FINANCIAL CRIME MODULE

MODULE	FC (Financial Crime)
CHAPTER	Table of Contents

MODULE	FC (Financial Crime)
CHAPTER	Table of Contents (continued)

MODULE	FC (Financial Crime)
CHAPTER	Table of Contents (continued)

Date Last Changed

APPENDICES (included in Volume 1 (Conventional Banks), Part B)

CBB Reporting Forms

Supplementary Information

FC-A.1 Purpose

Executive Summary

FC-A.1.1 This Module applies, to all conventional bank licensees, a comprehensive framework of Rules and Guidance aimed at combating money laundering and terrorist financing. In so doing, it helps implement the FATF Recommendations on combating money laundering and financing of terrorism and proliferation, issued by the Financial Action Task Force (FATF), and the requirements of the Basel Committee 'Customer Due Diligence for Banks' paper, that are relevant to conventional bank licensees. (Further information on these can be found in Chapter FC-10.)

FC-A.1.2 The Module requires conventional bank licensees to have effective anti-money laundering ('AML') policies and procedures, in addition to measures for combating the financing of terrorism ('CFT'). The Module contains detailed requirements relating to customer due diligence, reporting and the role and duties of the Money Laundering Reporting Officer (MLRO). Furthermore, examples of suspicious activity are provided, to assist conventional bank licensees monitor transactions and fulfil their reporting obligations under Bahrain law.

Legal Basis

FC-A.1.3 **This Module contains the Central Bank of Bahrain's ('CBB') Directive (as amended from time to time) regarding the combating money laundering and terrorism financing and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). The Directive in this Module is applicable to all conventional bank licensees.**

FC-A.1.4 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

FC-A.2 Module History

Changes to the Module

FC-A.2.1 This Module was first issued in July 2004 by the BMA as part of the conventional principles volume. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change was made: Chapter UG-3 provides further details on Rulebook maintenance and version control.

FC-A.2.2 When the CBB replaced the BMA in September 2006, the provisions of this Module remained in force. Volume 1 was updated in October 2007 to reflect the switch to the CBB; however, new calendar quarter dates were only issued where the update necessitated changes to actual requirements.

FC-A.2.3 A list of recent changes made to this Module is detailed in the table below:

Module Ref.	Change Date	Description of Changes
FC-1.11.1	01/01/06	New text for syndicated business
FC-1.1.3, FC-1.2.8, FC-1.2.11, FC-3.1.4	01/01/06	Correction of minor typos
FC-A.1	10/2007	Updated to reflect new CBB Law: new Rule FC-A.1.3 introduced Categorising this Module as a Directive.
FC-5.3.1	10/2007	Updated new e-mail address for the Compliance Directorate.
FC-7.1.1	10/2007	Guidance on customer instructions moved from OM-7.1
FC-1.11.1 & FC-4.3.5	04/2008	Minor guidance changes
FC-1.6.5-6	07/2009	New authorization requirement in respect of transfers of funds to and from foreign countries on behalf of charities.
FC-4.1.4	10/2009	Appointment of Deputy MLRO to require CBB prior approval.
FC-A.1.3	01/2011	Clarified legal basis.
FC-1.6.4, FC-4.2.1	01/2011	Corrected name of Compliance Directorate.
FC-1.10A	01/2011	Added Section on Enhanced due diligence: cross border cash transactions equal to an above BD 6,000 by courier.
FC-4.3.5 and FC-4.3.6	01/2011	Corrected minor typo.
FC-4.1.6	10/2011	Clarified requirements for MLRO.
FC-4.3	10/2011	Amended Section to allow for CBB-approved consultancy firm to do required sample testing and report under Paragraph FC-4.3.1.
FC-4.3.5 and FC-4.3.6	01/2012	Amended to reflect the addition of approved consultancy firm.
FC-1.6	01/2013	Added requirement dealing with sport associations registered with the Bahrain Olympic Committee (BOC).
FC-1.11.1	01/2013	Updated reference to Bahrain Bourse ('BHB').
FC-1.1.10 to FC-1.1.16, and FC-1.3.4	10/2013	Amended and updated due diligence requirements, including requirements in dealing with non-resident accounts.
FC-1.1.13 to FC-1.1.13C	04/2014	Added requirements regarding the opening of accounts for non-residents or companies under formation.
FC	10/2014	Updated to reflect February 2012 update to FATF Recommendations

FC-A.2 Module History (continued)

FC-A.2.3 (cont'd)

Module Ref.	Change Date	Description of Changes
FC-1.5	07/2016	Aligned definition of PEPs with FATF and moved to Glossary.
FC-4.1.1	07/2016	Deleted reference for Appendix FC-4 as requirements are covered under Form 3.
FC-5.2.3	07/2016	Updated instructions for STR.
FC-B.2.4	10/2016	Deleted reference to Module PCD.
FC-1.2.9A	01/2017	Added guidance paragraph on CR printing.
FC-8.2.1AA	04/2017	Implementing and complying with the United Nations Security Council resolutions requirement.
FC-1.1.2B	10/2017	Amended paragraph on CDD requirements.
FC-1.1.13D – FC-1.1.13H	10/2017	Added guidance paragraphs on opening accounts for companies under formation.
FC-1.2.7	10/2017	Amended paragraph.
FC-1.2.8A	10/2017	Added new paragraph on legal entities or legal arrangements CDD.
FC-1.12	10/2017	Added new Section on Simplified CDD: For entities Operating under Regulatory Sandbox.
FC-2.2.10 – FC-2.2.11	10/2017	Amended paragraphs on On-going CDD and Transaction Monitoring.
FC-4.1.3A	10/2017	Added paragraph on combining the MLRO or DMLRO position with any other position within the licensee.
FC-B.2.4	01/2018	Amended paragraph.
FC-1.8.1	01/2018	Amended paragraph.
FC-1.9.1	01/2018	Amended paragraph.
FC-1.11.1	01/2018	Deleted sub-paragraph (g).
FC-5.2.6	01/2018	Amended paragraph.
FC-8.1.4	01/2018	Amended Paragraph.
FC-8.2.2	01/2018	Deleted Paragraph.
FC-1.1.2	07/2018	Deleted sub-paragraph (g).
FC-1.10A	07/2018	Amended Section title deleting the threshold.
FC-1.10A.2	07/2018	Amended Paragraph deleting the threshold.
FC-1.11.3	07/2018	Deleted Paragraph.
FC-1.11.8	07/2018	Deleted Paragraph.
FC-1.12.10	07/2018	Amended Paragraph number (f).
FC-4.3.2C	10/2018	Amended Paragraph and changed from Guidance to Rule.
FC-1.11.1	01/2019	Amended references.
FC-4.3.2 - FC-4.3.5	01/2019	Amended references.
FC-7.1.2	01/2019	Amended references.
FC-1.6.1A	07/2019	Amended Paragraph (GOYS changed to Ministry of Youth & Sport Affairs).
FC-1.6.2	07/2019	Amended Paragraph (GOYS changed to Ministry of Youth & Sport Affairs).
FC-1.6.2A	07/2019	Added a new Paragraph on opening additional bank accounts for Clubs and Youth Centres.
FC-1.6.5	07/2019	Amended Paragraph on Fund Transfers.

FC-A.2 Module History (continued)

Module Ref.	Change Date	Description of Changes
FC-1.3.4	10/2019	Amended Paragraph on enhanced due diligence measures for non-GCC account holders.
FC-3.2.4	10/2019	Amended authority name.
FC-4.2.1	10/2019	Amended authority name.
FC-5.2.3	10/2019	Amended authority name.
FC-5.3.2	10/2019	Amended authority address.
FC-8.2.1AA	10/2019	Defined 'without delay'.
FC-1.1.1	01/2020	Amended Paragraph on procedures approval.
FC-1.2.1	01/2020	Added a new Sub-Paragraph.
FC-4.3.5	01/2020	Amended Paragraph on report submission date.
FC-2.1.3 & FC-2.1.4	04/2020	Added new Paragraphs on KPIs compliance with AML/CFT requirements.
FC-1.1.14	01/2021	Amended Paragraph on account opening for non-residents.
FC-3.1.10A	01/2021	Added a new Paragraph on rejecting payment transactions.
FC-6.1.6A	01/2021	Added a new Paragraph on requirements to hire new employees.
FC-1.1.14	04/2021	Amended Paragraph.
FC-A.1.3	01/2022	Amended Paragraph to replace financial crime with money laundering and terrorism financing
FC-C	01/2022	New chapter on risk-based approach (RBA)
FC-1.1	01/2022	Amendments to general requirements to introduce additional rules for non-resident customers, amendments to customers onboarded prior to full completion of customer due diligence, digital onboarding etc.
FC-1.2	01/2022	Amendments to recognise E-KYC and electronic documents law.
FC-1.3	01/2022	Amendments to introduce additional guidance in enhanced due diligence requirements.
FC-1.4	01/2022	Amendments to introduce detailed requirements for digital onboarding and related requirements.
FC-1.5	01/2022	Amendments relating to digital onboarding of Bahraini PEPs.
FC-1.11.7A	01/2022	Added a new Paragraph on not applying simplified CDD in situations where the licensee has identified high ML/TF/PF risks.
FC-1.12	01/2022	Deleted Section on simplified due diligence requirements relating to Regulatory Sandbox since they will be covered separately in the Regulatory Sandbox Framework.
FC-4.3.1B	01/2022	Amended Paragraph.
FC-4.3.2	01/2022	Amended Paragraph.
FC-4.3.5	01/2022	Amended Paragraph.
FC-4.3.6	01/2022	Deleted Paragraph.
FC-6.1.6A	01/2022	Deleted Paragraph.
FC-1.1.14A	07/2022	Added a new Paragraph on opening accounts for Bahraini national not physically present in Bahrain through a digital onboarding process.
FC-C.2.3	01/2023	Minor amendment to Paragraph.
FC-1.1.14	01/2023	Amended Paragraph on opening accounts for non-residents.
FC-1.1.14B	01/2023	Added a new Paragraph on opening accounts for non-residents with golden visa.
FC-8.2.4(c)	01/2023	Added a new Sub-paragraph on reporting any frozen assets or actions taken.

FC-A.2 Module History (continued)

Evolution of the Module

FC-A.2.4 Prior to the introduction of Volume 1 (Conventional Banks) of the CBB Rulebook, the BMA had issued various circulars containing requirements covering different aspects of financial crime. These requirements were consolidated into this Module.

