

# Group Financial Crime Compliance Policy

## Table of Contents

1.	Introduction .....	3
2.	Risk Appetite .....	3
3.	Roles and Responsibilities.....	5
4.	Risk-Based Approach Requirements.....	8
5.	Client Risk Assessment Methodology (C-RAM) .....	9
6.	Customer Due Diligence (CDD) Requirements.....	9
7.	Politically Exposed Persons Requirements .....	11
8.	Suspicious Activity/Transaction Reporting Requirements.....	12
9.	Sanctions and Terrorist Financing Requirements .....	13
10.	Anti-Bribery and Anti-Corruption Requirements (ABAC).....	15
11.	Law Enforcement and Regulatory Engagement .....	18
12.	FCC Training and Awareness Requirements .....	18
13.	FCC Outsourcing.....	18
14.	FCC Management Information Requirements.....	18
15.	Record Keeping Requirements .....	19
16.	Dispensations.....	19
17.	Non-Compliance .....	19
18.	Document Administration.....	19

## 1. Introduction

### 1.1. Purpose

The Bank ABC Group Financial Crime Compliance Policy (the “Policy”) and supporting Standards define the governance, roles and responsibilities, scope and high-level controls for Financial Crime Compliance (FCC) in Bank ABC and its Units.

This Policy forms part of the overall Bank ABC FCC Framework, which consists of this Policy and all supporting FCC Standards documented in Section 19. This Framework sets the key principles for FCC risk management within Bank ABC.

This Policy aims to:

- ensure a consistent approach to embedding Financial Crime Compliance with applicable statutory, regulatory and supervisory requirements, including industry codes with which the Group must by law comply with, or which it voluntarily adheres to (Regulatory Requirements);
- establish and maintain effective Financial Crime Compliance risk management and control systems, including monitoring and reporting;
- define the responsibilities of the Board of Directors, Senior Management, Group FCC Function and all Employees in relation to Financial Crime Compliance; and
- ensure there is consistent Group-wide application and oversight of the Bank ABC Financial Crime Compliance Framework.

### 1.2. Scope

This Policy applies to:

- all Bank ABC branches, subsidiaries and representative offices (collectively Bank ABC Units or Units). Bank ABC Units must also ensure that they are compliant with the Regulatory Requirements in the jurisdiction in which the Unit operates. If there is any conflict between local requirements and the requirements stipulated in this Policy, the particular Bank ABC Unit should apply the higher standard; and
- all permanent and fixed term contract staff employed directly by the Bank in addition to external consultants engaged directly by the Bank (Employees).

## 2. Risk Appetite

Bank ABC is committed to conducting its business operations in compliance with Regulatory Requirements and has no tolerance for regulatory breaches that are intentional or due to gross negligence. Bank ABC has accordingly established the following risk appetite statements in support of its commitment:

## 2.1. Customers and/or Transactions Risk Appetite

Bank ABC has no appetite for:

- the establishment of a relationship with a Customer prior to the completion of CDD, unless all accounts are blocked to ensure that no disbursement of funds take place, until such time that the account becomes CDD compliant; or
- the establishment of Non-Face-to-Face<sup>1</sup> business relationships; or
- the establishment or maintaining of:
  - anonymous, pseudonym, nominee (unless identified) or numbered accounts;
  - Nested Accounts/Payable Through Accounts (allowing a financial institution to gain access to another countries financial system by operating through a correspondent account belonging to Bank ABC);
  - Cross border Downstream Clearing on behalf of another Bank;
  - a business relationship with a Shell Bank, Unlicensed Bank or banks which are not regulated by a supervisory body;
  - a business relationship with Gaming/Gambling Companies;
  - a business relationship with the Adult Entertainment Industry or Alcohol Industry<sup>2</sup>;
  - a business relationship with unregulated Money Service Businesses;
  - a business relationship with Virtual/Digital Currency Companies;
  - accepting any cross-border cash delivered by couriers;
  - introduced business from Professional Intermediaries;
- the onboarding through a digital portal for<sup>3</sup>:
  - natural persons, residing outside the Unit's country (or GCC for Bahrain<sup>4</sup>); or
  - foreign PEPs;
- non-resident customers residing in jurisdictions on the "FATF High-Risk Jurisdictions Subject to a Call for Action List".

