wolfsberg Group (the Group) is designed to provide guidance to the financial services industry on how to develop, implement, and maintain an effective Anti-Bribery & Corruption (ABC) Compliance Programme, and should be read in conjunction with applicable legislation, regulation, and guidance issued by authorities in the jurisdictions in which a financial institution (FI) conducts business. The overall objective of the Guidance is to promote a culture of ethical business practices and compliance with ABC legal and regulatory requirements. This Guidance replaces the 2017 Wolfsberg ABC Compliance Programme Guidance, which has been retired.¹

The terms set out in this publication are used as generic terms that are known across the industry, and there is no expectation for FIs to adopt this specific terminology in their frameworks.

Definition of Corruption and Bribery²

Corruption,³ considered in the context of this Guidance, is the abuse of entrusted power for improper personal advantage. Bribery is a form of corruption and is commonly described as involving the offer, promise, giving, request, receipt, acceptance, or transfer of anything of value, either directly or

¹ The Wolfsberg Group has considered input to this paper from the UK Finance ABC Panel, the Basel Institute on Governance, and other initiatives including the World Economic Forum Partnership Against Corruption Initiative.

² While the aim is to focus on areas of risk that are of relevance to global FIs, adherence to this Guidance is not a substitute for legal advice. FIs should therefore seek the assistance of their own legal advisers for advice relevant to their businesses.

³ The following are additional sources on definitions of corruption, commonly used and which may be of use to readers:

- Corruption is “the abuse of trusted power for private gain” – [Transparency International](#)
- Corruption is “the abuse of public office for private gain” – [World Bank Group](#)

indirectly, to or by an individual, to induce, influence, or reward the performance of a function or an activity with improper intent, in a commercial or public office setting.

Risk-Based Approach

FIs should use a Risk-Based Approach (RBA) for the adequate development and implementation of programmes to prevent, detect, and report acts of Bribery and Corruption. In order to achieve that goal, FIs should periodically assess their business model including the locations in which they do business, their customer base, products and services, and the means by which they obtain and retain business such as through the use of Intermediaries (refer to section 5.1) and engagement with other third parties. Periodic assessments will enable FIs to identify inherent risks and adopt policies, procedures, and controls that are proportionate to the identified risks.

As highlighted in this Guidance, Bribery and Corruption risks generally are greater for FIs when pursuing business opportunities from, or providing benefits to, government or wholesale customer entities rather than customers in their individual capacity (e.g. a private wealth customer).

Overview of the Elements of an ABC Compliance Programme

While no ABC Compliance Programme (Programme) can prevent or protect against Bribery and Corruption risks completely, and there is no one-size-fits-all solution, this Guidance can help all FIs mitigate Bribery and Corruption risks across the following areas⁴:

- **Firm-wide Policy:** to capture key elements of a Programme, be applicable at a firm-wide level, set a no-tolerance appetite for Bribery and Corruption and prohibit facilitation payments ([Section 1](#)).
- **Governance, Roles and Responsibility:** the FI's Programme should be overseen by senior management, administered by an individual with sufficient authority, expertise, and resources, with access to the Board or other governing authority ([Section 2](#)).
- **Risk Assessment:** each FI should periodically assess the nature and extent of the Bribery and Corruption risks to which it is exposed, and the effectiveness of controls designed to mitigate those risks ([Section 3](#)).
- **Establishment of a Control Environment:** risk-based controls should be aligned to the firm-wide Policy and be designed to mitigate Bribery and Corruption risks associated with:
 - o **Anything of Value:** giving (including promising, offering, or authorising) or receiving anything of value, including gifts and hospitality, employment, work experience (paid or unpaid), donations and charitable contributions, corporate sponsorships, and political contributions ([Section 4](#)).
 - o **Third-Party Providers:** engagement of third parties, including Intermediaries, can create varying degrees of Bribery and Corruption legal, regulatory, and reputational risk ([Section 5](#)).
 - o **Customer-Related Transaction Risks:** certain customers, counterparties, or types of customer business activities may subject the FI to additional legal or reputational risks that should be considered and managed under an appropriate governance structure ([Section 6](#)).

⁴ In addition to domestic laws, internationally active FIs must also consider the relevance of other extraterritorial ABC laws and regulations. Programmes may also wish to explore alignment opportunities with other risks or emerging risk areas; this can include aspects of Bribery and Corruption risk which are connected to Human Rights or Environmental, Social, Governance (ESG) concerns.

- o **Principal Investments and Controlled Fund Acquisitions, Investments, or Joint Ventures**, i.e. the FI or a controlled fund acting on its own behalf ([Section 7](#)).
- **Training and Awareness:** The Programme should be communicated through policies, procedures, and guidance, with risk-based training of relevant employees and, as appropriate, certain third parties ([Section 8](#)). This includes the development of a framework to identify, analyse, and share lessons learned from internal and external events that are of relevance to the FI, in a timely manner, as part of the continuous evaluation of the Programme's adequacy ([Section 8.1](#)).
- **Monitoring and Testing for Compliance with Controls:** The FI should have mechanisms to test compliance with policies and procedures and to identify third party or employee-related risk, where there is failure to act in a manner consistent with the FI's business principles, policies, or codes of conduct, and applicable laws or regulations. Non-compliance should be investigated, remediated, and control improvements implemented, as appropriate ([Section 9](#)).

