

ABC Group

Financial Group Compliance

Table of Content

Contents

1. Introduction.....	3
2. Risk Appetite	4
3. Roles and Responsibilities	4
4. Key Elements of the Programme	8
5. Compliance with the Programme.....	15
6. Document Review and Approval	15
Appendix 1.....	16

1. Introduction

1.1. Purpose

This Financial Crime Programme and supporting Policies, Standards and Procedures (the “Programme”) define the governance, roles and responsibilities, scope and high level controls for Financial Crime (“FC”) risk management at Bank ABC and its Units¹ (“ABC” or the “Bank”).

1.2. Objectives

The objectives of this Programme are to:

- Ensure that ABC’s FC policies and procedures are consistently applied and supervised across the Group;
- define the responsibilities of the Board of Directors, Senior Management, the FC Function and other relevant personnel in relation to FC;
- set out the requirements for effective implementation and monitoring of compliance with this Programme; and
- implement a risk based approach to FC, focusing attention on areas which, following appropriate risk-assessment, appear to present a higher risk.

1.3. Policy Statement

ABC is committed to promoting the highest ethical and professional standards and strives to prevent the Bank from being used, intentionally or unintentionally, for FC.

We adhere to all applicable laws, regulations and international standards. This includes the FC regulations issued by the Central Bank of Bahrain (“CBB”) and local regulations of jurisdictions in which we operate. We also adhere to the recommendations issues by the Financial Action Task Force (“FATF”) and relevant Basel and Wolfsberg standards.

1.4. Definition of Financial Crime

Topics that typically fall under the definition of FC are:

- Money laundering
- Terrorist financing
- Breaches of applicable financial sanctions regimes
- Bribery and corruption.

This Programme covers risk management of money laundering, terrorist financing and sanctions breaches. Bribery and corruption are covered in separate policies.

¹ A Unit is defined as an ABC subsidiary, branch or representative office

1.5. Scope

This Programme applies to all Units within the ABC Group. All Units must ensure that they are compliant with existing local regulations. If there is any conflict between local requirements and the requirements stipulated in this Programme, the Unit must apply the higher standard.

2. Risk Appetite

ABC considers FC unacceptable and unethical and has adopted a risk based approach to manage its exposure to FC risk. This enables ABC to focus its control framework on those customers, products, channels and jurisdictions that are assessed as carrying a greater FC risk.

No ABC employee, or anyone acting on ABC's behalf, must do anything to circumvent ABC's FC policies and procedures.

3. Roles and Responsibilities

The roles and responsibilities for compliance with this Programme are set out below.

3.1. Group Board of Directors

The Group Board of Directors is ultimately responsible for ensuring that the Bank maintains an effective FC Programme and for providing adequate oversight.

The Group Board of Directors with the assistance of the Group Board Audit Committee is responsible for ensuring:

- That an appropriate risk appetite is established covering FC;
- the FC Function is adequately resourced and independent of business lines;
- that Senior Management develops, implements and effectively oversees a robust FC Programme;
- compliance with applicable FC laws and regulations Group-wide; and
- that systems and controls for compliance with the FC Programme are reviewed and approved annually.

The Group Board approves the overall FC Programme, and the supporting FC Policies and Standards, on an annual basis after having been reviewed and recommended for approval by the Group Compliance Oversight Committee and Group Board Audit Committee.

3.2. Group Board Audit Committee

The Group Board Compliance Committee, on behalf of the Group Board, is responsible for overseeing the adequacy and effectiveness of the overall, Group-wide, systems and controls in relation to FC.

3.3. Group Compliance Oversight Committee

The Group Compliance Oversight Committee ("GCOC") reports to the Group Chief Executive Officer and the Group Board Compliance Committee. The GCOC is the Senior Management Oversight Committee Group-wide for compliance and FC risks and policies.

3.4. The Group Compliance Officer

The Group Compliance Officer (“GCO”) reports to the Group Chief Executive Officer and the Group Board Compliance Committee. The GCO is, on behalf of the GCOC and Group Board Compliance Committee, responsible for ensuring that the Bank operates within a clearly defined Group-wide FC risk management framework.