## 2.2. Sanctions

Bank ABC has no appetite for:

- establishing or maintaining a customer relationship with an entity or individual designated by Applicable Sanction Authorities (ASA), in accordance with the regulatory requirement of

---

<sup>1</sup> Non-Face-to-Face for Bank ABC refers to cases wherein there is no engagement with Customer either via in-person meeting or technology to establish the authenticity and liveness of the customer.

<sup>2</sup> As defined in the Group FC Customer Due Diligence Standard

<sup>3</sup> Any exceptions must be approved by the Central Bank of Bahrain.

<sup>4</sup> Such restrictions do not apply for nationals of the Unit's country, even if they are currently located outside the Home country

the ASA;

- conducting business activity involving countries which are subject to comprehensive sanctions or for which the Bank has no appetite as determined by Group Head of Financial Crime Compliance (GHFCC) and approved by the Group Compliance Oversight Committee (Prohibited Countries);
- establishing or maintaining relationships with Customers which are located or registered in Prohibited Countries or owned/controlled by persons located, or registered in Prohibited Countries;
- knowingly entering into any transaction or business arrangement or providing banking services that have the purpose of permitting any government or persons to evade or circumvent the regulatory requirements issued by ASA;
- omitting, deleting or altering (payment stripping) in any way information in payment messages for the purpose of avoiding detection of such information by the Bank ABC screening systems or by other financial institutions processing such payments.

### 2.3. **Terrorist Financing**

Bank ABC Units are prohibited from establishing or maintaining a Customer relationship or entering into a transaction where the Unit suspects the Customer or transaction to be directly or indirectly related to the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations (Terrorist Financing). This includes activities related to proliferation of weapons of mass destruction.

### 2.4. **Anti-Bribery and Anti-Corruption**

Bank ABC has zero-tolerance to bribery and corruption. This includes giving or receiving gifts, entertainment, facilitation payments or anything else of value if it is intended to obtain, or appears to give, an improper business advantage.

## 3. **Roles and Responsibilities**

### 3.1. **Board of Directors**

The Board of Directors (the “Board”) refers to the Boards at Group and Unit level. With the assistance of the Board Compliance Committee, the Board is responsible for:

- a) promoting a strong and sustainable ethical culture across the Bank;
- b) overseeing the management of the Bank’s Financial Crime Compliance risk;
- c) ensuring that an independent Group FCC Function is established and adequately resourced commensurate with the scale and complexity of the Bank’s operations;
- d) at least annually, assessing the adequacy of the Bank’s FC systems and controls and the extent to which the Bank is managing its FCC risk effectively;
- e) ensuring that the agenda of the meetings of the Board Compliance Committee include

- Financial Crime Compliance as a topic at least every quarter; and
- f) ensuring an appropriate Financial Crime Compliance risk appetite is established and implemented.

The Group Board approves this Policy and reviews it annually. The Group Board delegates the approval of supporting Standards to the Group Compliance Oversight Committee.

The above responsibilities apply Group-wide for the Group Board and at the Unit level for the subsidiary Boards.

### 3.2. **Board Compliance Committee**

The Board Compliance Committee (BCC) refers to the Group Board Compliance Committee and Unit Board Audit Committees (or equivalent).

The BCC is responsible for assisting their respective Boards in discharging their compliance, governance, and oversight responsibilities.

### 3.3. **Senior Management**

Senior Management is responsible for the effective management of the Bank's compliance risk. It is responsible for establishing the operating framework and the processes to support a permanent and effective Group FCC Function. It is also responsible for establishing and communicating a written Group Compliance Policy through all levels of the Bank and for ensuring that it is adhered to in practice. Collectively the "Senior Management Compliance Responsibilities".

For the purpose of this Policy "Senior Management" is defined as members of the Group Compliance Oversight Committee and the Unit Compliance and Financial Crime Committees that are constituted to effectively discharge the Senior Management Compliance Responsibilities.