The elements summarised above are set out more in detail in the rest of the document.

1. Firm-Wide Policy

1.1 Prohibition on Bribery and Corruption

An ABC Policy (Policy) should be applicable firm-wide, include a no tolerance appetite for Bribery and Corruption, and prohibit facilitation payments.⁵ It should be driven by the “tone from the top” from senior management and the governing authority (e.g. Board) and serve as a basis for all related ABC standards and procedures.⁶ The Policy, code of conduct/ethics statement, or related handbooks should reference all employees’ personal accountability to protect their employer, its reputation, and themselves from the risks arising from Bribery and Corruption and set out the potential consequences for non-compliance.

The Policy should apply and be easily accessible to all employees including customer-facing staff, business/first line units, and those employees whose roles have the potential for increased exposure to Bribery and Corruption risks, e.g. Corporate Affairs, Marketing, Sponsorships, Facilities, Business Development, Corporate Real Estate, Human Resources, and Procurement, particularly employees having close interactions with external vendors and service providers. Certain temporary staff, outsourced service providers, contractors, and other personnel, by virtue of their role, may also be in scope.

1.2 Books and Records

All employees share responsibility for accurately documenting the offer or provision of anything of value⁷ to customers, potential customers, Public Officials, and third parties, as well as payments to third parties. Any assessments, due diligence, or approvals mandated by other internal policies and procedures should also be recorded in a manner that is transparent for monitoring and assurance purposes. FIs should also maintain documentation for anything of value received from or offered to customers, potential customers, Public Officials, and third parties, in accordance with their internal policies and procedures, and where required by applicable law or regulation.

1.3 Public Officials and State-Owned Entities

Policies should identify the heightened risk of interaction with Public Officials and State-Owned Entities (SOEs), as defined by the FI, and provide a clear definition of these terms to assist employees in identifying the associated risks. Such definition may include the degree of state ownership, control, or influence of an entity that would cause the FI to treat employees of that entity as Public Officials.

Since most ABC laws define Public Officials broadly, FIs should therefore also consider defining Public Officials broadly, i.e. as individuals at any rank or level within the following types of organisations:

- Supranational, national, regional, local, or municipal institutions/governmental bodies
- State-owned or state-controlled companies. Though dependent on applicable law or an FI’s internal thresholds and risk appetite, an entity would generally be deemed state-owned or controlled whenever any government body/bodies present(s) at least one of the following attributes:
 - More than 50% ownership

⁵ FIs should also consider highlighting in their Policy that providing anything of value due to a genuine threat of harm to life, limb, or liberty likely will not violate ABC laws, and that such payments should be reported promptly and accurately recorded.

⁶ The FI’s commitment to ABC risk management should also be publicly communicated (e.g. as a demonstration of corporate responsibility).

⁷ Please refer to Section 4 for a definition of the term.

- Voting control
- Board control
- Other indicia of control (e.g. a controlling – or “golden” – share by the government).
- Central banks
- Sovereign wealth funds
- International organisations, development banks, and public health agencies (e.g. the United Nations, World Bank Group, or International Monetary Fund)
- Royal families
- Political parties (including party officials and candidates for any level of political office).

2. Governance, Roles, and Responsibilities

In order to achieve an effective governance structure, roles and responsibilities should be allocated as follows:

- **Employees:** All directors and employees are responsible to uphold and comply with the FI’s principles and requirements set forth in the firm-wide ABC Policy.
- **Lines of Business:** The FI’s business personnel should have primary responsibility for achieving and evidencing compliance with the Programme’s requirements.
- **Programme Lead:** The Programme should be led by a function within the FI with the requisite expertise and authority. This unit should be part of a control function such as Compliance, Legal, or Risk.
- **Senior Management:** A member of the FI’s senior management should have oversight responsibility for the Programme and the FI should allocate adequate resources to execute the Programme within the FI’s risk tolerance and appetite. Periodic Programme updates and material issue reporting should be reviewed by the FI’s governing authority (e.g. Board and/or senior committees) as appropriate.
- **Independent Review:** FIs should review and test their control framework to determine whether controls are working in practice. The adequacy of the Programme should therefore be evaluated by an independent function, such as audit, that is separate from the Programme Lead.

3. Risk Assessment

Risk assessments should evaluate both inherent (including emerging) risks and corresponding controls to reach a residual risk level. There are many elements to a risk assessment, and its methodology may give different weightings to risk factors relevant to the FI’s risk profile and risk appetite. The core assessment should include:

- Potential liability created by Intermediaries and other third-party providers
- Bribery and Corruption risks associated with the countries and industries in which the FI does business
- Transactions, including those that involve state-owned or state-controlled entities or Public Officials
- Activities of the FI’s branches and subsidiaries, including third party engagements
- Bribery and Corruption risks associated with gifts and business hospitality, hiring (including internships), charitable donations, sponsorships, and political contributions
- Changes in business activities that may materially increase the FI’s Bribery and Corruption risk
- Identification of employees in roles which expose them to higher Bribery and Corruption risk.