MODULE	FC:	Financial Crime
CHAPTER	FC-B:	Scope of Application

FC-B.1 License Categories

FC-B.1.1 **This Module applies to all conventional bank licensees, including branches of banks incorporated outside of Bahrain, and Bahrain-incorporated subsidiaries of overseas groups.**

FC-B.1.2 The requirements of this Module are in addition to and supplement the requirements contained in Decree Law No. (4) of 2001 with respect to the prevention and prohibition of the laundering of money: this Law was subsequently updated, with the issuance of Decree Law No. 54 of 2006 with respect to amending certain provisions of Decree No. 4 of 2001 (collectively, 'the AML Law'). The AML Law imposes obligations generally in relation to the prevention of money laundering and the combating of the financing of terrorism, to all persons resident in Bahrain. All conventional bank licensees are therefore under the statutory obligations of that Law, in addition to the more specific requirements contained in this Module. Nothing in this Module is intended to restrict the application of the AML Law (a copy of which is contained in Part B of Volume 1 (conventional banks), under 'Supplementary Information'). Also included in Part B is a copy of Decree Law No. 58 of 2006 with respect to the protection of society from terrorism activities ('the anti-terrorism law').

FC-B.2 Overseas Subsidiaries and Branches

FC-B.2.1 **Conventional bank licensees must apply the requirements in this Module to all their branches and subsidiaries operating both in the Kingdom of Bahrain and in foreign jurisdictions. Where local standards differ, the higher standard must be followed. Conventional bank licensees must pay particular attention to procedures in branches or subsidiaries in countries that do not or insufficiently apply the FATF Recommendations and do not have adequate AML/CFT procedures, systems and controls (see also Section FC-8.1).**

FC-B.2.2 **Where another jurisdiction's laws or regulations prevent a conventional bank licensee (or any of its foreign branches or subsidiaries) from applying the same standards contained in this Module or higher, the licensee must immediately inform the CBB in writing.**

FC-B.2.3 In such instances, the CBB will review alternatives with the conventional bank licensee. Should the CBB and the licensee be unable to reach agreement on the satisfactory implementation of this Module in a foreign subsidiary or branch, the conventional bank licensee may be required by CBB to cease the operations of the subsidiary or branch in the foreign jurisdiction in question.

FC-B.2.4 **Financial groups (e.g. a bank with at least one financial entity as a subsidiary) must implement groupwide programmes against money laundering and terrorist financing, including policies and procedures for sharing information within the group for AML/CFT purposes, which must also be applicable, and appropriate to, all branches and subsidiaries of the financial group. These must include:**

(a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
(b) An ongoing employee training programme;
(c) An independent audit function to test the system;
(d) Policies and procedures for sharing information required for the purposes of CDD and money laundering and terrorist financing risk management;

FC-B.2 Overseas Subsidiaries and Branches (continued)

(e) The provision at group-level compliance, audit, and/or AML/CFT functions of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and

(f) Adequate safeguards on the confidentiality and use of information exchanged.

FC-C.1 Risk Based Approach

FC-C.1.1 A conventional bank licensee must implement Risk Based Approach (RBA) in establishing an AML/CFT/CPF program and conduct ML/TF/PF risk assessments prior to and during the establishment of a business relationship and, on an ongoing basis, throughout the course of its relationship with the customer. The licensee must establish and implement policies, procedures, tools and systems commensurate with the size, nature and complexity of its business operations to support its RBA.

FC-C.1.2 A conventional bank licensee must perform enhanced measures where higher ML/TF/PF risks are identified to effectively manage and mitigate those higher risks.

FC-C.1.3 A conventional bank licensee must maintain and regularly review and update the documented risk assessment. The risk management and mitigation measures implemented by a licensee must be commensurate with the identified ML/TF/PF risks.

FC-C.1.4 Conventional bank licensees must allocate adequate financial, human and technical resources and expertise to effectively implement and take appropriate preventive measures to mitigate ML/TF/PF risks.

FC-C.2 Risk Assessment

FC-C.2.1 A conventional bank licensee must ensure that it takes measures to identify, assess, monitor, manage and mitigate ML/TF/PF risks to which it is exposed and that the measures taken are commensurate with the nature, scale and complexities of its activities. The risk assessment must enable the licensee to understand how, and to what extent, it is vulnerable to ML/TF/PF.

FC-C.2.2 In the context of the risk assessment, "proliferation financing risk" refers to the potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in FATF Recommendation 7.

FC-C.2.3 The risk assessment must be properly documented, regularly updated and communicated to the conventional bank licensee's senior management. Licensees must have in place policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified. In conducting its risk assessments, the licensee must consider quantitative and qualitative information obtained from the relevant internal and external sources to identify, manage and mitigate these risks. This must include consideration of the risk and threat assessments using, national risk assessments, sectorial risk assessments, crime statistics, typologies, risk indicators, red flags, guidance and advisories issued by inter-governmental organisations, national competent authorities and the FATF, and AML/CFT/CPF mutual evaluation and follow-up reports by the FATF or associated assessment bodies.

FC-C.2.4 A conventional bank licensee must assess country/geographic risk, customer/investor risk, product/ service/ transactions risk and distribution channel risk taking into consideration the appropriate factors in identifying and assessing the ML/TF/PF risks, including the following:

a) The nature, scale, diversity and complexity of its business, products and target markets;
b) Products, services and transactions that inherently provide more anonymity, ability to pool underlying customers/funds, cash-based, face-to-face, non-face-to-face, domestic or cross-border;
c) The volume and size of its transactions, nature of activity and the profile of its customers;

FC-C.2 Risk Assessment (continued)

d) The proportion of customers identified as high risk;
e) Its target markets and the jurisdictions it is exposed to, either through its own activities or the activities of customers, especially jurisdictions with relatively higher levels of corruption or organised crime, and/or deficient AML/CFT/CPF controls and listed by FATF;
f) The complexity of the transaction chain (e.g. complex layers of intermediaries and sub intermediaries or distribution channels that may anonymise or obscure the chain of transactions) and types of distributors or intermediaries;
g) The distribution channels, including the extent to which the licensee deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD and the use of technology; and
h) Internal audit, external audit or regulatory inspection findings.

Country/Geographic risk

FC-C.2.5 Country/geographic area risk, in conjunction with other risk factors, provides useful information as to potential ML/TF/PF risks. Factors that may be considered as indicators of higher risk include:

(a) Countries identified by credible sources, such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT/CPF systems;
(b) Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
(c) Countries identified by credible sources as having significant levels of corruption or organized crime or other criminal activity, including source or transit countries for illegal drugs, human trafficking and smuggling and illegal gambling;
(d) Countries subject to sanctions, embargoes or similar measures issued by international organisations such as the United Nations Organisation; and
(e) Countries identified by credible sources as having weak governance, law enforcement, and regulatory regimes, including countries identified by the FATF statements as having weak AML/CFT/CPF regimes, and for which financial institutions should give special attention to business relationships and transactions.

FC-C.2 Risk Assessment (Continued)

Customer/Investor risk

FC-C.2.6 Categories of customers which may indicate a higher risk include:

(a) The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer).
(b) Non-resident customers;
(c) Legal persons or arrangements that are personal asset-holding vehicles;
(d) Companies that have nominee shareholders or shares in bearer form;
(e) Businesses that are cash-intensive;
(f) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
(g) Customer is sanctioned by the relevant national competent authority for non-compliance with the applicable AML/CFT/CPF regime and is not engaging in remediation to improve its compliance;
(h) Customer is a PEP or customer's family members, or close associates are PEPs (including where a beneficial owner of a customer is a PEP);
(i) Customer resides in or whose primary source of income originates from high-risk jurisdictions;
(j) Customer resides in countries considered to be uncooperative in providing beneficial ownership information; customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for AML/CFT/CPF or to financial crimes;
(k) Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities;
(l) Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business;
(m) The number of STRs and their potential concentration on particular client groups;
(n) Customers who have sanction exposure; and
(o) Customer has a non-transparent ownership structure.

Product/Service/Transactions risk

FC-C.2.7 An overall risk assessment should include determining the potential risks presented by product, service, transaction or the delivery channel of the conventional bank licensee. A licensee should assess, using a RBA, the extent to which the offering of its product, service, transaction or the delivery channel presents potential vulnerabilities to placement, layering or integration of criminal proceeds into the financial system.

FC-C.2 Risk Assessment (Continued)

FC-C.2.8 Determining the risks of product, service, transaction or the delivery channel offered to customers may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:

(a) Private banking;
(b) Anonymous transactions (which may include cash);
(c) Non-face-to-face business relationships or transactions;
(d) Payment received from unknown or un-associated third parties;
(e) Products or services that may inherently favour anonymity or obscure information about underlying customer transactions;
(f) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions;
(g) Products with unusual complexity or structure and with no obvious economic purpose;
(h) Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction; and
(i) Use of new technologies or payment methods not used in the normal course of business by the conventional bank licensee.

Distribution Channel Risk

FC-C.2.9 A customer may request transactions that pose an inherently higher risk to the conventional bank licensee. Factors that may be considered as indicators of higher risk include:

(a) A request is made to transfer funds to a higher risk jurisdiction/country/region without a reasonable business purpose provided; and
(b) A transaction is requested to be executed, where the licensee is made aware that the transaction will be cleared/settled through an unregulated entity.

FC-C.2.10 A conventional bank licensee should analyse the specific risk factors, which arise from the use of intermediaries and their services. Intermediaries' involvement may vary with respect to the activity they undertake and their relationship with the licensees. Licensees should understand who the intermediary is and perform a risk assessment on the intermediary prior to establishing a business relationship. Licensees and intermediaries should establish clearly their respective responsibilities for compliance with applicable regulation.

MODULE	FC:	Financial Crime
CHAPTER	FC-1:	Customer Due Diligence Requirements

FC-1.1 General Requirements

Verification of Identity and Source of Funds

FC-1.1.1 Conventional bank licensees must establish effective systematic internal procedures for establishing and verifying the identity of their customers and the source of their funds. Such procedures must be set out in writing and approved by the licensee's senior management and must be strictly adhered to.

FC-1.1.2 Conventional bank licensees must implement the customer due diligence measures outlined in Chapters 1, 2 and 3 when:

(a) Establishing business relations with a new or existing customer;
(b) A change to the signatory or beneficiary of an existing account or business relationship is made;
(c) A significant transaction takes place;
(d) There is a material change in the way that the bank account is operated or in the manner in which the business relationship is conducted;
(e) Customer documentation standards change substantially;
(f) The conventional bank licensee has doubts about the veracity or adequacy of previously obtained customer due diligence information;
(g) [This Sub-paragraph was deleted in July 2018];
(h) Carrying out wire transfers irrespective of amount; or
(i) There is a suspicion of money laundering or terrorist financing.

FC-1.1.2A Conventional bank licensees must understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship.

FC-1.1.2B Conventional bank licensees must conduct ongoing due diligence on the business relationship, including:

a) Scrutinizing transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds; and.

FC-1.1 General Requirements (continued)

b) Ensuring that documents, data or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

FC-1.1.2C **A conventional bank licensee must also review and update the customers' risk profile based on their level of ML/TF/PF risk upon onboarding and regularly throughout the life of the relationship. The risk management and mitigation measures implemented by a licensee must be commensurate with the risk profile of the customer or type of customer.**

FC-1.1.3 For the purposes of this Module, 'customer' includes counterparties such as financial markets counterparties, except where financial institutions are acting as principals where simplified due diligence measures may sometimes apply. These simplified measures are set out in Section FC 1.11.