### 3.4. **Group Compliance Oversight Committee**

The Group Compliance Oversight Committee ("GCOC"), with the assistance of the Group Financial Crime Compliance Function is responsible for ensuring that the Senior Management Compliance Responsibilities are properly discharged by the Bank.

The GCOC reports to the Group Board Compliance Committee.

### 3.5. **Unit Compliance and Financial Crime Committee**

The Unit Compliance and Financial Crime Committee ("CFCC"), with the assistance of the Unit Compliance Function is responsible for ensuring that the Senior Management Compliance Responsibilities are properly discharged by the Unit.

The CFCC reports to the respective BCC and a summary of key decisions and risks raised are tabled

at the GCOC.

Where the Unit does not have a BCC and in the case of the Bahrain CFCC, the CFCC reports directly to the GCOC.

### 3.6. **Group Internal Audit**

Group Internal Audit (GIA), in its capacity as the third line of defence, provides independent assurance on the adequacy and effectiveness of FCC risk management frameworks.

GIA assists Senior Management in accomplishing their FCC oversight objectives by bringing a systematic, disciplined, risk-based approach to the evaluation of Financial Crime Compliance risk management, controls, and governance processes.

This may include but is not limited to undertaking Group-wide audits pertaining to FCC control requirements, achieved through the completion of an annual risk-based audit plan, which is compiled in consultation with Group FCC.

GIA has the authority to independently determine the scope and extent of work to be performed across the Bank, as mandated by the Board Audit Committee.

### 3.7. **Group Compliance Oversight Testing**

Group Compliance Oversight Testing (GCOT) activities are performed across the Group to assess, on a risk-based approach in accordance with their annual plan, whether the Bank is complying with relevant FCC regulatory requirements and this Policy, including related GFCC Standards or Guidance Notes issued.

### 3.8. **Unit Money Laundering Reporting Officers (MLRO) and Deputy MLROs (DMLRO)**

Each ABC Unit is required to appoint an MLRO to take responsibility for ensuring the implementation and compliance with the Bank ABC FCC Framework.

Bank ABC Units are also required to appoint a DMLRO to support and assist the MLRO in the discharge of their responsibilities.

The DMLRO is responsible for deputising for the MLRO in their absence. Specific tasks may be delegated to the DMLRO at the discretion of the MLRO who retains overall responsibility.

The appointment of the Unit MLRO and DMLRO are subject to approval by the Group Head of Financial Crime Compliance (GHFCC) and local management and the local Regulatory Body, where required.

### 3.9. **Group Head of Financial Crime Compliance**

The GHFCC reports to the Group Head of Compliance and is accountable for oversight of the

Bank's FC systems and controls supporting the Board of Directors, BCC and GCOC in promoting a positive FCC culture throughout the Bank ABC Group. This includes the development and maintenance of an adequate and effective corporate governance structure as it relates to FCC, as well as, for the co-ordination of the overall FCC framework.

The GHFCC is responsible for oversight of the Bank ABC's FCC systems and controls including:

- Developing and maintaining Bank ABC's FCC policies and standards on an ongoing basis in-line with applicable legal and regulatory requirements and industry best practice.
- Ensuring that Unit FCC policies and standards are in-line with Group standards and where there are deviations that they are appropriately approved.
- Providing training and guidance to Unit MLROs, Senior Management and the Board on Group FCC matters generally and the Bank's FCC policies and procedures including ensuring that they are aware of their responsibilities under these policies and procedures.
- Approving appointments of Unit MLROs.
- Acting as the Bank's external contact and reporting officer for FCC related matters, with the regulatory authority in Bahrain (and other jurisdictions as required).
- Based on a review of the periodic reports on FCC submitted by the Unit MLROs, perform an overall assessment of the effectiveness of the Bank ABC's FCC Policies and Procedures, adherence to them, and make recommendations to Senior Management where improvements are required including enhancements to FCC related systems and technologies.
- Reporting to the GCOC on critical FCC issues across Bank ABC which require the attention of the Senior Management.
- Consulting with the business stakeholders and conducting training needs analysis for FCC related matters. Establishing an annual Bank ABC FCC training plan.