The GCO meets with the Group Board Compliance Committee on a quarterly basis to provide a status update on Compliance and FC risk for the Group and proactively advises on acting in a manner that is compliant with applicable FC laws and regulations.

The Group Board designates and authorises the Group Compliance Officer to appoint the Group MLRO and MLROs across ABC Units, including to delegate authority to appoint Unit MLROs to the Group MLRO.

3.5. Group Money Laundering Reporting Officer

The Group Money Laundering Reporting Officer reports to the GCO and is responsible for oversight of the Bank’s FC systems and controls including:

- Developing and maintaining the Bank’s FC Policies and Standards on an ongoing basis in-line with applicable legal and regulatory requirements and industry best practice.
- Ensuring that Unit FC 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 FC matters generally and also the Bank’s FC 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 FC related matters, with the regulatory authority in Bahrain (and other jurisdictions as required).
- Based on a review of the periodic reports on FC submitted by the Unit MLROs, perform an overall assessment of the effectiveness of the Bank’s FC Policies and Procedures adherence by ABC Group-wide and make recommendations to Senior Management where improvements are required including enhancements to FC related systems and technologies.
- Reporting to the GCO on critical FC issues across the Group which require the attention of the Senior Management.
- Consulting with the business stakeholders and conducting training needs analysis for FC related matters. Establishing an annual Group-wide FC training plan including minimum standards for training material, frequency and relevant staff (including Senior Management and Board).

3.6. Subsidiary Board

The Subsidiary Board is ultimately responsible for ensuring the local Unit maintains an effective FC Programme and for providing adequate oversight over the FC Programme.

The Subsidiary Board, with the assistance of the Subsidiary Board Compliance / Audit Committee is responsible for ensuring:

- That an appropriate risk appetite, in-line with Group Standards, is established covering FC;
- the FC Function is adequately resourced and independent of business lines;
- that Senior Management develops, implements and effectively oversees a robust FC Programme;
- compliance with applicable FC laws and regulations and Group standards; and
- that systems and controls for compliance with the FC Programme are reviewed and approved annually.

3.7. Subsidiary Board Audit Committee

The Subsidiary Board Audit / Compliance Committee is responsible for, on behalf of the Subsidiary Board, overseeing the adequacy and effectiveness of the subsidiary's systems and controls in relation to FC.

3.8. Senior Management

Senior Management refers to the CEO/Unit Head and heads of functions. Senior Management is responsible for:

- Leading by example, including by knowing and applying the rules of the Programme and monitoring compliance with these rules within the Bank.
- Understanding and owning the FC risks and integrating FC compliance into business processes and controls.
- Establishing a permanent, effective FC function within the Unit which is composed of an appropriate number of staff with sufficient experience, technical skills and seniority to discharge their responsibilities considering the size and complexity of the Unit.
- Reviewing periodic reports submitted by the MLRO.
- Reviewing the findings of compliance reports, internal or external audits and of examinations by the regulators on FC issues and developing plans to rectify any weaknesses.
- Ensuring that FC compliance is integrated into discipline and compensation policies and that appropriate action is taken in case of breach of compliance with applicable laws, regulations or this FC Programme.
- Ensuring that MLROs and FC staff receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall FC risk profile of the Unit.

3.9. Unit Compliance and Financial Crime Committee

The Unit Compliance and Financial Crime Committee (“CFCC”), or equivalent, reports to the Unit Management Committee and the Unit Board Audit / Compliance Committee (when applicable) and supports Senior Management with the oversight of compliance and FC risks and policies.

Minutes of the CFCC are tabled to the GCOC.

3.10. Unit MLRO

The Unit MLRO reports to the local Head of Compliance/CEO/Unit Head as appropriate, with a functional reporting line to the Group MLRO. The Unit MLRO is responsible for:

- Establishing and implementing an annual FC Plan
- Reporting on:
 - FC Plan implementation;
 - significant risk, incident or issue identified in the Unit’s operations;
 - effectiveness of the Unit’s FC Programme; and
 - significant changes to FC regulatory requirements;
- Ensuring that appropriate arrangements are in place within the Unit for:
 - Customer due diligence and ongoing monitoring;
 - reporting of suspicious activity;
 - Record keeping;
 - FC operational processes and controls;
 - FC risk assessment and management;
 - the monitoring and management of FC compliance;
 - the internal communication of FC policies and procedures; and
 - training relevant employees on applicable aspects of FC;

and that they are aligned with Group Standards.