FIs should include consideration of emerging Bribery and Corruption risks as part of existing methodologies for assessing Bribery and Corruption risks on a periodic basis. An emerging Bribery and Corruption risk is a new or evolving risk that may, at the outset, be difficult to assess fully, but has a reasonably high potential to manifest into significant concerns, including financial loss, impact to customers or competitive position, reputational harm, or legal/regulatory action if not addressed proactively. Emerging Bribery and Corruption risks do not always have fully comprehensive controls in place or fully developed monitoring and reporting mechanisms, and thus may require more active management oversight.

FIs should revise their Programme to mitigate the residual risk identified by the risk assessment, as appropriate. Some areas of business may be more susceptible to acts of Bribery and Corruption and may therefore need more frequent or detailed review. The output of the assessment should be shared with senior management to ensure appropriate actions are taken to mitigate identified areas of concern.

In addition to the Bribery and Corruption risks addressed in this guidance, FIs face the risk of being used by a customer to process financial transactions involving improper payments (e.g. by taking deposits or transferring funds that are the proceeds of Bribery and Corruption). These risks may be addressed through the measures put in place to detect and prevent money laundering. For example, adequate customer due diligence procedures, including enhanced due diligence (EDD) for politically exposed persons (PEPs)⁸, support the mitigation of money laundering risk by customers.

3.1 Reporting, Investigation, and Remediation of Misconduct

Relevant data should be collected to inform senior management as to the effectiveness of the Programme. Reporting should address the following, including but not limited to:

- Status updates on Programme implementation and operation including key performance indicators/metrics
- Significant deviations from internal policies and procedures by employees or associated persons/third parties
- Engagements of third parties, including Intermediaries, and customers identified as presenting heightened Bribery and Corruption risks
- Relevant legal and regulatory developments or regulatory reporting or filings
- Updates on any internal reviews of the Programme (e.g. audits, and compliance testing).

The FI's governing authority should receive periodic updates as to the effectiveness of the Programme and any material matters requiring the governing authority's attention.

The process to trigger an internal investigation into alleged Bribery and Corruption should include a "hotline" or other reporting mechanisms that are available to all employees and external parties. The process should allow for anonymous reporting, where legally permissible, accessible using a variety of media including email, telephone, and social media, and accommodate all relevant languages. Further, each FI should prohibit retaliation against employees who make good faith reports of potential misconduct.

FIs should have appropriate guidance in place for persons who are responsible for investigating allegations of misconduct. The guidance should require appropriate confidentiality throughout the

⁸ See [Wolfsberg Guidance on Politically Exposed Persons \(PEPs\)](#).

process (i.e. a need-to-know-basis) and compliance with applicable laws or regulations. In some situations, it may be advisable to retain outside counsel or accounting resources to assist in conducting the investigation.

Investigations into alleged Bribery and Corruption should include timely root cause analysis to remediate any control weaknesses and ensure continuous improvement in the Programme and alignment to, and integration with, policies, procedures, and processes for the purposes of compliance with the FI's external reporting obligations.

The status of material internal investigations into alleged Bribery and Corruption should also be reported to senior management in coordination with the FI's legal department, as appropriate.⁹

Appropriate disciplinary measures should also be taken against employees when an investigation confirms a violation of ABC laws or Policy.

4. Anything of Value

Bribery and Corruption risks are not limited to cash payments and may arise from an offer or transfer of anything of value.¹⁰ Accordingly, a Programme should include risk-based controls to mitigate risks associated with the following activities:

4.1 Gifts and Business Hospitality

FIs provide gifts and business hospitality to a wide range of stakeholders including customers, prospective customers, shareholders, employees, third parties such as speakers and vendors, and where laws permit, to Public Officials. Such activity is generally acceptable when it is incidental to facilitating business engagements, is undertaken to establish and maintain cordial business relations, or promotes the FI's products or services. Gifts and business hospitality should not, however, be given or received to influence (or create the appearance of influencing) the recipient in an improper manner.

Business hospitality should be construed broadly to include meals, entertainment, transportation, lodging, training, and invitations to events and conferences. If no representative of the FI providing the business hospitality is present (e.g. if an FI merely offers tickets to a concert or sporting event), the business hospitality should be treated as a gift, which may be subject to different (usually lower) monetary limits under laws prohibiting giving beyond prescribed thresholds.

FIs should have detailed policies and procedures governing the provision and receipt of gifts and business hospitality. The presence of one or more of the following risk factors can affect the appropriateness of a gift or business hospitality:

- The customer/third party is a Public Official
- The value is lavish or excessive for the specific event or in aggregate
- Family members or other guests of primary business contact are invited
- Gifts and business hospitality are in close proximity to the award of new business opportunities or recent business opportunities
- There is no clear commercial rationale or business nexus

⁹ External reporting requirements should be incorporated by the FI into its Programme's reporting processes.

¹⁰ The FI should consider ensuring that the provision or receipt of anything of value does not contravene the FI's commitments towards health and safety, human rights, and diversity and inclusion. For example, the elimination of offensive, discriminatory, or sexually explicit content in the FI's Policies, codes of conduct, employee manuals, training materials, etc.