### 3.10. **Business Units**

It is the responsibility of the Business Unit owning the customer relationship to ensure compliance with the requirements of this Policy and related Group FCC Standards.

### 3.11. **Employee Responsibilities**

All employees are required to comply with both the letter and spirit of this Policy, supporting Standards and Procedures in addition to the Regulatory Requirements. Employees are also responsible for ensuring effective management of FCC risks as applicable to their role.

## 4. **Risk-Based Approach Requirements**

### 4.1. **Enterprise-Wide Risk Assessment**

Bank ABC and its Units must take the following steps to identify and assess their FCC risks.

The FCC Risk Assessment includes several steps in assessing the most effective and proportionate



way to manage and mitigate the FCC risks faced by Bank ABC and its Units. These steps must include:

- identifying the inherent FCC risks that are relevant to Bank ABC Units.
- assessing the inherent FCC risks presented by Bank ABC Units:
  - customers;
  - products;
  - delivery channels; and
  - geographical areas of operation.
- assessing the FCC control environment to determine the residual risk;
- developing and implementing controls to manage and mitigate any residual risk falling outside the risk appetite of Bank ABC; and
- recording the results of the risk assessment and any additional controls or control enhancements that have been identified and put in place to improve the effective operation of existing controls.

The annual FCC Risk Assessment results must be captured and:

- reported to Unit Senior Management and relevant committees including the local CFCC, to agree the implementation of risk management controls; and
- reported to the GHFCC for consolidation and tabling to the GCOC and the BCC.

The FCC Risk Assessment Methodology shall be reviewed annually, updated where required and submitted to the GCOC for approval.

Bank ABC Units must ensure that the residual FCC risks of new products are determined, and the results are included in their FCC Risk Assessment.

## **5. Client Risk Assessment Methodology (C-RAM)**

The C-RAM defines the metrics that underpin the Model used to calculate the Customer's Financial Crime Risk Category (FCRC). The Model evaluates various customer attributes within defined risk factors to inform a composite risk rating for each customer dependent on the perceived FC risk identified.

ABC Units must establish and maintain adequate procedures to ensure that a Customer's FCRC is determined in accordance with the Customer Risk Assessment Methodology (C-RAM).

## **6. Customer Due Diligence (CDD) Requirements**

A Customer is defined as an individual or entity that has been provided with an account, product or service by the Bank or for whom a limit has been established (including market counterparties).

The CDD process enables Bank ABC to develop a risk profile for all customers. This enables the

Bank to effectively manage the FC risk associated with its customers and meet its regulatory obligations.

ABC Units must apply the required level of due diligence based on the FCRC assigned to the Customer; and ensure that CDD is performed in accordance to the Group FC CDD Standard at onboarding and prior to account opening or undertaking any transaction or providing any service to the Customer.

In the instances where a Customer is introduced between two Units of Bank ABC, the onboarding Unit must ensure that the documents received comply with the requirements set by local regulators and the Group FC CDD Standards. Should any additional documentation be required it is the obligation of the requesting ABC Unit to ensure that these documents are obtained.

### 6.1. **Simplified Due Diligence**

Reduced due diligence requirements may be applied by ABC Units in the instances where local regulatory requirements allow for the implementation of Simplified Customer Due Diligence (SiDD).

The following minimum requirements must be adhered to before considering the implementation of SiDD:

- it will not apply to a Customer risk rated as high risk in accordance with the C-RAM model; and
- all qualifying regulatory criteria have been met; and
- the SiDD requirements set out in the Group FC CDD Standard must be followed.

### 6.2. **Standard Due Diligence**

Standard due diligence must be applied to all customers rated as low and medium risk, except where SiDD is applied as documented in the Group FC CDD Standard.

### 6.3. **Enhanced Due Diligence for Higher Risk Relationships (“EDD”)**

Enhanced Due Diligence (EDD) must be applied to Customers risk rated as “High Risk” or “Restricted”.

Bank ABC Units must establish and maintain adequate procedures to ensure that required EDD measures are applied in accordance with the Group FC CDD Standards.