In particular:

- Maintaining and updating the Unit’s internal assessment of FC risk relevant to the operating environment; and for presenting the risk assessment findings to the Board and/or relevant board committees;
- ensuring appropriate arrangements in place for assessing and responding to higher-risk customers, such as, Politically Exposed Persons (“PEPs”) and other high-risk relationships in accordance with the FC policies and procedures;
- liaising with law enforcement and regulatory bodies on matters relating to Court Orders and investigations relating to FC;
- ensuring monitoring and assurance arrangements for FC are in place, in coordination with Internal Audit; and
- monitoring relevant guidance and other sources of information on regulatory changes, country risk, new/emerging trends in money laundering, such as reports produced by FATF or local regulatory agents.

3.11. All Employees

All employees are responsible for:

- Understanding and complying with the Banks's FC policies and procedures, and all applicable laws and regulations.
- Identifying red flags indicating that a customer may be seeking to engage in a relationship or transaction for other than a lawful purpose or with the proceeds of alleged illegal activity.
- Ensuring Customer Due Diligence is in place and in compliance with the Bank's policies before establishing and during the course of customer relationships or engaging in transactions with customers.
- Attending required FC training.
- Reporting suspicious activity immediately to the Unit MLRO.

3.12. Internal Audit

Internal Audit is responsible for:

- Considering FC risk in the annual audit plan
- Reporting to the Board on FC risks identified in assurance testing of systems and controls.

4. Key Elements of the Programme

4.1. Senior Management Responsibilities

Responsibilities and accountabilities for managing FC risk must be established and clearly communicated (as set out in this Programme).

4.2. Risk Based Approach

All Unit's must take appropriate steps to identify and assess their FC risks at least annually. This informs the Unit's Compliance Monitoring Plan and overall annual FC Compliance Plan which shall be tabled to the Board for approval.

Minimum standards for FC compliance testing required in the Compliance Monitoring Plan shall be established at Group level and approved by the Group MLRO.

Senior Management owns the FC risks and should be involved in the risk assessment process. The annual risk assessment must be tabled to the Board and/or relevant committees.

The risk-based approach undertakes a number of steps in assessing the most cost effective and proportionate way to manage and mitigate the FC risks faced by the Bank.

These steps are to:

- identify the FC risks that are relevant to the Bank;
- assess the risks presented by the Bank's:

-
- customers, counterparties and all underlying beneficial owners;
 - products;
 - delivery channels; and
 - geographical areas of operation;
-
- design and implement controls to manage and mitigate these assessed risks, in the context of the Bank's risk appetite statement;
 - record the results of the risk assessment and the controls that have been put in place; and
 - monitor and improve the effective operation of these controls.

The FC Risk Assessment Methodology shall be reviewed and updated annually by the Group MLRO and submitted to the GCOC for approval.

FC risks must also be identified and assessed for new products, business practices and technologies.

4.3. Business Policies and Procedures

Appropriate risk-based policies and procedures must be available in all Units to support the requirements of this Programme. They must be clear, relevant and accessible to all personnel.

Documented policies and procedures should be available at each Unit for those listed in Appendix 1, and any others required by local laws and regulations.

The policies and procedures must be in-line with Group standards that are approved annually by the GCOC. Any exceptions must be submitted by the local CFCC, in consultation with the Group MLRO, and approved by the local Board Audit / Compliance Committee/Unit Head (as applicable) and GCOC.

Group and Unit FC Policies and Procedures should be reviewed at least annually in conjunction with the FC risk assessment and approved by the Board/local Unit Head as applicable.