- The gift creates an actual or apparent conflict of interest for the recipient, which could reasonably be expected to compromise the recipient’s judgment
- Supporting documentation is missing or incomplete
- Cash or cash equivalents are used (unless part of a local custom or tradition)
- The activity is indecent, offensive, discriminatory, or sexually explicit
- The event includes travel itineraries with unnecessary accommodation, flights, or side trips to holiday spots
- The gift is being used to facilitate the provision a government service, such as a permit or license
- The gifts and business hospitality are funded (in whole or part) by the employee paying out of their own pocket
- Employees split expenses into multiple small claims to circumvent the FI’s threshold limits
- Required prior approval is not logged and/or obtained
- The activity is illegal, or non-compliant with the giver’s or recipient’s local laws and regulations.

Procedures addressing gifts and business hospitality should consider each of these risk factors and may include a risk-based combination of monetary thresholds for pre-approval (by business management and/or Legal/Compliance), appropriate expense monitoring scenarios that may aggregate individual expenses over time, and applicable registration, expense approvals, and record keeping requirements. In most instances, escalating levels of approvals should be required as the risk from the provision/receipt of gifts and business hospitality increases. FIs should design risk-based controls that dedicate a proportionate degree of attention and resources to gifts and business hospitality posing less Bribery and Corruption risk compared to higher-risk activities or arrangements (e.g. the use of Intermediaries to obtain business).

FIs should also consider having provisions in policies and procedures that address:

- Cash gifts, cash equivalents like vouchers, gift cards and certificates, red envelopes¹¹, or payments (which should be prohibited to the extent feasible)
- Speakers’ fees and benefits, particularly if the speaker is a Public Official
- Expenses expected by a recipient to be reimbursed (e.g. travel and entertainment related to a securities offering)
- Employee receipt of gifts in the form of customer bequeathed requests or inheritances
- Where the instance relates to virtual/remote business hospitality, the FI should ensure evidence of the virtual meeting is maintained to avoid any doubt that the business hospitality is a gift.

4.2 Employment and Work Experience

Offers of employment or other paid or unpaid work experience (e.g. internships) 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 may violate applicable ABC laws. Accordingly, in collaboration with

¹¹ ‘Red envelopes’ are monetary gifts given during holidays or special occasions.

Human Resources (HR), a Programme should include risk-based processes covering hiring, particularly for candidates referred by a Public Official or by an employee of a customer or potential customer.

To prevent offers of employment or other work experience from being used improperly, FIs should consider the following:

- A consistent recruitment process
- Merit-based hiring procedures designed to ensure that candidates are qualified/eligible and do not receive special treatment based upon relationships with a Public Official, an employee of a customer, or potential customer. These procedures should be communicated to all appropriate employees.
- Heightened scrutiny (including additional approvals) for candidates referred by a Public Official or an employee of a customer or potential customer, particularly if the FI is, or soon will be, engaged with the employer of the referring person on business opportunities or legal/regulatory matters
- Monitoring or testing procedures (e.g. review of communications regarding referred candidates described above)
- The effectiveness of governance and supervisory control of hiring programmes
- Training for hiring managers and HR employees.

Such activities may be administered by the Programme, and/or other control partners, particularly HR, which should be well positioned to support Bribery and Corruption risk management in this area.

4.3 Donations and Charitable Contributions

While FIs frequently provide charitable support to communities, such charitable activity must not be used as a disguise for Bribery and Corruption. FIs should implement controls that address the risk of illicit use of charitable giving, such as when a charity is illegitimate and merely a vehicle for transferring a bribe, or when charitable giving is made to a legitimate charity, but for the purpose of influencing a supporter or director of that charity improperly.

Charitable giving takes many forms including: FIs providing philanthropic global donations from a central fund or through business-owned budgets; FIs providing specific contributions to local charitable dinners or sporting events; employees undertaking fundraising which includes only internal employees or extends to customers/vendors (e.g. fundraising initiatives in branches for local disaster relief); or FIs providing match funding initiatives or support collaborative charitable giving in association with external partners.

FIs should have processes that identify various types of charitable giving and address the risks in a reasonable and risk-based manner. Controls can include:

- Restrictions/limitations on giving
- Identification of high-risk activities (e.g. charitable giving at the request of a Public Official, vendor, customer, or potential customer; or where the facts and circumstances indicate that such an individual may derive an improper personal benefit from the FI's giving)
- Due diligence procedures regarding the recipient organisation (including its longevity, negative news, and legal status as a charity or non-profit)
- Risk-based Business, Compliance, or Legal pre-approval
- Documentation and recordkeeping requirements for charitable giving.

4.4 Corporate Sponsorships

Many FIs advertise themselves through sponsorships, the purpose of which is to promote the FI's brand. Where sponsorships might influence a supporter or director of the sponsored entity, or where sponsorships afford the FI opportunities to invite third parties to exclusive entertainment events, such activities may create the risk or appearance that they will be used to influence the award/retention of business or other advantage improperly.

Internal policies or procedures may specify criteria for the approval of, or limitations on, sponsorships. FIs should consider implementing reviews of sponsorships requested by a Public Official, customer, or potential customer, or where the facts and circumstances indicate that such an individual may derive an improper personal benefit from the FI's sponsorship.

4.5 Political Contributions

The laws on contributions to political candidates and parties vary widely around the world. Therefore, FIs must adopt standards that account for applicable laws and implement controls to mitigate the risks that political contributions may be made (or may be perceived to be made) to influence action, or obtain business or any other commercial advantage, improperly. Heightened scrutiny should be applied where the contribution is solicited, particularly by a Public Official.