Approval levels for Customer on-boarding should be incremental with higher levels of approval required for Customers that are assessed as posing a higher financial crime risk. All Customers must be approved in accordance with the incremental levels agreed by the GHFCC and the Group Head of Wholesale Banking or Retail Banking Head prior to account opening or undertaking any transaction or providing any service to the Customer.

#### 6.4. Ongoing Due Diligence

ABC Units must establish and maintain adequate procedures to ensure all relevant CDD information and supporting documentation is kept up to date throughout the life of the Customer relationship where changes are identified during periodic or event driven reviews.

When a periodic or event driven review is performed, Bank ABC Units must use a risk-based approach to scrutinize the transactions undertaken since the last review to ensure that the activity is consistent with the Unit's knowledge of the Customer, their FCRC and their source of funds.

#### 6.5. Periodic Reviews and Trigger Events (Event Driven Reviews)

ABC Units must perform periodic reviews on their Customers' CDD information within the time frames set out in the Group FC CDD Standard. Frequency of reviews are defined on a risk-based approach.

Event driven reviews must be performed when a trigger event occurs, as defined in the Group FC CDD Standards.

If an event driven review is triggered due to the identification of relevant adverse media or the filing of a material SAR, Bank ABC Unit must assess increasing the risk rating of the Customer to Restricted, while documenting the rationale. Should the ABC Unit want to subsequently reduce the risk rating to the original risk rating approval has to be obtained from the Unit MLRO.

### 7. Politically Exposed Persons Requirements

#### 7.1. PEP Due Diligence

A Politically Exposed Person (PEP) is defined as an individual, including PEP by Association (being their family members or close associates) who is or has been entrusted with a Prominent Public Function including, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations or senior political party officials or such other senior officials, defined as PEP, per the Bank ABC Unit's applicable rules.

Bank ABC Units must establish and maintain adequate procedures to screen and identify PEPs during the Customer On-boarding process and during the Ongoing Due Diligence Process.

ABC Units must ensure that all PEP relationships are risk rated as "High" as a minimum, and "Restricted" if there is relevant adverse media.

Due diligence of PEPs must be conducted in accordance with the requirements set out in the Group FC CDD Standard.

Legal Entities must be classified PEP Entities and "Restricted" where the UBO is a PEP or multiple PEPs that directly or indirectly own 50% or more in the entity; or exercise effective control over

the entity.

Where an individual PEP has been identified, such information must be recorded in a PEP Register and the PEP Register should be kept up to date with the relevant information obtained during Ongoing Due Diligence or Periodic reviews.

For PEP Entities, the name of the legal entity must be recorded in the PEP Register together with the names of any associated UBOs that are PEPs.

## 7.2. PEP Declassification

In line with the guidance issued by the FATF and Wolfsberg in relation to the risk-based approach, ABC Units may consider declassifying an individual as a PEP if:

- the individual has been retired from all prominent public functions/positions for a minimum of three (3) years; and
- Bank ABC Units have determined that the individual cannot exercise any significant informal influence over the position that the individual held as a PEP; and
- Bank ABC Units have determined that any current industry in which the individual operates or is employed, is not linked to the position that the individual held as PEP; and
- there is no material adverse FC or reputational risk information on the individual.

Where a PEP is deceased Units may consider declassifying the PEPs by Association (Family Members and/or Close Associates) if:

- a risk assessment has been completed; and
- the outcome confirms that these individuals do not exercise any significant informal influence over the position which was previously held by the PEP.

The declassification of a PEP must be signed-off by Bank ABC Unit's Head of Retail/Wholesale Banking, Unit MLRO and the GHFCC, whilst the declassification of a Family Member and/or Close Associate must be signed off by Bank ABC Unit's Head of Retail/Wholesale Banking and Unit MLRO.

## 8. Suspicious Activity/Transaction Reporting Requirements

All Units are required to monitor customer transactions and activity to identify transactions or behavior that appear abnormal when analyzed against the customer's transaction history, income and known lifestyle, business or anticipated behavior (Unusual Activity) and report suspicions of Financial Crime activity to Competent Authorities in their respective jurisdictions.