FC-1.1.4 The CBB's specific minimum standards to be followed with respect to verifying customer identity and source of funds are contained in Section FC-1.2. Enhanced requirements apply under certain high-risk situations: these requirements are contained in Sections FC-1.3 to FC-1.8 inclusive. Additional requirements apply where a conventional bank licensee is relying on a professional intermediary to perform certain parts of the customer due diligence process: these are detailed in Section FC-1.9. Simplified customer due diligence measures may apply in defined circumstances: these are set out in Section FC-1.11.

Verification of Third Parties

FC-1.1.5 **Conventional bank licensees must obtain a signed statement, in hard copy or through digital means from all new customers confirming whether or not the customer is acting on his own behalf or not. This undertaking must be obtained prior to conducting any transactions with the customer concerned.**

FC-1.1.6 **Where a customer is acting on behalf of a third party, the conventional bank licensee must also obtain a signed statement from the third party, confirming they have given authority to the customer to act on their behalf. Where the third party is a legal person, the conventional bank licensee must have sight of the original Board resolution (or other applicable document) authorising the customer to act on the third party's behalf, and retain a certified copy.**

FC-1.1 General Requirements (continued)

FC-1.1.7 Conventional bank licensees must establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting, including the Beneficial Owner of the funds. Verification must take place in accordance with the requirements specified in this Chapter.

FC-1.1.8 Where financial services are provided to a minor or other person lacking full legal capacity, the normal identification procedures as set out in this Chapter must be followed. In the case of minors, licensees must additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open an account, the licensee must establish the identity of that third party as well as the intended account holder.

Anonymous and Nominee Accounts

FC-1.1.9 Conventional bank licensees must not establish or keep anonymous accounts or accounts in fictitious names. Where conventional bank licensees maintain a nominee account, which is controlled by or held for the benefit of another person, the identity of that person must be disclosed to the conventional bank licensee and verified by it in accordance with the requirements specified in this Chapter.

Timing of Verification – Companies under Formation or New Arrivals

FC-1.1.10 Conventional bank licensees must not commence a business relationship or undertake a transaction with a customer before completion of the relevant customer due diligence measures specified in Chapters 1, 2 and 3. Licensees must also adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification. However, verification may be completed after receipt of funds in the case of: Bahrain companies under formation which are being registered with the Ministry of Industry, Commerce and Tourism; or newly arrived persons in Bahrain who are taking up employment or residence; or non-face-to-face business, or the subsequent submission of CDD documents by the customer after undertaking initial customer due diligence provided that no disbursement of funds takes place in any of the above cases until after the requirements of these Chapters have been fully met.

FC-1.1 General Requirements (continued)

Incomplete Customer Due Diligence

FC-1.1.11 **Where a conventional bank licensee is unable to comply with the requirements specified in Chapters 1, 2 and 3, it must consider whether: it should freeze any funds received and file a suspicious transaction report; or to terminate the relationship; or not proceed with the transaction; or to return the funds to the counterparty in the same method as received.**

FC-1.1.12 See also Chapter FC-5, which covers the filing of suspicious transaction reports. Regarding the return of funds to the counterparty, if funds are received in cash, funds should be returned in cash. If funds are received by wire transfer, they should be returned by wire transfer.

Non-Resident Accounts

FC-1.1.12A **Conventional retail bank licensees that open bank accounts or otherwise transact or deal with non-resident customers must have documented criteria for acceptance of business from such persons. For non-resident customers, conventional retail bank licensees must ensure the following:**

(a) Ensure there is a viable economic reason for the business relationship;
(b) Perform enhanced due diligence;
(c) Obtain and document the country of residence for tax purposes where relevant;
(d) Obtain evidence of banking relationships in the country of residence;
(e) Obtain the reasons for dealing with licensee in Bahrain;
(f) Obtain an indicative transaction volume and/or value of incoming funds; and
(g) Test that the persons are contactable without unreasonable delays.

FC-1.1.12B **Conventional retail bank licensees that open bank accounts or otherwise transact or deal with non-resident customers must have documented approved policies in place setting out the products and services which will be offered to non-resident customers. Such policy document must take into account a comprehensive risk assessment covering all risks associated with the products and services offered to non-residents. The licensee must also have detailed procedures to address the risks associated with the dealings with non-resident customers including procedures and processes relating to authentication, genuineness of transactions and their purpose.**

FC-1.1 General Requirements (continued)

FC-1.1.12C Conventional bank licensees must not accept non-residents customers from high risk jurisdictions subject to a call for action by FATF.

FC-1.1.12D Conventional bank licensees must take adequate precautions and risk mitigation measures before onboarding non-resident customers from high risk jurisdictions. The licensees must establish detailed assessments and criteria that take into consideration FATF mutual evaluations, FATF guidance, the country national risk assessments (NRAs) and other available guidance on onboarding and retaining non-resident customers from the following high risk jurisdictions:

a) Jurisdictions under increased monitoring by FATF;
b) Countries upon which United Nations sanctions have been imposed except those referred to in Paragraph FC-1.1.12C; and
c) Countries that are the subject of any other sanctions.

FC-1.1.12E Conventional retail bank licensees that deal with non-resident customers, other than with financial institutions, listed companies and governmental authorities in FATF countries referred to in FC-1.11.1, must perform enhanced due diligence for all its non-resident customers before establishing the account relationship and, thereafter, also perform enhanced transaction monitoring throughout the course of the relationship with all non-resident customers.

FC-1.1.12F All conventional bank licensees must establish systems and measures that are proportional to the risk relevant to each jurisdiction and this must be documented. Such a document must show the risks, mitigation measures for each jurisdiction and for each non-resident customer.

FC-1.1.12G All conventional bank licensees must establish a comprehensive documented policy and procedures describing also the tools, methodology and systems that support the licensee's processes for:

(a) The application of RBA;
(b) Customer due diligence;
(c) Ongoing transaction monitoring; and
(d) Reporting in relation to their transactions or dealings with non-resident customers.

FC-1.1.12H Conventional bank licensees must ensure that only official/government documents are accepted for the purpose of information in Subparagraphs FC-1.2.1 (a) to (f) in the case of non-resident customers.

FC-1.1 General Requirements (continued)

FC-1.1.13 **Where a non-resident customer intends to take up employment or to do business in Bahrain and has not completed residence permit and registration requirements and is currently awaiting receipt of his formal Bahraini identification documents, the licensee must open an account if requested by such customer, unless it has serious reasons to decline opening the account.**

FC-1.1.13A In complying with the requirements of Paragraph FC-1.1.13, examples of serious reasons for denying the request for opening an account may include failure to provide a valid passport. It may also include instances where a potential customer's conduct or activity appears suspicious or the customer's name appears in one of the local, regional or international sanction lists.

FC-1.1.13B **Where a company under formation in the Kingdom of Bahrain, which presents formal documents providing evidence that it has applied for and is awaiting its final commercial registration (CR), requests to open an account at a retail bank in Bahrain, the bank must open the requested account unless it has serious reasons to decline.**

FC-1.1.13C In complying with the requirements of Paragraph FC-1.1.13B, examples of serious reasons for denying the request for opening an account may include instances where a potential customer's conduct or activity appears suspicious or one of the principal's (shareholder or management) or the company under formation appears in one of the local, regional or international sanction lists.

FC-1.1.13D Retail banks shall continue to open accounts for companies under formation, which have been granted a commercial registration but not yet completed all other formalities.

FC-1.1.13E In order for the companies to operate the accounts, they shall be required to complete the KYC and other establishment requirements within a period of six months from the date of opening the account. The period of six months shall be extendable subject to a bilateral understanding between the two parties, taking into account the official required procedures of obtaining the license.

FC-1.1 General Requirements (continued)

FC-1.1.13F If the company under formation did not complete the license formalities nor submitted all required KYC documents to the subject bank within the agreed period and the company is not cooperating with the bank, the account of the company must be classified as dormant.

FC-1.1.13G **Retail banks must notify the Ministry of Industry, Commerce and Tourism when the account of companies under formation is classified as dormant and/or when the initial capital is withdrawn.**

FC-1.1.13H Closure of the accounts thereafter shall be subject to the discretion of the bank.

FC-1.1.14 **Accounts opened for customers residing outside Bahrain, are subject to the enhanced customer due diligence measures outlined in Section FC-1.3. Licensees must not open accounts for natural persons residing outside the GCC through a digital onboarding process, excluding Golden Visa holders.**

FC-1.1.14A **Notwithstanding the requirement in Paragraph FC-1.1.14, conventional bank licensees may open accounts for Bahraini nationals not physically present in Bahrain through a digital onboarding process using the National E-KYC system, taking into consideration the risk-based approach requirements set out in Chapter FC-C and non-resident requirements set out in Paragraphs FC-1.1.12A to FC-1.1.12H.**

FC-1.1.14B Licensees may open accounts for non-resident customers with Golden Visa taking into consideration the non-resident requirements set out in Paragraphs FC-1.1.12A to FC-1.1.12H.

FC-1.1.15 **Where a non-resident account is opened, the customer must be informed by the conventional bank licensee of any services which may be restricted or otherwise limited, as a result of their non-resident status.**

FC-1.1.16 For purposes of Paragraph FC-1.1.15, examples of limitations or restrictions for non-resident accounts may include limitations on banking services being offered including the granting of loans or other facilities, including credit cards or cheque books.

FC-1.2 Face-to-face Business

Natural Persons

FC-1.2.1 **If the customer is a natural person, conventional bank licensees must identify the person's identity and obtain the following information before providing financial services of any kind:**

(a) Full legal name and any other names used;
(b) Full permanent address (i.e. the residential address of the customer; a post office box is insufficient);
(c) Date and place of birth;
(d) Nationality;
(e) Passport number (if the customer is a passport holder);
(f) Current CPR or Iqama number (for residents of Bahrain or GCC states) or government issued national identification proof;
(g) Telephone/fax number and email address (where applicable);
(h) Occupation or public position held (where applicable);
(i) Employer's name and address (if self-employed, the nature of the self-employment);
(j) Type of account, and nature and volume of anticipated business dealings with the conventional bank licensee;
(k) Signature of the customer(s);
(l) Source of funds; and
(m) Reason for opening the account.

FC-1.2.1A **Conventional bank licensees obtaining the information and customer signature electronically using digital applications must comply with the applicable laws governing the onboarding/business relationship including but not limited to the Electronic Transactions Law (Law No. 54 of 2018) for the purposes of obtaining signatures as required in Subparagraph FC-1.2.1 (k) above.**

FC-1.2.2 See Part B, Volume 1 (Conventional Banks), for Guidance Notes on source of funds (FC-1.2.1 (1)) and requirements for residents of Bahrain (FC-1.2.1 (c) & (f)).