4.4. Customer Due Diligence and Monitoring

Each Unit must have documented customer due diligence and monitoring Policies and Procedures in line with the local regulations and Group Standards. They should include the following as a minimum:

- Client acceptance and risk classification.
- Obtaining background information about a customer prior to establishing a relationship. In particular, to verify the identity of the customer and establish the customer's occupation/business, source of funds, purpose of transactions and the expected level and pattern of activity.
- Screening the customer and its related parties when initiating the relationship as well as on a regular basis against Group mandatory watch lists and other lists as required by the local regulator.
- Taking appropriate steps to evaluate the robustness of the customer due diligence procedures of any other bank or agent wishing to use ABC as its correspondent bank, before entering into a relationship.
- Provide guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient, inaccurate or adverse information is

obtained.

- Undertaking enhanced due diligence on customers, banks or agents that are deemed to present a higher risk.
- Establishing the underlying beneficial ownership and controllers of all legal entities with which ABC conducts business. In addition, establishing the beneficial ownership of all funds or other properties handled by the Bank.
- Collecting sufficient information and having processes in place in order to identify when a customer is a PEP.
- Keeping customer and correspondent bank due diligence information relevant and up to date on a risk based approach.
- Monitoring customer activity, paying special attention to higher risk customers or activities and reporting suspicious activities to appropriate regulatory agencies.
- Monitoring inward and outward SWIFT T messages to ensure that prohibited financial services are not provided to persons and entities on the Group mandatory watch lists and other lists as required by the local regulator.

4.5. Terrorist Financing and Economic Sanctions

It is ABC's policy to fully comply with all applicable terrorist financing and economic sanctions laws and regulations and not to enter into any transaction in breach of these laws and regulations.

The ABC Group Sanctions Policy has been established as a stand-alone document. All Units must have policies and procedures in place to ensure compliance with this policy.

4.6. Politically Exposed Person Relationship

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing.

The risks associated with PEPs needs to be classified and managed appropriately in accordance with the Group PEP Policy.

Each Unit, as a minimum, must:

- Have appropriate risk-management systems to determine whether the customer or the beneficial owner of a customer is a PEP;
- obtain Senior Management approval for establishing (or continuing, for existing customers) such business relationships;
- take reasonable measures to establish the source of wealth and source of funds; and
- conduct enhanced ongoing monitoring of the business relationship.

4.7. Correspondent Banking Relationships

Correspondent banking relationships are considered high risk. Each Unit must develop appropriate controls and monitoring for these relationships.

Vostro Accounts may only be used for the clearing and settlement of payments of the Vostro Account holder itself, on its own behalf². Vostro Accounts may not be used to clear or settle incoming and outgoing payments:

- For or on behalf of clients of the Vostro Account holder; or
- for or on behalf of non-clients of the Vostro Account holder.

ABC will not allow 'nested payments'/'downstream' accounts or similar arrangements that give Vostro Account holders indirect access to ABC's own Nostro Accounts.

4.8. Dormancy and Terminating Relationships

Relationships should be marked as dormant where there have been no client initiated transactions on the accounts or utilisation of limits for the qualifying period specified in the Group-wide Control Standard on Dormant Accounts and Blocking Accounts.

A relationship must be terminated after having given appropriate notice in circumstances where customers refuse to provide adequate due diligence information. Consideration should be given to the need to complete the suspicious activity reporting process in these circumstances.

Reactivation of an account should serve as a trigger to examine the adequacy of the Customer Due Diligence file for the customer and observe any approval processes required for such customers.

4.9. Shell Banks

Units must ensure that they do not directly or indirectly deal with 'shell' banks. Units should additionally ensure that they conduct business only with correspondent banks that possess licences to operate in their countries of origin.

4.10. Transaction Monitoring

Units must define appropriate standards and implement processes for transaction monitoring in-line with business activity. Processes must identify unusual transactions and unusual patterns of transactions.

Enhanced monitoring applies to all relationships assessed as high risk and includes, but is not limited to:

- All PEP relationships which have been determined as higher risk,
- those customers with a higher risk business or location or transacting in higher risk products; and
- all customers with a higher risk profile due to the fact that multiple Suspicious Transaction

² For MENA Units, there are no special restrictions on the provision of local clearing in the domestic currency. Refer to the Group Control Standard – Management of Vostro Accounts.