Employees must report all suspicions of Financial Crime by submitting an Unusual Activity Report (UAR) to their Unit MLRO.

Bank ABC Units must establish and maintain appropriate procedures and controls to enable the

identification and reporting of Suspicious Activity Reports (SARs) originating from UARs generated from automated transaction monitoring systems or raised by staff.

All UARs must be investigated and reviewed by the Unit MLRO (or delegate) who will decide if they should be:

- discounted as not being suspicious; or
- reported to the competent authority, as a SAR where there is a suspicion of Financial Crime activity.

All UARs must be recorded as case files in the Bank's transaction monitoring system and/or a local format (Register) agreed with Group Head of FCC. The results of all investigations and narratives for discounting of UARs must be recorded within the system and/or Register.

Where external SARs are filed, a copy of the disclosure must be scanned and retained within the case file. The status of the case file must reflect that a SAR has been reported to local competent authorities.

The Unit MLRO must ensure that a SAR is reported within the prescribed regulatory timeframe to the relevant authority using the applicable local protocol.

Bank ABC Unit MLROs must retain a record of all SARs filed with competent authorities.

Bank ABC prohibits all Employees from informing a customer either directly or indirectly that the Bank is investigating or has filed a suspicious activity report involving them. Bank ABC Units must ensure that all Employees are aware of their obligations not to 'tip-off' the customer.

## 8.1. Transaction Monitoring Systems (TMS)

All ABC Units must deploy an automated system to help identify unusual transactions and activity and generate alerts based on source customer and transaction data against a set of scenarios and parameters appropriate to Bank ABC Units' risks. Automated monitoring may be supplemented by manual monitoring techniques.

Whilst GFCC is the owner of the TMS, the Unit MLROs remain responsible for ensuring that FCC risks are mitigated by requesting any additional detection scenarios required or expected by local regulators and for reviewing the effectiveness and efficiency of scenarios periodically to ensure that these remain appropriate to the Unit's risks.

## 9. Sanctions and Terrorist Financing Requirements

### 9.1. Applicable Sanctions Authorities

ABC Units must comply with the requirements of the sanctions programs issued by the following Applicable Sanctions Authorities (ASA):

- Central Bank of Bahrain;
- United Nations Security Council (“UNSC”);
- United States Office of Foreign Assets Control (“OFAC”);
- Her Majesty’s Treasury, United Kingdom (“HMT”);
- European Union (“EU”); and
- Any local Sanctions regulatory requirements that may be applicable to Bank ABC Units in the jurisdictions in which they are located.

## 9.2. Sanctions and Terrorist Financing Screening Requirements

Bank ABC must establish and maintain appropriate procedures, systems and controls to ensure screening against the lists issued by the ASA for:

- a) Customers and related parties prior to the establishment of a business relationship;
- b) All existing customers and their related parties;
- c) Cross-Border inward and outward transactions prior to completing such transactions;
- d) Employees prior to commencing employment;
- e) Suppliers and Non-Customer Relationships prior to entering into a contractual agreement or establishing a Non-Customer Relationships.

Where Bank ABC Unit is subject to a regulatory requirement to screen domestic transactions, or a defined set of domestic transactions, it must advise the GFCC.

On-going screening against the lists issued by the ASA must be performed:

- daily for the relationships defined in Section 9.2.1.b and 9.2.1.d; and
- annually for the relationships defined in Section 9.2.1.e.

Bank ABC Units must report to GFCC:

- all business relationships, transactions, activities with new and/or existing clients involving sanctioned person(s) or prohibited jurisdictions; and
- all dealings with Competent Authorities relating to Sanctions.

## 9.3. Sanctions and Terrorist Financing Screening Systems

All sanctions screening must be performed using automated screening systems which have been approved by the GCOC.

Manual (online) screening tools may be used as part of preliminary due diligence, investigation or any ad-hoc screening. Such tools must also be approved by the GCOC.

While GFCC is the owner of the Bank’s sanctions screening (Name and Transactions) solutions, the Unit MLROs remain responsible for ensuring that thresholds, screening parameters and sanction lists meet the requirements of local regulations and the expectations of local regulators.