FC-1.2 Face-to-face Business (continued)

FC-1.2.2A Conventional retail bank licensees must verify the information in Paragraph FC-1.2.1 (a) to (f) by the following methods; at least one of the copies of the identification documents mentioned in (a) and (b) below must include a clear photograph of the customer:

(a) Confirmation of the date of birth and legal name, by use of the national E-KYC application and if this is not practical, obtaining a copy of a current valid official original identification document (e.g. birth certificate, passport, national identity card, CPR or Iqama); and

(b) Confirmation of the permanent residential address by use of the national E-KYC application and if this is not practical, obtaining a copy of a recent utility bill, bank statement or similar statement from another licensee or financial institution, or some form of official correspondence or official documentation card, such as national identity card or CPR, from a public/governmental authority, or a tenancy agreement or record of home visit by an official of the conventional bank licensee.

FC-1.2.3 Conventional wholesale bank licensees must verify the information in Paragraph FC-1.2.1 (a) to (f) by the following method; at least one of the copies of the identification documents mentioned in (a) and (b) below must include a clear photograph of the customer:

(a) Confirmation of the date of birth and legal name, by taking a copy of a current valid official original identification document (e.g. birth certificate, passport, national identity card, CPR or Iqama);

(b) Confirmation of the permanent residential address by a copy of a recent utility bill, bank statement or similar statement from another licensee or financial institution, or some form of official correspondence or official documentation card, such as national identity card or CPR, from a public/governmental authority, or a tenancy agreement or record of home visit by an official of the conventional bank licensee; and

(c) Where appropriate, direct contact with the customer by phone, letter or email to confirm relevant information, such as residential address information.

FC-1.2 Face-to-face Business (continued)

FC-1.2.4 Any document copied or obtained for the purpose of identification verification in a face-to-face customer due diligence process must be an original. An authorised official of the licensee must certify the copy, by writing on it the words 'original sighted', together with the date and his signature. Equivalent measures must be taken for electronic copies.

FC-1.2.5 Identity documents which are not obtained by an authorised official of the licensee in original form (e.g. due to a customer sending a copy by post following an initial meeting) must instead be certified (as per FC-1.2.4) by one of the following from a GCC or FATF member state:

(a) A lawyer;
(b) A notary;
(c) A chartered/certified accountant;
(d) An official of a government ministry;
(e) An official of an embassy or consulate; or
(f) An official of another licensed financial institution or of an associate company of the licensee.

FC-1.2 Face-to-face Business (continued)

FC-1.2.6 The individual making the certification under FC-1.2.5 must give clear contact details (e.g. by attaching a business card or company stamp). The conventional bank licensee must verify the identity of the person providing the certification through checking membership of a professional organisation (for lawyers or accountants), or through checking against databases/websites, or by direct phone or email contact.

Legal Entities or Legal Arrangements (such as trusts)

FC-1.2.7 If the customer is a legal entity or a legal arrangement such as a trust, the conventional bank licensee must obtain and record the following information from original identification documents, databases or websites, in hard copy or electronic form, to identify the customer and to take reasonable measures to verify its identity, legal existence and structure:

(a) The entity's full name and other trading names used;
(b) Registration number (or equivalent);
(c) Legal form and proof of existence;
(d) Registered address and trading address (where applicable);
(e) Type of business activity;
(f) Date and place of incorporation or establishment;
(g) Telephone, fax number and email address;
(h) Regulatory body or listing body (for regulated activities such as financial services and listed companies);
(hh) The names of the relevant persons having a senior management position in the legal entity or legal arrangement;
(i) Name of external auditor (where applicable);
(j) Type of account, and nature and volume of anticipated business dealings with the conventional bank licensee; and
(k) Source of funds.

FC-1.2 Face-to-face Business (continued)

FC-1.2.8 The information provided under FC-1.2.7 must be verified by obtaining certified copies of the following documents, as applicable (depending on the legal form of the entity):

(a) Certificate of incorporation and/or certificate of commercial registration or trust deed;
(b) Memorandum of association;
(c) Articles of association;
(d) Partnership agreement;
(e) Board resolution seeking the banking services (only necessary in the case of private or unlisted companies);
(f) Identification documentation of the authorised signatories to the account (certification not necessary for companies listed in a GCC/FATF state);
(g) Copy of the latest financial report and accounts, audited where possible (audited copies do not need to be certified); and
(h) List of authorised signatories of the company for the account and a Board resolution (or other applicable document) authorising the named signatories or their agent to operate the account (resolution only necessary for private or unlisted companies).

FC-1.2.8A For customers that are legal persons, conventional bank licensees must identify and take reasonable measures to verify the identity of beneficial owners through the following information:

(a) The identity of the natural person(s) who ultimately have a controlling ownership interest in a legal person, and
(b) To the extent that there is doubt under (a) as to whether the person(s) with the controlling ownership interest is the beneficial owner(s), or where no natural person exerts control of the legal person or arrangement through other means; and

FC-1.2 Face-to-face Business (continued)

(c) Where no natural person is identified under (a) or (b) above, the identity of the relevant natural person who holds the position of senior managing official.

FC-1.2.9 **Documents obtained to satisfy the requirements in FC-1.2.8 above must be certified in the manner specified in FC-1.2.4 to FC-1.2.6.**

FC-1.2.9A For the purpose of Paragraph FC-1.2.8(a), the requirement to obtain a certified copy of the commercial registration, may be satisfied by obtaining a commercial registration abstract printed directly from the Ministry of Industry, Commerce and Tourism's website, through "SIJILAT Commercial Registration Portal".

FC-1.2.10 The documentary requirements in FC-1.2.8 above do not apply in the case of FATF/GCC listed companies: see Section FC-1.11 below. Also, the documents listed in FC-1.2.8 above are not exhaustive: for customers from overseas jurisdictions, documents of an equivalent nature may be produced as satisfactory evidence of a customer's identity.

FC-1.2.11 **Licensees must also obtain and document the following due diligence information. These due diligence requirements must be incorporated in the licensee's new business procedures:**

(a) Enquire as to the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and the ultimate controller of the funds (if different);

(b) Ascertain whether the legal entity has been or is in the process of being wound up, dissolved, struck off or terminated;

(c) Obtain the names, country of residence and nationality of Directors or partners (only necessary for private or unlisted companies);

(d) Require, through new customer documentation or other transparent means, updates on significant changes to corporate ownership and/or legal structure;

(e) Obtain and verify the identity of shareholders holding 20% or more of the issued capital (where applicable). The requirement to verify the identity of these shareholders does not apply in the case of FATF/GCC listed companies;

FC-1.2 Face-to-face Business (continued)

(f) In the case of trusts or similar arrangements, establish the identity of the settler(s), trustee(s), and beneficiaries (including making such reasonable enquiries as to ascertain the identity of any other potential beneficiary, in addition to the named beneficiaries of the trust); and

(g) Where a licensee has reasonable grounds for questioning the authenticity of the information supplied by a customer, conduct additional due diligence to confirm the above information.

FC-1.2.12 For the purposes of Paragraph FC-1.2.11, acceptable means of undertaking such due diligence might include taking bank references; visiting or contacting the company by telephone; undertaking a company search or other commercial enquiries; accessing public and private databases (such as stock exchange lists); making enquiries through a business information service or credit bureau; confirming a company's status with an appropriate legal or accounting firm; or undertaking other enquiries that are commercially reasonable.

FC-1.2.13 Where a licensee is providing investment management services to a regulated mutual fund, and is not receiving investors' funds being paid into the fund, it may limit its CDD to confirming that the administrator of the fund is subject to FATF-equivalent customer due diligence measures (see FC-1.9 for applicable measures). Where there are reasonable grounds for believing that investors' funds being paid into the fund are not being adequately verified by the administrator, then the licensee should consider terminating its relationship with the fund.

FC-1.3 Enhanced Customer Due Diligence: General Requirements

FC-1.3.1 **Enhanced customer due diligence must be performed on those customers identified as having a higher risk profile, and additional inquiries made or information obtained in respect of those customers.**

FC-1.3.2 Licensees should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of money laundering or terrorist financing are higher, licensees should conduct enhanced CDD measures, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. The additional inquiries or information referred to in Paragraph FC-1.3.1 include:

(a) Obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;
(b) Obtaining additional information on the intended nature of the business relationship;
(c) Obtaining information on the source of funds or source of wealth of the customer;
(d) Obtaining information on the reasons for intended or performed transactions;
(e) Obtaining the approval of senior management to commence or continue the business relationship;
(f) Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
(g) Taking specific measures to identify the source of the first payment in this account and applying RBA to ensure that there is a plausible explanation in any case where the first payment was not received from the same customer's account;
(h) Obtaining evidence of a person's permanent address through the use of a credit reference agency search, or through independent governmental database or by home visit;
(i) Obtaining a personal reference (e.g. by an existing customer of the conventional bank licensee);
(j) Obtaining another licensed entity's reference and contact with the concerned licensee regarding the customer;
(k) Obtaining documentation outlining the customer's source of wealth;
(l) Obtaining additional documentation outlining the customer's source of income; and
(m) Obtaining additional independent verification of employment or public position held.

FC-1.3.3 In addition to the general rule contained in Paragraph FC-1.3.1 above, special care is required in the circumstances specified in Sections FC-1.4 to FC-1.9 inclusive.

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies

FC-1.3.4 Additional enhanced due diligence measures for non-resident account holders may include the following:

(a) References provided by a regulated bank from a FATF country;
(b) Certified copies of bank statements for a recent 3-month period; or
(c) References provided by a known customer of the conventional bank licensee.

FC-1.4.1 **Conventional bank licensees must establish specific procedures for verifying customer identity where no face-to-face contact takes place.**

FC-1.4.2 **Where no face-to-face contact takes place, conventional bank licensees must take additional measures (to those specified in Section FC-1.2), in order to mitigate the potentially higher risk associated with such business. In particular, conventional bank licensees must take measures:**

(a) To ensure that the customer is the person they claim to be; and
(b) To ensure that the address provided is genuinely the customer's.

FC-1.4.3 There are a number of checks that can provide a conventional bank licensee with a reasonable degree of assurance as to the authenticity of the applicant. They include:

(a) Telephone contact with the applicant on an independently verified home or business number;
(b) With the customer's consent, contacting an employer to confirm employment, via phone through a listed number or in writing;
(c) Salary details appearing on recent bank statements;
(d) Independent verification of employment (e.g.: through the use of a national E-KYC application, or public position held;
(e) Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile;
(f) Carrying out additional searches focused on financial crime risk indicator (i.e. negative news);
(g) Evaluating the information provided with regard to the destination of fund and the reasons for the transaction;
(h) Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship; and
(i) Increasing the frequency and intensity of transaction monitoring.