5. Third-Party Providers

Relationships with third parties can create risks such as third-party providers making corrupt payments to others when acting for, or on behalf of, the FI; or providing personal benefits to the FI's employees in return for business mandates that may not be in the FI's best interest. Moreover, the extent to which the FI's liability may be triggered by the actions of a third-party provider can differ across jurisdictions and can be expansive in certain jurisdictions.¹² FIs should therefore adopt an RBA and consider relevant jurisdictional requirements when implementing a control structure to manage these risks effectively.

FIs may categorise, define, and consider their third-party relationships differently (e.g. suppliers, vendors, service providers, intermediaries, associated persons). Regardless of the terminology used, it is the *activity* performed by a third-party provider that will determine the level of Bribery and Corruption risk presented and therefore should guide an FI on how to manage and mitigate that risk effectively. In other words, the Bribery and Corruption risk presented by a third party depends on what role the third party is being engaged to undertake by the FI.

5.1 Intermediaries

Third parties who act for or on behalf of an FI to: 1) find, introduce, obtain, or maintain business or any other commercial advantage or 2) obtain government approvals or action (collectively herein, Intermediaries), pose a particularly heightened risk for Bribery and Corruption.

Intermediaries can create substantial legal liability and reputational risks to FIs and, as a result, should be appropriately managed throughout the lifecycle of the engagement. As repeatedly identified in

¹² For example, under the UK Bribery Act, a commercial organisation may in some circumstances be liable for the acts of an 'Associated Person', with 'Person' defined broadly as any person who performs services for or on behalf of the organisation, regardless of whether the FI has actual knowledge of corrupt conduct attributable to the Associated Persons.

enforcement actions, payments to Intermediaries have been used to make and conceal bribes to Public Officials or wholesale customers.

As a result of these inherent risks, FIs should: 1) take an expansive view of which third parties should be considered as Intermediaries and 2) risk assess potential engagements to inform the appropriate level of due diligence, approvals, and monitoring. The assessment should examine:

- Business necessity and scope of the engagement
- Fee structures/payment terms (requests for or making large “success fees”, “discretionary bonuses” or up-front payments are risk factors)
- The Intermediary’s qualifications for the services to be provided
- Likelihood of interactions with a Public Official on the FI’s behalf
- Connections to Public Officials (e.g. whether the Intermediary was recommended by a Public Official or whether its key beneficial owners, directors, or employees are current or former Public Officials or relatives/close associates of Public Officials)
- Industry corruption risk
- Country corruption risk
- For introducers or finders (of customers or new business), what type of prospect will be introduced (e.g. individual or entity) and whether any personal or professional relationships exist with the customer
- The proposed use of any subcontractor(s).

Depending on the assessment, subsequent due diligence may include media searches on the Intermediary and its principal officers using reputable sources for negative news related to Bribery and Corruption.¹³ Some higher-risk Intermediaries may warrant local language media searches or further investigation of publicly available records or materials:

- If the Intermediary is regulated, checks of regulators’ databases for censures, penalties, and verification of valid license status
- Reviews of the Intermediary’s internal policies and/or procedures for managing Bribery and Corruption risk, including any associated training activities.

Where red flags are identified (see [Appendix A](#) for examples of red flags), the FI should consider EDD (including the option to use external due diligence reports) and escalate as appropriate to ensure a fully informed decision is made as to whether to engage the Intermediary. Intermediaries should not be engaged unless key stakeholders are satisfied that the associated risks have been appropriately mitigated.

When the FI decides to engage an Intermediary, risk mitigation controls may include:

- Training of the FI’s employees responsible for managing the relationship, as well as the relevant individuals employed by the Intermediary to undertake the engagement, in the local language if warranted, and with periodic follow-up as necessary
- Contractual terms with ABC representations and warranties, which may vary depending on the level of Bribery and Corruption risk posed by the engagement. Provisions may include:
 - o A prohibition on all types of Bribery and Corruption

¹³ See [The Wolfsberg Group Frequently Asked Questions \(FAQs\) on Negative News Screening](#).

- o An acknowledgement that appropriate ABC policies and procedures are in place
- o A termination clause for acts of Bribery and Corruption, audit rights, and/or provisions requiring accurate books and records
- o A representation that the Intermediary is responsible for the oversight of its sub-contractors
- Communication to, and acknowledgement from, the Intermediary of the FI's ABC expectations
- Monitoring of fees and expenses, including potential audits if warranted
- Review of invoices and payments made to the Intermediary to ensure consistency with contract terms.

FIs should maintain a record of the Intermediaries they have engaged, including names, terms of engagement, due diligence conducted, services undertaken, and payments made.