#### 9.4. Cross Border Electronic Funds Transfer Content Requirements

Units must ensure that information accompanying all cross border electronic fund transfers always contains:

- the name of the originator;
- the originator account number where such an account is used to process the transaction or any other unique transaction reference permitting traceability of the transaction;
- the originator's address, or national identity number, or customer identification number, or date and place of birth;
- the name of the beneficiary;
- the beneficiary address, including country of residence; and
- the beneficiary account number.

If individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the requirement under 9.4.1 in respect of originator information may be exempted, provided the originator's account number or unique transaction reference number are included, and the batch file contains the required and accurate originator information, and full beneficiary information or alternatively it is traceable.

### 10. Anti-Bribery and Anti-Corruption Requirements (ABAC)

#### 10.1. ABAC Risk Assessment and Controls

Bank ABC and all Units are required to have in place appropriate procedures aimed at identifying and mitigating the risks of Bribery and Corruption.

Bribery is defined as an offer, promise, giving, soliciting or receipt of financial or non-financial incentives (such as a promise of employment) to or from another person, directly or indirectly, immediately or in the future:

- to induce that person to perform improperly a relevant function or activity;
- to reward that person for the improper performance of such a function or activity; or
- knowing or believing that the acceptance of such incentive would itself constitute the improper performance of a relevant function or activity.

Corruption is defined as the abuse of public or private office for personal gain and can include graft, bribery, facilitation payments or other forms of improper business practice.

The aim of the ABAC requirements is to minimise the risk of making or receiving a bribe by Bank ABC Units, its Employees or others acting on behalf of Bank ABC, or for its benefit. Bank ABC must ensure that an ABAC Risk Assessment is completed at least every two years, and submitted to the GCOC and BCC to ensure that the appropriate management actions are taken to address the risks identified.

The ABAC Risk Assessment process must as a minimum:

- identify the inherent bribery and corruption risks;
- document the corresponding ABAC controls; and
- determine residual risks which should be addressed through management action.

The ABAC Risk Assessment must include the evaluation of the following elements as a minimum:

- potential liability created by *Associated Persons* or *Third Parties*;
- *Corruption* risks associated with the countries and industries in which Bank ABC does business, directly or through *Associated Persons*;
- transactions, products or services, including those that involve state-owned or state-controlled entities or *Public Officials*;
- *Corruption* risks associated with gifts and hospitality, hiring/internships, charitable donations and political contributions; and
- changes in business activities that may materially change Bank ABC's corruption risk.

## 10.2. ABAC Training and Awareness

ABC Units must ensure that annual ABAC training and awareness is completed by all Employees.

## 10.3. Gifts and Entertainment

All gifts and entertainment must be given and received in accordance with the Gifts and Entertainment Standard.

The Bank prohibits offering, giving or receiving of gifts or entertainment to or from any third party, customer or public official prior and/or during sign-off of a tender process.

## 10.4. Political Party Funding and Political Donations

Bank ABC Units are prohibited from making donations, or sponsoring, political parties or organisations affiliated to political parties or political campaigns if not reviewed and approved by the GCOC.

## 10.5. Charitable Donations

Charitable donations, on behalf of Bank ABC may only be offered or given in accordance with the principles set out in the Bank ABC Charitable Donations Policy.

## 10.6. Reciprocal Agreements

Bank ABC prohibits entering into of reciprocal agreements where the Bank directly or indirectly may get something of value in return (or any other form of 'quid pro quo') unless they are legitimate business arrangements which are properly documented and approved by Group Legal.



### 10.7. Procurement

The providers of goods and service must be selected in accordance with the Managing Service Providers Procedure (or local equivalent).

All Employees involved in the procurement of goods and services must ensure that they only accept gifts and/or entertainment from suppliers or potential suppliers in accordance with Bank ABC Group Anti-Bribery and Corruption Standard.

### 10.8. Facilitation Payments

Whilst this Policy prohibits facilitation payments, Employees are not expected to place their liberty or personal safety at risk. Should such a scenario materialise the requested payment should be made and reported to the GHFCC, as soon as practically possible.