Enhanced monitoring routines need to be defined by the MLRO and be appropriate to the risk. They must include routines in addition to the normal transaction monitoring routines or must be carried out with lower thresholds or increased frequency.

4.11. Electronic Fund Transfers

In accordance with the Group-wide Control Standard on Payments, 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;
- 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.

Additionally, systems and controls must be in place to identify wire transfers that do not meet with these requirements.

4.12. Law Enforcement Enquiries and Orders

Units must ensure that adequate systems and controls are in place to comply in a timely manner with externally received requests from law enforcement or any other official authorised bodies. All such requests must be immediately notify to the MLRO. The MLRO must immediately notify Senior Management and the Group MLRO if an enquiry involves a customer of the Bank.

The official request process should trigger a review of the relationship and include a retrospective review of the customer due diligence and monitoring on the account. Consideration should be given to whether a suspicious activity report needs to be made.

4.13. Staff Recruitment, Training and Awareness

All Units must develop adequate screening procedures to ensure high standards when hiring employees. These procedures must include controls to prevent criminals or their associates from being employed by ABC.

All Units must provide training on joining and at least annually thereafter to ensure that staff who handle customer transactions (including staff involved in their processing and settlement) or are managerially responsible for the handling of such transactions, are made aware of:

- Their legal and regulatory responsibilities with respect to FC;
- the identity and responsibilities of the MLRO and their Deputy MLRO;
- the potential consequences, both individual and corporate, of any breach of applicable FC laws and regulations;
- the Bank's current FC Policies and Procedures;

- money laundering and terrorist financing typologies and trends;
- the type of customer activity or transaction that may justify an internal STR/Unusual Activity Report (“UARs”);
- the Bank's procedures for making internal STRs/UARs; and
- customer due diligence measures with respect to establishing business relations with customers.

The training must be in line with local regulatory requirements and Group standards approved by the Group MLRO. It should be relevant and specific to the day to day activities of those being trained.

In addition, training should be ongoing and incorporate current developments and changes to any FC related regulations. The training programme should reinforce the importance that the Board and Senior Management place on the Bank's compliance with the FC programme and ensure that all employees understand their role in maintaining an effective FC compliance programme.

Records of all training and awareness activity must be kept in accordance with record keeping requirements.

Training to FC Staff

All Staff should receive training, at least annually, that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall FC risk profile of the Bank.

Training to Board of Directors and Senior Management

The Board of Directors and Senior Management should be informed of changes and new developments in the FC regulations to ensure they understand the importance of FC regulatory requirements, the ramifications of non-compliance, and the risks posed to the Bank.

4.14. Suspicious Activity Reporting

Senior Management of each Unit must ensure:

- All relevant staff are aware of their personal obligations under local applicable laws and regulations, to raise an internal report where they have knowledge or reasonable grounds for suspicion of money laundering or terrorist activity.
- All relevant staff are trained on how to identify and report suspicious activity.
- There is a clear and defined escalation process from the point of initial detection to disposition of the investigation.
- There are appropriate systems and controls in place to facilitate and manage STRs. This must include, where required, mechanisms for ensuring compliance with threshold driven mandatory reporting requirements.
- Appropriate actions are taken in addition to filing an STR such as determining whether it is necessary to terminate a relationship with the customer this is the subject of the filing.
- Procedures are in place to ensure the timely investigation of customers which have been the subject of an STR, or which are the subject of law enforcement information requests, Court Orders, or Notices issued by any other relevant authority.

- Appropriate arrangements are in place to protect the confidentiality of STRs and never to alert any persons suspected of illegal activity that their activities are subject to investigation or have been reported as suspicious.
- Sufficient information on STR filings is provided to the Board or appropriate committees in order to fulfil its fiduciary duties.

4.15. Management Information

Units must ensure that appropriate key indicators are in place in order to assess compliance standards and highlight potential weaknesses. Such indicators should be regularly reviewed.

These indicators should be incorporated in a regular report to Senior Management in order to inform them of compliance standards and existing or potential risks. Businesses should develop key risk and performance indicators in line with Group standards and which are relevant to their own operating environment.