5.2 Non-Intermediaries

Third parties providing goods and services directly to the FI are defined broadly as Non-Intermediaries. As opposed to Intermediaries, Non-Intermediaries generally interact only with employees of the FI itself in connection with their specific engagement, i.e. they are not asked to interact in a material way on the FI's behalf with other entities or individuals. Non-Intermediaries, in the absence of other risks, can therefore pose less risk from a Bribery and Corruption perspective compared to Intermediaries. Examples of Non-Intermediaries may include, but are not limited to:

- Property/maintenance providers (e.g. janitorial services, security)
- Information Technology service providers
- Payroll service providers, consultancy, and professional services firms (that are not engaged to provide Intermediary services)
- Suppliers of goods (e.g. office supplies).¹⁴

While Non-Intermediaries can generally present lower Bribery and Corruption risk than Intermediaries, FIs should nonetheless implement clear, risk-based guidance on their engagement, set forth expectations for their conduct, and undertake appropriate ongoing monitoring of these relationships. In many FIs, responsibility for the engagement of Non-Intermediaries sits with a dedicated supplier/vendor management team, which is responsible for managing various risks throughout the relationship lifecycle. ABC controls may therefore be integrated into the overall control framework. The development of ABC controls for Non-Intermediaries should consider existing controls that manage other risks, such as commercial, fraud, and reputational risks, which could be leveraged to manage and mitigate Bribery and Corruption risk.¹⁵

In adopting an appropriate control framework (such as deploying behavioral conduct training or offering whistleblower protections/recourse) and an RBA, FIs should be aware of the risk that a Non-Intermediary may offer or provide improper personal benefits to the FI's employees to retain or obtain new or additional business from the FI. As mitigation, there should be clear guidelines relating to the selection of third-party service providers, as well as risk-based restrictions on the receipt of anything of value from such third parties by employees involved in the selection process. On-boarding

¹⁴ In some cases, the nature of the relationship with a Non-Intermediary may change to that of an Intermediary (or vice versa); or a third-party may be acting in both an Intermediary and Non-Intermediary capacity. FIs should be aware of these potential scenarios and periodically reassess the relationship based on their third-party control framework.

¹⁵ FIs may wish to consider the applicability of the due diligence factors described for Intermediaries in Section 5.1. Depending on an FI's risk appetite, the factors may be given different weightings or considerations in forming the overall risk assessment, which will necessarily be broader than ABC.

procedures should also include Bribery and Corruption related questions or guidance to help an FI identify the circumstances under which a Non-Intermediary party may present increased Bribery and Corruption risks. Increased risks may require EDD, continuous monitoring such as negative media screening, oversight, and appropriate contractual protections, before commencing, or continuing to maintain, such engagements.

Once an FI has on-boarded a vendor or third-party service provider, it should continue to use an RBA to determine whether to institute forward-looking risk mitigation controls, such as risk-based monitoring of expense activity (including potential audits if warranted).

6. Customer-Related Transaction Risks

FIs may also encounter customer-related transaction risks such as:

- Wilful blindness in ignoring obvious red flags about the customer's activities
- Insider threat from employees becoming involved in a customer's illicit activity
- Bribery and Corruption as a predicate offence for money laundering
- Reputational risk (including ESG).

An FI's response may vary based on its organisational structure. For example, some FIs may assign and/or delegate responsibility for managing customer-related Bribery and Corruption risks to units other than the Programme Lead (section 2 of this Guidance) with the authority to manage such risks. It is advisable that FIs, as part of assessing and managing the above transaction risks, consider the holistic risk profile of the transaction.

6.1 Facilitation and/or Reputational Risk

FIs should consider where there may be increased facilitation and/or reputational risks arising from certain types of customers (e.g. governments, SOEs, or wholesale customers) and certain types of deal-related business activities (e.g. financing, such as underwriting, lending, and advisory transactions), as well as business activities with customers who present identified Bribery and Corruption risks.

FIs should consider risk-based due diligence of any known Intermediaries engaged by a customer or other third party in the transaction or related business activities.

For example, project finance initiatives to support public sector infrastructure/construction projects or the exploitation of natural resources may be vulnerable to the payment of bribes or other corrupt activities, particularly in high-risk jurisdictions. In some circumstances, although neither the FI nor its employees have been directly involved in the illicit activity, the FI may incur liability for systems and controls failures associated with indirectly facilitating or aiding the customer's illicit activity.

The FI should understand how the proceeds of equity or debt financing will be used in appropriate detail based on the risk, examining the business rationale for the purported use. Where risk is high, FIs may consider conducting further independent checks to confirm the validity of the use of proceeds of financing. In addition, measures implemented by FIs to ensure that wire payments contain complete and accurate information may also assist in the prevention and detection of the proceeds of Bribery and Corruption. Where the FI deems the transaction to carry elevated risk, consideration can be given to conducting checks on the customer's representatives and the end recipient of funds to ascertain if the transaction is at arm's length.

Applying an RBA, FIs should consider the potential Bribery and Corruption implications of proposed transaction-related activities and establish mitigating controls where appropriate.¹⁶ Factors to consider in the risk assessment and due diligence process include:

- Purpose and structure of any corporate vehicle set up to support transactions
- Nature and structure of transactions
- Customer's/counterparty's reputation concerning Bribery and Corruption or business ethics
- Relevant jurisdictions and industries involved
- Distribution of proceeds generated
- Involvement, payment, and reputation of known third parties (e.g. local agents, Intermediaries, representatives, and subcontractors)
- Nature of any government nexus.

How FIs deal with Bribery and Corruption red flags or negative news arising from these factors will depend on the FI's risk appetite, escalation/reporting processes, and its governance structures, but may include a review by the Programme Lead or another senior Compliance resource as appropriate.