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies (continued)

New Technologies

FC-1.4.4 **Financial services provided using digital channels or internet pose greater challenges for customer identification and AML/CFT purposes. Conventional bank licensees must identify and assess the money laundering or terrorist financing risks relevant to any new technology or channel and establish procedures to prevent the misuse of technological developments in money laundering or terrorist financing schemes. Specifically, licensees which provide electronic and internet banking services to their customers, must establish systems or programmes to monitor, detect and highlight unusual transactions. The risk assessments must be consistent with the requirements in Section FC-C-2.**

FC-1.4.5 **Conventional bank licensees must identify and assess the money laundering or terrorist financing risks that may arise in relation to:**

(a) The development of new products and new business practices, including new delivery mechanisms; and

(b) The use of new or developing technologies for both new and pre-existing products.

FC-1.4.6 **For purposes of Paragraph FC-1.4.5, such a risk assessment consistent with the requirements in Section FC-C.2 and must take place prior to the launch of the new products, business practices or the use of new or developing technologies. Conventional bank licensees must take appropriate measures to manage and mitigate those risks.**

Enhanced Monitoring

FC-1.4.7 **Customers on boarded digitally must be subject to enhanced on-going account monitoring measures.**

FC-1.4.8 The CBB may require a licensee to share the details of the enhanced monitoring and the on-going monitoring process for non face-to-face customer relationships.

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies (continued)

Licensee's digital ID applications

FC-1.4.9 Conventional bank licensees may use its digital ID applications that use secure audio-visual real time (live video conferencing/live photo selfies) communication means to identify the natural person.

FC-1.4.10 Conventional bank licensees must maintain a document available upon request for the use of its digital ID applications that includes all the following information:

(a) A description of the nature of products and services for which the proprietary digital ID application is planned to be used with specific references to the rules in this Module for which it will be used;
(b) A description of the systems and IT infrastructure that are planned to be used;
(c) A description of the technology and applications that have the features for facial recognition or biometric recognition to authenticate independently and match the face and the customer identification information available with the licensee. The process and the features used in conjunction with video conferencing include, among others, face recognition, three-dimensional face matching techniques etc.;
(d) "Liveness" checks created in the course of the identification process;
(e) A description of the governance arrangements related to this activity including the availability of specially trained personnel with sufficient level of seniority; and
(f) Record keeping arrangements for electronic records to be maintained and the relative audit.

FC-1.4.11 Conventional bank licensees that intend to use its digital ID application to identify the customer and verify identity information must meet the following additional requirements:

(a) The digital ID application must make use of secure audio visual real time (live video conferencing /live photo selfies) technology to (i) identify the customer, (ii) verify his/her identity, and also (iii) ensure the data and documents provided are authentic;
(b) The picture/sound quality must be adequate to facilitate unambiguous identification;
(c) The digital ID application must include or be combined with capability to read and decrypt the information stored in the identification document's machine readable zone (MRZ) for authenticity checks from independent and reliable sources;

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies (continued)

(d) Where the MRZ reader is with an outsourced provider, the licensee must ensure that such party is authorized to carry out such services and the information is current and up to date and readily available such that the licensee can check that the decrypted information matches the other information in the identification document;
(e) The digital ID application has the features for allowing facial recognition or biometric recognition that can authenticate and match the face and the customer identification documents independently;
(f) The digital ID solution has been tested by an independent expert covering the governance and control processes to ensure the integrity of the solution and underlying methodologies, technology and processes and risk mitigation. The report of the expert's findings must be retained and available upon request;
(g) The digital ID application must enable an ongoing process of retrieving and updating the digital files, identity attributes, or data fields which are subject to documented access rights and authorities for updating and changes; and
(h) The digital ID application must have the geo-location features which must be used by the licensee to ensure that it is able to identify any suspicious locations and to make additional inquiries if the location from which a customer is completing the onboarding process does not match the location of the customer based on the information and documentation submitted.

FC-1.4.12 Conventional bank licensees using its digital ID application must establish and implement an approved policy which lays down the governance, control mechanisms, systems and procedures for the CDD which include:
(a) A description of the nature of products and services for which customer due diligence may be conducted through video conferencing or equivalent electronic means;
(b) A description of the systems, controls and IT infrastructure planned to be used;
(c) Governance mechanism related to this activity;
(d) Specially trained personnel with sufficient level of seniority; and
(e) Record keeping arrangements for electronic records to be maintained and the relative audit trail.

FC-1.4.13 Conventional bank licensees must ensure that the information referred to in Paragraph FC-1.2.1 is collected in adherence to privacy laws and other applicable laws of the country of residence of the customer.

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies (continued)

FC-1.4.14 Conventional bank licensees must ensure that the information referred to in Subparagraphs FC-1.2.1 (a) to (f) is obtained prior to commencing the digital verification such that:

(a) The licensee can perform its due diligence prior to the digital interaction/communication and can raise targeted questions at such interaction/communication session; and

(b) The licensee can verify the authenticity, validity and accuracy of such information through digital means (See Paragraph FC.1.4.16 below) or by use of the methods mentioned in Paragraph FC-1.2.3 and /or FC-1.4.3 as appropriate.

FC-1.4.15 The licensee must also obtain the customer's explicit consent to record the session and capture images as may be needed.

FC-1.4.16 Conventional bank licensees must verify the information in Paragraph FC-1.2.1 (a) to (f) by the following methods below:

(a) Confirmation of the date of birth and legal name by digital reading and authenticating current valid passport or other official original identification using machine readable zone (MRZ) or other technology which has been approved under paragraph FC-1.4.9, unless the information was verified using national E-KYC application;

(b) Performing real time video calls with the applicant to identify the person and match the person's face and /other features through facial recognition or bio-metric means with the office documentation, (e.g. passport, CPR);

(c) Matching the official identification document, (e.g. passport, CPR) and related information provided with the document captured/displayed on the live video call; and

(d) Confirmation of the permanent residential address by, unless the information was verified using national E-KYC application capturing live, the recent utility bill, bank statement or similar statement from another licensee or financial institution, or some form of official correspondence or official documentation card, such as national identity card or CPR, from a public/governmental authority, or a tenancy agreement or record of home visit by an official of the conventional bank licensee.

FC-1.4 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies (continued)

FC-1.4.17 For the purposes of Paragraph FC-1.4.16, actions taken for obtaining and verifying customer identity could include:

(a) *Collection*: Present and collect identity attributes and evidence, either in person and/or online (e.g., by filling out an online form, sending a selfie photo, uploading photos of documents such as passport or driver's license, etc.);

(b) *Certification*: Digital or physical inspection to ensure the document is authentic and its data or information is accurate (for example, checking physical security features, expiration dates, and verifying attributes via other services);

(c) *De-duplication*: Establish that the identity attributes and evidence relate to a unique person in the ID system (e.g., via duplicate record searches, biometric recognition and/or deduplication algorithms);

(d) *Verification*: Link the individual to the identity evidence provided (e.g., using biometric solutions like facial recognition and liveness detection); and

(e) *Enrolment* in identity account and binding: Create the identity account and issue and link one or more authenticators with the identity account (e.g., passwords, one-time code (OTC) generator on a smartphone, etc.). This process enables authentication.

FC-1.4.18 Not all elements of a digital ID system are necessarily digital. Some elements of identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding and authentication must be digital.

FC-1.4.19 **Sufficient controls must be put in place to safeguard the data relating to customer information collected through the video conference and due regard must be paid to the requirements of the Personal Data Protection Law (PDPL). Additionally, controls must be put in place to minimize the increased impersonation fraud risk in such non face-to-face relationship where there is a chance that customer may not be who he claims he is.**

Overseas branches

FC-1.4.20 **Where conventional bank licensees intend to use a digital ID application in a foreign jurisdiction in which it operates, it must ensure that the digital ID application meets with the requirements under Paragraph FC-B.2.1.**

FC-1.5 Enhanced Customer Due Diligence: Politically Exposed Persons ('PEPs')

FC-1.5.1 **Conventional bank licensees must have appropriate risk management systems to determine whether a customer or beneficial owner is a Politically Exposed Person ('PEP'), both at the time of establishing business relations and thereafter on a periodic basis. Conventional bank licensees must utilise publicly available databases and information to establish whether a customer is a PEP.**

FC-1.5.2 **Conventional bank licensees must establish a client acceptance policy with regard to PEPs, taking into account the reputational and other risks involved. Senior management approval must be obtained before a PEP is accepted as a customer. Licensees must not accept a non-Bahraini PEP as a customer based on customer due diligence undertaken using digital ID applications.**

FC-1.5.3 **Where an existing customer is a PEP, or subsequently becomes a PEP, enhanced monitoring and customer due diligence measures must include:**

(a) Analysis of complex financial structures, including trusts, foundations or international business corporations;
(b) A written record in the customer file to establish that reasonable measures have been taken to establish both the source of wealth and the source of funds;
(c) Development of a profile of anticipated customer activity, to be used in on-going monitoring;
(d) Approval of senior management for allowing the customer relationship to continue; and
(e) On-going account monitoring of the PEP's account by senior management (such as the MLRO).

FC-1.5.3A **In cases of higher risk business relationships with such persons, mentioned in Paragraph FC-1.5.1, conventional bank licensees must apply, at a minimum, the measures referred to in (b), (d) and (e) of Paragraph FC-1.5.3.**

FC-1.5.3B **The requirements for all types of PEP must also apply to family or close associates of such PEPs.**

FC-1.5.3C For the purpose of Paragraph FC-1.5.3B, 'family' means spouse, father, mother, sons, daughters, sisters and brothers. 'Associates' are persons associated with a PEP whether such association is due to the person being an employee or partner of the PEP or of a firm represented or owned by the PEP, or family links or otherwise.

FC-1.5 Enhanced Customer Due Diligence: Politically Exposed Persons ('PEPs') (continued)

FC-1.5.4 [This Paragraph was deleted in July 2016 and the definition moved to the Glossary under Part B.].

FC-1.6 Enhanced Due Diligence: Charities, Clubs and Other Societies

FC-1.6.1 **Financial services must not be provided to charitable funds and religious, sporting, social, cooperative and professional and other societies, until an original certificate authenticated by the relevant Ministry confirming the identities of those purporting to act on their behalf (and authorising them to obtain the said service) has been obtained.**

FC-1.6.1A **For the purpose of Paragraph FC-1.6.1, for clubs and societies registered with the Ministry of Youth and Sport Affairs, Conventional bank licensees must contact the Ministry to clarify whether the account may be opened in accordance with the rules of the Ministry. In addition, in the case of sport associations registered with the Bahrain Olympic Committee (BOC), Conventional bank licensees must contact BOC to clarify whether the account may be opened in accordance with the rules of BOC.**

FC-1.6.2 Conventional bank licensees are reminded that clubs and societies registered with the Ministry of Youth and Sport Affairs may only have one account with banks in Bahrain.