### 10.9. Duress payments

Whilst several international laws, the GFCC Policy and this Standard prohibit facilitation payments, there might be situations that arise where an Employees and/or Associated Person's life, body, possessions, safety or honour may be threatened and, in these situations, making of a payment may be the only way to escape it, and hence permissible, considering section 10.8.

### 10.10. Principal Investments and Controlled Fund Acquisitions/Joint Ventures

Bank ABC could attract corruption related liability when merging, partnering or acquiring a significant stake in another company/entity or joint venture (collectively the "Target").

Bank ABC must accordingly ensure, as a minimum, that the following steps are taken during these processes:

- a risk-based ABAC due diligence of the Target;
- obtain contractual protections related to bribery and corruption; and
- ensure a risk-based post-acquisition oversight of the Target's ABAC controls.

### 10.11. Reporting Requirements

The responsibility for identifying instances of suspected Bribery and Corruption lies with Employees within Bank ABC. It is the responsibility of all Employees and Associated Persons to be vigilant of the risk of Bribery and to report any suspicion or incident of Bribery or Corruption.

Employees or Associated Persons who have knowledge, become suspicious, or have reasonable grounds to be suspicious that Bribery or Corruption may be taking place, within Bank ABC or by a customer, must as soon as reasonably practicable after the event giving rise to knowledge, suspicion or reasonable grounds, notify the Unit MLRO by submitting an Unusual Activity Report to the MLRO.

## **11. Law Enforcement and Regulatory Engagement**

- 11.1 Bank ABC Units must establish and maintain appropriate procedures and controls to ensure that requests or instructions from regulators, government agencies and law enforcement in relation to Financial Crime Compliance are responded to promptly and effectively.

## **12. FCC Training and Awareness Requirements**

- 12.1. The Bank ABC prescribed mandatory FCC training must be completed by relevant employees within 90 days of joining the Bank and annually thereafter.
- 12.2. Relevant employees performing AML/CTF control processes, as determined by GFCC, must complete the mandatory role-based training prior to commencement of their responsibilities and on an ongoing basis as determined by GFCC.

## **13. FCC Outsourcing**

The FCC function, as a whole, must not be outsourced, while sub-processes (such as e-KYC) may be outsourced.

Where ABC Units outsource any FCC sub-processes to an entity outside of the Bank. The responsibility for Financial Crime Risk Management remains with the Senior Management of Bank ABC Unit undertaking the outsourcing.

Senior Management of Bank ABC Unit must also ensure that the third party has adequate resources and procedures in place to enable Bank ABC Unit to meet the requirements set out in this Policy and all related Group FCC Standards.

The legal agreement with the supplier and/or any other third party must reflect such requirements.

All instances of outsourcing related to FCC must be approved by the GHFCC and noted at the GCOC.

## **14. FCC Management Information Requirements**

Group FCC has defined FCC reporting requirements to be submitted by Units on a monthly basis. The Group FCC dashboard includes Key Risk Indicators (KRIs) on financial crime data points including AML to enable Senior Management to effectively manage the Banks financial crime risk.

All Units must provide Group FCC with accurate data on a monthly basis. Units must also share the FCC dashboard information with their CFCC.

## **15. Record Keeping Requirements**

- 15.1. The Bank must establish and maintain adequate procedures to ensure that the documents related to evidencing compliance with Group Financial Crime requirements are stored for a minimum of 5 years. The Group Data Retention Standard sets the overarching framework for retention of data across Bank ABC, including the minimum period for which records should be retained.

## **16. Dispensations**

Any deviations from this Policy require approval in line with the Group Dispensations Standard.

## **17. Non-Compliance**

Failure to comply with this Policy, including the intentional circumvention of Regulatory Requirements, may have personal consequences and could impact performance ratings or result in disciplinary action, including dismissal. Employees may also be liable to financial penalties or imprisonment by external authorities for violations of applicable laws or regulations.

## **18. Document Administration**

This Policy will be reviewed annually by the policy owner and updated in response to any changes in the legal and regulatory environment.

The Bank ABC Board of Directors must approve this Policy at issuance and on an annual basis thereafter.