An annual report from the MLRO on the operation and effectiveness of systems and controls must be produced and presented to the Group MLRO, local CFCC, Board Compliance Committee and Board (as applicable) in accordance with local regulations and in accordance with Group requirements.

4.16. Record Keeping

Each Unit must have documented record keeping procedures in place that comply with the local regulations or Group standards (as defined in the FC Policies and Standards), whichever is the longer.

Documentation retained, whether physical or electronic, must be accurate, legible, auditable, and easily retrievable. Documents that must be retained as a minimum include:

- Identification, due diligence and transaction records
- Internal STRs/UARs and SARs
- Staff training records
- Records of screening of customers and filtering of transactions against applicable watch lists as well as decisions made for possible matches
- Records relating to information shared with law enforcement authorities
- Management information and other reports submitted by the MLRO to the Board and relevant Committees. Also the minutes of the meetings considering these reports and agreeing to any actions taken in respect of the recommendations.

4.17. Escalation Process

Any significant issues or risks involving legal, regulatory or reputational matters relating to money laundering, terrorism or financial sanctions must be escalated in line with the Group Escalation Policy.

4.18. Independent Assurance

The FC Function of each Unit must obtain an independent review of the quality and effectiveness of its FC procedures, systems and controls at least once each calendar year (CBB AML Agreed Upon Procedures). This review must be made by the Bank's external auditor or a consultancy firm approved

by the CBB. The report is provided to Group MLRO and Senior Management. The findings are reviewed and any remediating actions required are tracked until resolution at the local CCFC and local/Group Board Compliance / Audit Committees), as applicable.

4.19. System Validation

The minimum Group standards and rational for determining appropriate transaction monitoring must be documented and approved by the Group MLRO. Each Unit MLRO is responsible for ensuring any local regulatory requirements are also taken into consideration. Any exceptions to the Group standards must be approved by the Group MLRO.

AML and watch list screening systems must be validated periodically to verify accuracy and effectiveness and confirm the system produces results that meet with the design specifications. This may be conducted by an independent consultant or an internally assigned appropriate skilled person approved by the Group MLRO.

5. Compliance with the Programme

A wilful breach or any failure to disclose a known inadvertent breach of this Programme and supporting policies and procedures could result in consequences for the Bank and its employees and may result in disciplinary action including dismissal, or in some circumstances, criminal prosecution.

6. Document Review and Approval

The FC Programme and FC Policies and Standards shall be reviewed and updated annually by the Group MLRO and submitted to the Board of Directors for approval. It will also be amended on an adhoc basis in response to any changes in the legal or regulatory environment.

The local MLRO is responsible for ensuring the local FC Programme and FC policies and standards are aligned with the Group documents at all times and are approved by the local Board (subsidiaries)/General Manager (branches), on an annual basis or more frequently in response to Group updates or changes in local legal or regulatory environment.

Where a local Unit's FC Programme varies to Group a documented gap analysis shall be submitted as part of the approval process.

Where local laws or regulations prevent any Unit from applying the CBB FC regulatory requirements, or Senior Management wishes to exclude a requirement or deviate from a requirement in this FC Programme or supporting FC policies and standards, it must be submitted by the local CFCC in consultation with the GCOC and approved by the local Board Compliance / Audit Committee.

Where local laws or regulations prevent any Unit from applying the CBB FC regulatory requirements, the Group MLRO, must inform the CBB in writing.

Appendix 1

As a minimum, documented Policies, Standards and Procedures should be available at each Unit for the following:

- Legal Obligations and Penalties
- Appointment of a Money Laundering Reporting Officer
- Customer Due Diligence and Monitoring
- Electronic Fund Transfers
- Reporting Suspicious Activity
- Staff Recruitment, Awareness and Training
- Record Keeping Requirements
- Law Enforcement Enquiries and Requests
- Sanctions and Terrorist Financing
- Compliance Monitoring
 - Annual Risk Assessment
 - Annual MLRO Report
 - Management Information
 - Compliance Monitoring Programme
- System Validation.