FC-1.6.2A **Pursuant to Article (20) of the Consolidated Financial Regulations for Sports Clubs issued in 2005, Conventional bank licensees must not change or open additional bank accounts for Clubs and Youth Centres without obtaining the prior approval of the Ministry of Youth and Sport Affairs.**

FC-1.6.3 **Charities should be subject to enhanced transaction monitoring by banks. Conventional bank licensees should develop a profile of anticipated account activity (in terms of payee countries and recipient organisations in particular).**

FC-1.6.4 **Conventional bank licensees must provide a monthly report of all payments and transfers of BD3,000 (or equivalent in foreign currencies) and above, from accounts held by charities registered in Bahrain. The report must be submitted to the CBB's Compliance Directorate (see FC-5.3 for contact address), giving details of the amount transferred, account name, number and beneficiary name account and bank details. Conventional bank licensees must ensure that such transfers are in accordance with the spending plans of the charity (in terms of amount, recipient and country).**

FC-1.6 Enhanced Due Diligence: Charities, Clubs and Other Societies (continued)

FC-1.6.5 Article 20 of Decree Law No. 21 of 1989 (issuing the Law of Social and Cultural Societies and Clubs and Private Organizations Operating in the Area of Youth and Sport and Private Institutions) provides that Conventional bank licensees must not accept or process any incoming or outgoing fund transfers in any form (wire transfer, cheques, etc.) from or to any foreign association on behalf of charity and non-profit organisations, societies and clubs licensed by the Ministry of Labour and Social Development or the Ministry of Youth and Sport Affairs without the prior approval of the relevant Ministry.

FC-1.6.6 The receipt of a Ministry letter mentioned in FC-1.6.5 above does not exempt the concerned bank from conducting normal CDD measures as outlined in other parts of this Module.

FC-1.7 Enhanced Due Diligence: 'Pooled Funds'

FC-1.7.1 Where conventional bank licensees receive pooled funds managed by professional intermediaries (such as investment and pension fund managers, stockbrokers and lawyers or authorised money transferors), they must apply CDD measures contained in Section FC-1.9 to the professional intermediary. In addition, conventional bank licensees must verify the identity of the beneficial owners of the funds where required as shown in Paragraphs FC-1.7.2 or FC-1.7.3 below.

FC-1.7.2 Where funds pooled in an account are not co-mingled (i.e. where there are 'sub-accounts' attributable to each beneficiary), all beneficial owners must be identified by the conventional bank licensee, and their identity verified in accordance with the requirements in Section FC-1.2.

FC-1.7.3 For accounts held by intermediaries resident in Bahrain, where such funds are co-mingled, the conventional bank licensee must make a reasonable effort (in the context of the nature and amount of the funds received) to look beyond the intermediary and determine the identity of the beneficial owners or underlying clients, particularly where funds are banked and then transferred onward to other financial institutions (e.g. in the case of accounts held on behalf of authorised money transferors). Where, however, the intermediary is subject to equivalent regulatory and money laundering regulation and procedures (and, in particular, is subject to the same due diligence standards in respect of its client base) the CBB will not insist upon all beneficial owners being identified provided the conventional bank licensee has undertaken reasonable measures to determine that the intermediary has engaged in a sound customer due diligence process, consistent with the requirements in Section FC-1.8.

FC-1.7 Enhanced Due Diligence: 'Pooled Funds' (continued)

FC-1.7.4 For accounts held by intermediaries from foreign jurisdictions, the intermediary must be subject to requirements to combat money laundering and terrorist financing consistent with the FATF Recommendations and the intermediary must be supervised for compliance with those requirements. The bank must obtain documentary evidence to support the case for not carrying out customer due diligence measures beyond identifying the intermediary. The bank must satisfy itself that the intermediary has identified the underlying beneficiaries and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries. The due diligence process contained in Section FC-1.8 must be followed.

FC-1.7.5 Where the intermediary is not empowered to provide the required information on beneficial owners (e.g. lawyers bound by professional confidentiality rules) or where the intermediary is not subject to the same due diligence standards referred to above, a bank must not permit the intermediary to open an account or allow the account to continue to operate, unless specific permission has been obtained in writing from the CBB.

FC-1.8 Enhanced Due Diligence for Correspondent Banking Relationships

FC-1.8.1 Conventional bank licensees which intend to act as correspondent banks must gather sufficient information (e.g. through a questionnaire) about their respondent banks to understand the nature of the respondent's business. Factors to consider to provide assurance that satisfactory measures are in place at the respondent bank include:

(a) Information about the respondent bank's ownership structure and management;

(b) Major business activities of the respondent and its location (i.e. whether it is located in a FATF compliant jurisdiction) as well as the location of its parent (where applicable);

(c) Where the customers of the respondent bank are located;

(d) The respondent's AML/CFT controls;

(e) The purpose for which the account will be opened;

(f) Confirmation that the respondent bank has verified the identity of any third party entities that will have direct access to the correspondent banking services without reference to the respondent bank (e.g. in the case of 'payable through' accounts);

(g) The extent to which the respondent bank performs on-going due diligence on customers with direct access to the account, and the condition of bank regulation and supervision in the respondent's country (e.g. from published FATF reports). Banks should take into account the country where the respondent bank is located and whether that country abides by the FATF Recommendations when establishing correspondent relationships with foreign banks. Banks should obtain where possible copies of the relevant laws and regulations concerning AML/CFT and satisfy themselves that respondent banks have effective customer due diligence measures consistent with the FATF Recommendations;

FC-1.8 Enhanced Due Diligence: Correspondent Banking Relationships (continued)

(h) Confirmation that the respondent bank is able to provide relevant customer identification data on request to the correspondent bank; and

(i) Whether the respondent bank has been subject to a money laundering or terrorist financing investigation.

FC-1.8.2 Conventional bank licensees must implement the following additional measures, prior to opening a correspondent banking relationship:

(a) Complete a signed statement that outlines the respective responsibilities of each institution in relation to money laundering detection and monitoring responsibilities; and

(b) Ensure that the correspondent banking relationship has the approval of senior management.

FC-1.8.3 Conventional bank licensees must refuse to enter into or continue a correspondent banking relationship with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. 'shell banks', see Section FC-1.10). Banks must pay particular attention when entering into or continuing relationships with respondent banks located in jurisdictions that have poor KYC standards or have been identified by the FATF as being 'non-cooperative' in the fight against money laundering/terrorist financing.

MODULE	FC:	Financial Crime
CHAPTER	FC-1:	Customer Due Diligence Requirements

FC-1.9 Introduced Business from Professional Intermediaries

FC-1.9.1 A conventional bank licensee may only accept customers introduced to it by other financial institutions or intermediaries, if it has satisfied itself that the financial institution or intermediary concerned is subject to FATF-equivalent measures and customer due diligence measures. Where conventional bank licensees delegate part of the customer due diligence measures to another financial institution or intermediary, the responsibility for meeting the requirements of Chapters 1 and 2 remains with the conventional bank licensee, not the third party.

FC-1.9.2 Conventional bank licensees may only accept introduced business if all of the following conditions are satisfied:

(a) The customer due diligence measures applied by the introducer are consistent with those required by the FATF Recommendations;

(b) A formal agreement is in place defining the respective roles of the licensee and the introducer in relation to customer due diligence measures. The agreement must specify that the customer due diligence measures of the introducer will comply with the FATF Recommendations;

(c) The introducer immediately provides all necessary information required in Paragraph FC-1.2.1 or FC-1.2.7 and FC-1.1.2A pertaining to the customer's identity, the identity of the customer and beneficial owner of the funds (where different), the purpose of the relationship and, where applicable, the party/parties on whose behalf the customer is acting; also, the introducer has confirmed that the conventional bank licensee will be allowed to verify the customer due diligence measures undertaken by the introducer at any stage; and

(d) Written confirmation is provided by the introducer confirming that all customer due diligence measures required by the FATF Recommendations have been followed and the customer's identity established and verified. In addition, the confirmation must state that any identification documents or other customer due diligence material can be accessed by the conventional bank licensee and that these documents will be kept for at least five years after the business relationship has ended.

FC-1.9.3 The conventional bank licensee must perform periodic reviews ensuring that any introducer on which it relies is in compliance with the FATF Recommendations. Where the introducer is resident in another jurisdiction, the conventional bank licensee must also perform periodic reviews to verify whether the jurisdiction is in compliance with the FATF Recommendations.

FC-1.9 Introduced Business from Professional Intermediaries (continued)

FC-1.9.4 Should the conventional bank licensee not be satisfied that the introducer is in compliance with the requirements of the FATF Recommendations, the licensee must conduct its own customer due diligence on introduced business, or not accept further introductions, or discontinue the business relationship with the introducer.

FC-1.10 Shell Banks

FC-1.10.1 Conventional bank licensees must not establish business relations with banks, which have no physical presence or 'mind and management' in the jurisdiction in which they are licensed and which are unaffiliated with a regulated financial group ('shell banks'). Banks must not knowingly establish relations with banks that have relations with shell banks.

FC-1.10.2 Conventional bank licensees must make a suspicious transaction report to the Anti-Money Laundering Unit and the Compliance Directorate if they are approached by a shell bank or an institution they suspect of being a shell bank.

FC-1.10A Enhanced Due Diligence: Cross Border Cash Transactions by Courier

FC-1.10A.1 The cross-border movement of cash funds warrants special attention under the FATF Recommendations where transactions are large in value (Recommendation 12), in addition to the general requirement under Recommendation 32 to verify monitor, declare and keep records of all cross-border transfers of cash. Cash shipments are therefore subject to inspection and investigation procedures by the Customs Directorate of the Kingdom of Bahrain. There are also certain specific legal measures mentioned below which are relevant to cross-border cash shipments. Under Article 4 of Decree Law No. 4 of 2001, licensees of the CBB are required to comply with the CBB's Rules and Regulations concerning the prevention and prohibition of money laundering, which include regulations concerning the cross-border movement of cash. Also, licensees' attention is drawn to the disclosure provisions of Decree Law No 54 of 2006 and Ministerial Order No 6 of 2008 with respect to cross-border transportation of funds (see Part B of the Rulebook for Decree Law No 54). Licensees are also reminded of the rules of the unified customs arrangements of the Gulf Cooperation Council as laid out in Decree Law No 10 of 2002. With respect to the above Law No. 4 of 2001 and the concerned parts of other legislation mentioned above, all money changers must implement the enhanced measures below in respect of all cash received from foreign countries or sold/transferred to foreign countries.

FC-1.10A.2 **Cash coming into Bahrain via courier (whether a representative of a Bahrain money changer or a foreign institution) must be accompanied by original documentation stating the source of funds and identity of the originator of the funds. Furthermore, the documentation must state the full name and address of the beneficiary of the funds. This documentation must be signed in original by (a representative) of the originator of the cash. This means that where a courier is importing cash via any customs point of entry (e.g. via the Causeway or the Airport), the aforementioned courier must carry original documentation which clearly shows the source of funds and identity of the originator of the funds and the intended beneficiaries' names and address.**

FC-1.10A.3 **In the case of incoming cash, the courier must carry original documentation signed by the originator stating whether the cash shipment is for local use or for onward transmission.**

FC-1.10A Enhanced Due Diligence: Cross Border Cash Transactions Equal to and above BD6,000 by Courier (continued)

FC-1.10A.4 **If the imported cash is for onward transmission, the original documentation must provide the full name and address of the final beneficiaries, as well as the local recipient (e.g. the bank).**

FC-1.10A.5 Failure to provide complete and detailed original signed documentation by the originator of the funds referred to in Paragraph FC-1.10A.2 may cause the cash shipment to be blocked, whereupon the blocking costs will be borne by the concerned money changer in Bahrain. Licensees are also reminded of the penalties and enforcement measures in Law No. 4 of 2001, Decree Law No. 54 of 2006, Ministerial Order No. 7 of 2001 issued by the Minister of Finance and National Economy, the rules of the unified customs arrangements of the Gulf Cooperation Council as laid out in Decree Law No. 10 of 2002 and the CBB Law No. 64 of 2006.