Where increased Bribery and Corruption risks are identified, the FI's final decision-makers/approvers should be made aware, through relevant governance committees, such as transaction review committees, reputational risk committees, or credit approval committees, so that they have a holistic view of the risks associated with a particular deal-related activity, both at inception and through the lifecycle of the transaction.

7. Principal Investments & Controlled Fund Acquisitions, Investments, or Joint Ventures

Liability relating to Bribery and Corruption may arise after an FI or an FI-managed/controlled fund¹⁷ has merged, partnered with, or acquired a significant stake in another company/entity or joint venture (Target). Generally, a majority equity stake or control of Board of Directors is considered significant.¹⁸

To manage the risk associated with a significant investment in a Target, FIs should:

- Conduct risk-based ABC due diligence of such Targets, including principals and, in the case of joint ventures, the joint venture partner(s)
- Seek contractual protections related to Bribery and Corruption
- Undertake risk-based post-acquisition oversight of the Target's ABC-related controls.

Such risk management should apply not only to proprietary investments and acquisitions made by the FI, but also to significant equity investments made by asset management funds managed by the FI.

Risk-based due diligence should aim to identify past or current red flags for Bribery and Corruption over a reasonable period of time prior to the anticipated closing date of the transaction and assess the Target's ABC-related compliance controls in light of its risk profile. To the extent possible, such due diligence should be conducted prior to the investment. In some instances, it may not be possible to carry out some or, more rarely, any pre-acquisition due diligence, perhaps due to conflicting confidentiality obligations, commercial sensitivities, or other restrictions. In such cases, the FI should

¹⁶ This may include leveraging KYC and other AML-related processes, not necessarily as part of the FI's ABC Programme.

¹⁷ FI-controlled funds may include funds comprised of client assets managed by the FI or where the FI cedes day-to-day control of a fund's assets to a third-party manager.

¹⁸ The FI may also consider risks associated with investments (i) involving a substantial (but less than majority) equity stake that would give the FI influence over the entity's activities and/or (ii) considered significantly strategic for the FI.

conduct post-investment/acquisition due diligence as soon as practicable after closing the transaction and address any identified issues promptly.

The scope of the due diligence should be informed by the risk profile of the Target. Risk-based ABC due diligence of the Target may consider various factors, including:

- Whether the Target, principals, joint venture partners, or management are Public Officials or SOEs
- Any government nexus, including whether the Target's business involves significant touchpoints with Public Officials or SOEs
- The Target's, and its management's, owners', and/or significant shareholders' reputation for ethics and compliance issues
- Whether the Target has operations or employees (as opposed to a Special Purpose Vehicle that merely holds financial instruments, such as a collateralised debt obligation) or is managed by another party
- The extent to which the Target utilises Intermediaries and assessment of its overall third-party risk management programme
- The adequacy of the Target's ABC-related compliance policy and procedures, and review of reporting management information regarding the performance of compliance processes and controls, if any¹⁹
- Country risk of the geographies where the Target does business
- Industry risk of the Target and wider business operations.

Identified red flags should be considered and escalated to appropriate parties; for example, the FI's relevant investment committee or management personnel responsible for considering and managing risk appetite on behalf of the FI. Where due diligence identifies a material – actual or suspected – Bribery and Corruption issue, the FI should consider whether to engage legal or accounting professional services and/or engage directly with relevant law enforcement agencies and regulators regarding appropriate action to take.

In addition to conducting due diligence, FIs should seek ABC-focused contractual protections in acquisitions or investments, the scope of which may be negotiated on a case-by-case basis. Contractual provisions may include:

- A representation and warranty (and where appropriate a covenant) with respect to compliance with relevant ABC laws
- A contractual right to cause the Target to adopt or enhance appropriate ABC Policies and procedures and to provide regular reporting to the FI
- A contractual right to withdraw from the transaction upon discovery of a violation of ABC laws prior to closing the acquisition
- A contractual right to appoint new management where violations of ABC laws are detected, or where there is a failure to maintain an adequate control environment that leads to such a violation
- A contractual right to inspect or audit the books and records of the Target.

¹⁹ In instances where the Target is a newly formed entity, diligence should focus on whether the proposed managing partner has such Policies or whether the senior management team has experience and/or is willing to implement such Policies.

Post-investment, if the Target does not have ABC controls, FIs should take reasonable and timely steps to require (when holding a majority interest or control of the Board) or encourage (when holding a substantial minority interest or at least one Board seat) the Target to develop, implement, and maintain appropriate ABC controls and management of inherent Bribery and Corruption risk. The FI may also consider:

- Any necessary due diligence that the FI was unable to perform prior to the acquisition
- Prompt application or enhancement of ABC Policies and procedures at the newly acquired Target
- Training of relevant employees and Board members on applicable Policies and procedures, regulatory reporting requirements and regulator expectations, and the identification of red flags
- Compliance review of newly acquired Target
- Ongoing monitoring of Target's operations and transactions
- Prompt and thorough disposition of any Bribery and Corruption-related issues or control weaknesses.