FC-1.11 Simplified Customer Due Diligence

FC-1.11.1 Conventional bank licensees may apply simplified customer due diligence measures, as described in Paragraphs FC-1.11.2 to FC-1.11.7, if:

(a) The customer is the Central Bank of Bahrain ('CBB'), the Bahrain Bourse ('BHB') or a licensee of the CBB;

(b) The customer is a Ministry of a Gulf Cooperation Council ('GCC') or Financial Action Task Force ('FATF') member state government, a company in which a GCC or FATF government is a majority shareholder, or a company established by decree in the GCC;

(c) The customer is a company listed on a GCC or FATF member state stock exchange (where the FATF state stock exchange has equivalent disclosure standards to those of the BHB);

(d) The customer is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements;

(e) The customer is a financial institution which is a subsidiary of a financial institution located in a FATF or GCC member state, and the AML/CFT requirements applied to its parent also apply to the subsidiary;

(f) The customer is a borrower in a syndicated transaction where the agent bank is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements; or

(g) [This sub-paragraph was deleted in January 2018].

FC-1.11.2 For customers falling under categories a-f specified in Paragraph FC-1.11.1, the information required under Paragraph FC-1.2.1 (for natural persons) or FC-1.2.7 (for legal entities or legal arrangements such as trusts) must be obtained. However, the verification and certification requirements in Paragraphs FC-1.2.3 and FC-1.2.8, and the due diligence requirements in Paragraph FC-1.2.11, may be dispensed with. Where the account is a correspondent banking relationship, enhanced due diligence applies. Refer to Section FC-1.8.

FC-1.11 Simplified Customer Due Diligence (continued)

FC-1.11.3 [This Paragraph was deleted in July 2018.]

FC-1.11.4 **Conventional bank licensees wishing to apply simplified due diligence measures as allowed for under Paragraph FC-1.11.1 must retain documentary evidence supporting their categorisation of the customer.**

FC-1.11.5 Examples of such documentary evidence may include a printout from a regulator's website, confirming the licensed status of an institution, and internal papers attesting to a review of the AML/CFT measures applied in a jurisdiction.

FC-1.11.6 **Conventional bank licensees may use authenticated SWIFT messages as a basis for confirmation of the identity of a financial institution under FC-1.11.1 (d) and (e) where it is dealing as principal. For customers coming under Paragraph FC-1.11.1 (d) and (e), conventional bank licensees must also obtain and retain a written statement from the parent institution of the subsidiary concerned, confirming that the subsidiary is subject to the same AML/CFT measures as its parent.**

FC-1.11.7 **Simplified customer due diligence measures must not be applied where a conventional bank licensee knows, suspects, or has reason to suspect, that the applicant is engaged in money laundering or terrorism financing or that the transaction is carried out on behalf of another person engaged in money laundering or terrorism financing.**

FC-1.11.7A **Simplified customer due diligence measures must not be applied in situations where the licensee has identified high ML/TF/PF risks.**

FC-1.11.8 **[This Paragraph was deleted in July 2018.]**

FC-1.12 [This Section has been deleted and moved to the CBB Regulatory Sandbox Framework in January 2022]

FC-1.12.1 **[This Paragraph was deleted in January 2022].**

FC-1.12.2 **[This Paragraph was deleted in January 2022].**

FC-1.12.3 **[This Paragraph was deleted in January 2022].**

FC-1.12.4 **[This Paragraph was deleted in January 2022].**

FC-1.12.5 **[This Paragraph was deleted in January 2022].**

FC-1.12.6 **[This Paragraph was deleted in January 2022].**

FC-1.12.7 **[This Paragraph was deleted in January 2022].**

FC-1.12.8 [This Paragraph was deleted in January 2022].

FC-1.12.9 **[This Paragraph was deleted in January 2022].**

FC-1.12.10 **[This Paragraph was deleted in January 2022].**

FC-1.12.11 **[This Paragraph was deleted in January 2022].**

FC-1.12.12 **[This Paragraph was deleted in January 2022].**

FC-1.12.13 [This Paragraph was deleted in January 2022].

FC-1.12.14 **[This Paragraph was deleted in January 2022].**

FC-2.1 General Requirements

FC-2.1.1 **Conventional bank licensees must implement programmes against money laundering and terrorist financing which establish and maintain appropriate systems and controls for compliance with the requirements of this Module and which limit their vulnerability to financial crime. These systems and controls must be documented, and approved and reviewed annually by the Board of the licensee. The documentation, and the Board's review and approval, must be made available upon request to the CBB.**

FC-2.1.2 The above systems and controls, and associated documented policies and procedures, should cover standards for customer acceptance, on-going monitoring of high-risk accounts, staff training and adequate screening procedures to ensure high standards when hiring employees.

FC-2.1.3 **Conventional bank licensees must incorporate Key Performance Indicators (KPIs) to ensure compliance with AML/CFT requirements by all staff. The performance against the KPIs must be adequately reflected in their annual performance evaluation and in their remuneration (See also Paragraph HC-5.4.9A).**

FC-2.1.4 In implementing the policies, procedures and monitoring tools for ensuring compliance with Paragraph FC-2.1.3, conventional bank licensees should consider the following:

(a) The business policies and practices should be designed to reduce incentives for staff to expose the conventional bank licensee to AML/CFT compliance risk;
(b) The performance measures of departments/divisions/units and personnel should include measures to address AML/CFT compliance obligations;
(c) AML/CFT compliance breaches and deficiencies should be attributed to the relevant departments/divisions/units and personnel within the organisation as appropriate;
(d) Remuneration and bonuses should be adjusted for AML/CFT compliance breaches and deficiencies; and
(e) Both quantitative measures and human judgement should play a role in determining any adjustments to the remuneration and bonuses resulting from the above.

FC-2.2 On-going Customer Due Diligence and Transaction Monitoring

Risk Based Monitoring

FC-2.2.1 **Conventional bank licensees must develop risk-based monitoring systems appropriate to the complexity of their business, their number of clients and types of transactions. These systems must be configured to identify significant or abnormal transactions or patterns of activity. Such systems must include limits on the number, types or size of transactions undertaken outside expected norms; and must include limits for cash and non-cash transactions.**

FC-2.2.2 Conventional bank licensees' risk-based monitoring systems should therefore be configured to help identify:

(a) Transactions which do not appear to have a clear purpose or which make no obvious economic sense;

(b) Significant or large transactions not consistent with the normal or expected behaviour of a customer; and

(c) Unusual patterns of activity (relative to other customers of the same profile or of similar types of transactions, for instance because of differences in terms of volumes, transaction type, or flows to or from certain countries), or activity outside the expected or regular pattern of a customer's account activity.

Automated Transaction Monitoring

FC-2.2.3 **Conventional bank licensees must consider the need to include automated transaction monitoring as part of their risk-based monitoring systems to spot abnormal or unusual flows of funds. In the absence of automated transaction monitoring systems, all transactions above BD 6,000 must be viewed as 'significant' and be captured in a daily transactions report for monitoring by the MLRO or a relevant delegated official, and records retained by the conventional bank licensee for five years after the date of the transaction.**

FC-2.2.4 CBB would expect larger conventional bank licensees to include automated transaction monitoring as part of their risk-based monitoring systems. See also Chapters FC-4 and FC-7, regarding the responsibilities of the MLRO and record-keeping requirements.

FC-2.2 On-going Customer Due Diligence and Transaction Monitoring (continued)

Unusual Transactions or Customer Behaviour

FC-2.2.5 **Where a conventional bank licensee's risk-based monitoring systems identify significant or abnormal transactions (as defined in FC-2.2.2 and FC-2.2.3), it must verify the source of funds for those transactions, particularly where the transactions are above the transactions threshold of BD 6,000. Furthermore, conventional bank licensees must examine the background and purpose to those transactions and document their findings.**

FC-2.2.6 **The investigations required under FC-2.2.5 must be carried out by the MLRO (or relevant delegated official). The documents relating to these findings must be maintained for five years from the date when the transaction was completed (see also FC-7.1.1 (b)).**

FC-2.2.7 **Conventional bank licensees must consider instances where there is a significant, unexpected or unexplained change in customer activity.**

FC-2.2.8 **When an existing customer closes one account and opens another, the conventional bank licensee must review its customer identity information and update its records accordingly. Where the information available falls short of the requirements contained in Chapter FC-1, the missing or out of date information must be obtained and re-verified with the customer.**

FC-2.2.9 Once identification procedures have been satisfactorily completed and, as long as records concerning the customer are maintained in line with Chapters FC-1 and FC-7, no further evidence of identity is needed when transactions are subsequently undertaken within the expected level and type of activity for that customer, provided reasonably regular contact has been maintained between the parties and no doubts have arisen as to the customer's identity.

FC-2.2 On-going Customer Due Diligence and Transaction Monitoring (continued)

On-going Monitoring

FC-2.2.10 Conventional bank licensees must take reasonable steps to:
(a) Scrutinize transactions undertaken throughout the course of that relationship to ensure that transactions being conducted are consistent with the conventional bank licensee's knowledge of the customer, their business risk and risk profile; and
(b) Ensure that they receive and maintain up-to-date and relevant copies of the identification documents specified in Chapter FC-1, by undertaking reviews of existing records, particularly for higher risk categories of customers. Conventional bank licensees must require all customers to provide up-to-date identification documents in their standard terms and conditions of business.

FC-2.2.11 Conventional bank licensees must review and update their customer due diligence information at least every three years, particularly for higher risk categories of customers. If, upon performing such a review, copies of identification documents are more than 12 months out of date, the conventional bank licensee must take steps to obtain updated copies as soon as possible.

FC-3.1 Electronic Transfers

Outward Transfers

FC-3.1.1 **Conventional bank licensees must include all required originator information and required beneficiary information details with the accompanying electronic transfers of funds they make on behalf of their customers. Non-routine transfers must not be batched, if batching increases the risks of money laundering or terrorist financing. This obligation does not apply where the transfer is made by a bank acting as principal or acting on behalf of another bank as principal such as in the case of payment of spot FX transactions.**

FC-3.1.2 **[This Paragraph has been deleted in October 2014 and its contents moved to Paragraph FC-3.1.5.]**

FC-3.1.3 [This paragraph has been deleted in October 2014 and its contents moved to Paragraph FC-3.1.10.]