8. Training and Awareness

ABC Policies, standards, and procedures should be effectively communicated, include a commitment statement from senior management, and apply to relevant officers, director, employees, and contingent workers at all levels of the FI. Specific ABC training should also be provided to senior management, members of governing authority (e.g. the Board), and appropriate employees such as those with heightened exposure to Bribery and Corruption risks as a part of their roles (e.g. customer/government facing, managers of Intermediaries, and relevant control functions which handle hiring, donations, sponsorships, and vendors). Training and/or communications should be provided/shared upon joining the FI and thereafter on a periodic basis, with the frequency informed by the Bribery and Corruption risk posed, and be extended to third parties identified as presenting heightened levels of risk to the FI (e.g. high-risk Intermediaries).

Substantively, training should include relevant definitions (e.g. Bribery and Corruption, Public Officials, Intermediaries, etc.), references to applicable internal policies, procedures, and/or laws and regulations, along with case studies, practical examples, and/or lessons learned which present potential scenarios that employees may encounter. The training should include information on when and how to seek advice and how to report any concerns or suspicions of Bribery and Corruption.

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. Retention of such records will facilitate tracking and reporting.

8.1 Lessons Learned and Continuous Improvement

FIs should establish a framework and requirements for the timely identification, analysis, reporting, tracking, and sharing of lessons learned from qualifying material adverse events (which could be internal and/or external), as defined by the FI. The purpose of sharing lessons learned is to improve awareness of Policy and Programme requirements, and strengthen existing processes and controls, thereby reducing potential future risk that could stem from the same root cause and enable continuous improvement across the FI.

An objective of continuous improvement is to ensure that the FI's Programme evolves appropriately, in line with internally- and externally-driven demands. FIs should review and, if necessary, enhance

their Programmes regularly. For example, the FI's Programme should evolve as its business lines change over time, responding to the environments in which it operates, the profiles of its customers, the laws that govern its actions, and the standards of the industry.

Examples of adverse events may include but are not limited to: 1) significant internal issues identified during audits, testing, or comparable reviews that may impact other businesses or geographical regions, or a significant loss; and 2) external events such as peer/industry enforcement actions or reported violations or non-conformance with applicable local, national, or cross-border ABC laws, rules, and regulations.

FIs should consider analysing identified adverse events to understand:

- How and when the event took place
- What root cause led to the event, including an assessment of any control failings
- How and when the event was escalated
- If the event is external, an assessment of its applicability to the FI's circumstances and control framework
- What the adverse financial and non-financial impact was and what are the remaining risk exposures
- What remediation actions are or were required and taken.

FIs should report the conclusions of their lessons learned analyses under existing escalation and reporting processes and governance structures, which should include dissemination to both business/first line and control functions, as appropriate.

9. Monitoring and Testing for Compliance with Controls

FIs should review compliance with ABC controls through ongoing monitoring and periodic testing. Risk-based monitoring or testing of employees' activities to detect instances of non-compliance with Policy and procedural requirements should be part of the overall ABC control framework (e.g. post-transaction monitoring of expense reimbursement, business hospitality, sponsorships, and corporate events).

APPENDIX A: EXAMPLES OF BRIBERY AND CORRUPTION RED FLAGS

The following is a non-exhaustive selection of red flags which may warrant EDD or review:

- Little to no relevant experience regarding the services to be provided
- No obvious added commercial value added by the person or entity of concern
- Use of consultants or vendors who serve no clear purpose, or a forced or strongly recommended use of a vendor who would not meet procurement standards
- Flawed background or reputation (for example, prior corruption or a negative reputation for integrity)
- Recent senior Public Official of the same government department or business responsible for the award of the contract or matter at issue, or who worked in a procurement or decision-making position
- Transaction or Intermediary suggested by a Public Official, particularly one connected to the business or matter at issue
- Close business, personal, or family relationship with a Public Official or third party who has discretionary authority over the business or transaction at issue
- Party to a transaction or contract makes unreasonable/unsupported objections to ABC due diligence or representations or warranties being included in the agreement
- Party does not reside or have a significant business presence in the country where the service is to be provided
- Use of a shell company or some other non-transparent corporate structure
- Use of nominees or proxies with no obvious commercial purpose
- Use of entities with names mirroring more reputable entities with no connections to those reputable entities
- Key contacts' use of non-official communication channels such as personal email, text messages, or communication apps
- Requests for payment of a commission or a significant portion thereof, before, or immediately upon award of the contract
- Requests for unusual contract terms such as deviation from progress payment models for construction contracts
- Requests for payment in cash, advance payments, payment to an individual or entity that is not 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
- Requests for payments that cannot plausibly be justified vis-à-vis the role undertaken
- Demand to adjust remuneration during the engagement, particularly in close proximity to the award of business
- Vague or unsupported business rationale and bookkeeping (e.g. no clear or disclosed purpose as to the proposed use of funds) on cash or requests for cash payments
- Deviation from standard procurement practice especially for public projects
- Unusual involvement of Public Officials in commercial matters
- Sudden unexplained resignations of key professionals (e.g. members of the Board, lawyers, or auditors).
- Recommendation(s) to rely on the customer's and or Intermediary's due diligence without written evidence of what the due diligence has encompassed, or the written results thereof
- High-value and or complex deals or transactions that bypass or exclude the involvement of Compliance in the review processes.