Inward Transfers

FC-3.1.4 **Banks must:**

(a) Maintain records (in accordance with Chapter FC-7 of this Module) of all originator information received with an inward transfer; and

(b) Carefully scrutinise inward transfers which do not contain originator information (i.e. full name, address and account number or a unique customer identification number). Licensees must presume that such transfers are 'suspicious transactions' and pass them to the MLRO for review for determination as to possible filing of an STR, unless (a), the originating institution is able to promptly (i.e. within two business days) advise the licensee in writing of the originator information upon the licensee's request; or (b) the originating institution and the licensee are acting on their own behalf (as principals).

FC-3.1 Electronic Transfers (continued)

Cross-Border Wire Transfers

FC-3.1.5 **Information accompanying all wire transfers must always contain:**

(a) The name of the originator;

(b) The originator account number or IBAN where such an account is used to process the transaction;

(c) The originator's address, or national identity number, or customer identification number, or date and place of birth;

(d) The name of the beneficiary; and

(e) The beneficiary account number where such an account is used to process the transaction.

FC-3.1.6 In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.

FC-3.1.7 Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements of Paragraph FC-3.1.5 in respect of originator information, provided that they include the originator's account number or unique transaction reference number (as described in Paragraph FC-3.1.6), and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

Domestic Wire Transfers

FC-3.1.8 **Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and the CBB by other means. In this latter case, the originating financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.**

FC-3.1 Electronic Transfers (continued)

FC-3.1.9 For purposes of Paragraph FC-3.1.8, the information should be made available by the originating financial institution within three business days of receiving the request either from the beneficiary financial institution or from the CBB.

FC-3.1.10 It is not necessary for the recipient institution to pass the originator information on to the beneficiary. The obligation is discharged simply by notifying the beneficiary financial institution of the originator information at the time the transfer is made.

Rejecting Payment Transactions

FC-3.1.10A **Licensees have the right to reject (i.e. reverse) any payment transaction where it has come to their knowledge that the relevant customer did not actually initiate the transaction instruction. The fund-transmitting licensees must file a Suspicious Transactions Report for such cases.**

FC-3.1 Electronic Transfers (continued)

Responsibilities of Originating, Intermediary and Beneficiary Banks

Originating Bank

FC-3.1.11 The originating bank must ensure that wire transfers contain required and accurate originator information, and required beneficiary information.

FC-3.1.12 The originating bank must maintain all originator and beneficiary information collected in accordance with Paragraph FC-7.1.1.

FC-3.1.13 The originating bank must not execute the wire transfer if it does not comply with the requirements of Paragraphs FC-3.1.11 and FC-3.1.12.

Intermediary Bank

FC-3.1.14 For cross-border wire transfers, banks processing an intermediary element of such chains of wire transfers must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

FC-3.1.15 Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept, for at least five years, by the receiving intermediary bank of all the information received from the originating bank or another intermediary bank.

FC-3.1.16 An intermediary bank must take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures must be consistent with straight-through processing.

FC-3.1 Electronic Transfers (continued)

FC-3.1.17 An intermediary bank must have effective risk-based policies and procedures for determining:

(a) When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) The appropriate follow-up action.

Beneficiary Bank

FC-3.1.18 A beneficiary bank must take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

FC-3.1.19 For wire transfers, a beneficiary bank must verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Paragraph FC-7.1.1.

FC-3.1.20 A beneficiary bank must have effective risk-based policies and procedures for determining:

(a) When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and

(b) The appropriate follow-up action.

FC-3.2 Remittances on behalf of Money or Value Transfer Service (MVTS) Providers

FC-3.2.1 **Whenever a conventional bank licensee uses the services of Authorised Money or Value Transfer Service Providers to effect the transfer of funds for a customer to a person or organisation in another country, that licensee must, in respect of the amount so transferred, maintain records of:**

(a) The identity of its customer(s) in accordance with Chapters FC-1 and FC-7 of this Module; and

(b) The exact amount transferred for each such customer (particularly where a single transfer is effected for more than one customer).

FC-3.2.1A For purposes of this Section, money or value transfer service (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include new payment methods.

FC-3.2.2 **Conventional bank licensees must be able to produce this information for inspection immediately upon request by the CBB.**

FC-3.2.3 **Conventional bank licensees must not transfer funds for customers to a person or organisation in another country by any means other than through an authorised MVTS provider. Where a licensee is found to be in contravention of this rule, the Central Bank will not hesitate to impose sanctions upon that licensee (and in serious cases may revoke that licensee's license).**

FC-3.2.4 **In the case of an authorised MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the authorised MVTS provider:**

(a) Must take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(b) Must file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Directorate and the CBB.

FC-4.1 Appointment of MLRO

FC-4.1.1 **Conventional bank licensees must appoint a Money Laundering Reporting Officer ('MLRO' who is an approved person. The MLRO must be approved by CBB prior to his appointment. The licensee must submit to the CBB a completed Form 3, in accordance with Chapter LR-1A.**

FC-4.1.2 **The position of MLRO must not be combined with functions that create potential conflicts of interest, such as an internal auditor or business line head. The position of MLRO may not be outsourced.**

FC-4.1.3 Subject to Paragraph FC-4.1.2, however, the position of MLRO may otherwise be combined with other functions in the conventional bank licensee, such as that of Compliance Officer, in cases where the volume and geographical spread of the business is limited and, therefore, the demands of the function are not likely to require a full time resource. Paragraph FC-4.1.6 requires that the MLRO is a Director or employee of the licensee, so the function may not be outsourced to a third party employee.

FC-4.1.3A For the purpose of Paragraphs FC-4.1.2 and FC-4.1.3 above, conventional bank licensees must clearly state in the Application for Approved Person Status – Form 3 – when combining the MLRO or DMLRO position with any other position within the conventional bank licensee.

FC-4.1.4 **Conventional bank licensees must appoint at least one deputy MLRO (or more depending on the scale and complexity of the licensee's operations) to act for the MLRO in his absence. The position of Deputy MLRO is a controlled function and the DMLRO is an approved person. The DMLRO must be approved by CBB prior to his appointment. The DMLRO must satisfy the conditions outlined in Subparagraphs FC-4.1.6 (d) to (g).**

FC-4.1.5 Conventional bank licensees should note that although the MLRO may delegate some of his functions, either within the licensee or even possibly (in the case of larger groups) to individuals performing similar functions for other group entities, that the responsibility for compliance with the requirements of this Module remains with the licensee and the designated MLRO.

FC-4.1 Appointment of MLRO (continued)

FC-4.1.6 So that he can carry out his functions effectively, conventional bank licensees must ensure that their MLRO:

(a) Is a member of senior management of the licensee;

(b) Has a sufficient level of seniority within the conventional bank licensee, has the authority to act without interference from business line management and has direct access to the Board and senior management (where necessary);

(c) Has sufficient resources, including sufficient time and (if necessary) support staff, and has designated a replacement to carry out the function should the MLRO be unable to perform his duties;

(d) Has unrestricted access to all transactional information relating to any financial services provided by the conventional bank licensee to a customer, or any transactions conducted by the conventional bank licensee on behalf of that customer;

(e) Is provided with timely information needed to identify, analyse and effectively monitor customer accounts;

(f) Has access to all customer due diligence information obtained by the conventional bank licensee; and

(g) Is resident in Bahrain.

FC-4.1.7 [This Paragraph is left blank].

FC-4.1.8 In addition, conventional bank licensees must ensure that their MLRO is able to:

(a) Monitor the day-to-day operation of its policies and procedures relevant to this Module; and

(b) Respond promptly to any reasonable request for information made by the Anti-Money Laundering Unit or the CBB.

FC-4.1.9 If the position of MLRO falls vacant, the conventional bank licensee must appoint a permanent replacement (after obtaining CBB approval), within 120 calendar days of the vacancy occurring. Pending the appointment of a permanent replacement, the licensee must make immediate interim arrangements (including the appointment of an acting MLRO) to ensure continuity in the MLRO function's performance. These interim arrangements must be approved by the CBB.

FC-4.2 Responsibilities of the MLRO

FC-4.2.1 The MLRO is responsible for:

(a) Establishing and maintaining the conventional bank licensee's AML/CFT policies and procedures;

(b) Ensuring that the licensee complies with the AML Law and any other applicable AML/CFT legislation and regulations;

(c) Ensuring day-to-day compliance with the licensee's own internal AML/CFT policies and procedures;

(d) Acting as the conventional bank licensee's main point of contact in respect of handling internal suspicious transaction reports from the licensee's staff (refer to Section FC-5.1) and as the main contact for the Financial Intelligence Directorate, the CBB and other concerned bodies regarding AML/CFT;

(e) Making external suspicious transactions reports to the Financial Intelligence Directorate and the Compliance Directorate (refer to Section FC-5.2);

(f) Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters (whether internal or external), as per Chapter FC-5;

(g) Producing annual reports on the effectiveness of the licensee's AML / CFT controls, for consideration by senior management, as per Paragraph FC-4.3.3;

(h) On-going monitoring of what may, in his opinion, constitute high-risk customer accounts; and

(i) Ensuring that the conventional bank licensee maintains all necessary CDD, transactions, STR and staff training records for the required periods (refer to Section FC-7.1).

FC-4.3 Compliance Monitoring

Annual Compliance Review

FC-4.3.1 **Conventional bank licensees must take appropriate steps to identify and assess their money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). They must document those assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the CBB. The nature and extent of any assessment of money laundering and terrorist financing risks must be appropriate to the nature and size of the business.**

FC-4.3.1A Conventional bank licensees should always understand their money laundering and terrorist financing risks, but the CBB may determine that individual documented risk assessments are not required, if the specific risks inherent to the sector are clearly identified and understood.

FC-4.3.1B **A conventional bank licensee must review the effectiveness of its AML/CFT procedures, systems and controls at least once each calendar year. The review must cover the conventional bank licensee and its branches and subsidiaries both inside and outside the Kingdom of Bahrain. A conventional bank licensee must monitor the implementation of those controls and enhance them if necessary. The scope of the review must include:**

(a) A report, containing the number of internal reports made in accordance with Section FC-5.1, a breakdown of all the results of those internal reports and their outcomes for each segment of the licensee's business, and an analysis of whether controls or training need to be enhanced;

(b) A report, indicating the number of external reports made in accordance with Section FC-5.2 and, where a conventional bank licensee has made an internal report but not made an external report, noting why no external report was made;

(c) A sample test of compliance with this Module's customer due diligence requirements; and

(d) A report as to the quality of the conventional bank licensee's anti-money laundering procedures, systems and controls, and compliance with the AML Law and this Module.

FC-4.3.2 **The reports listed under Paragraph FC-4.3.1B (a) and (b) must be made by the MLRO. The sample testing and report required under Paragraph FC-4.3.1B (c) and (d) must be made by the licensee's external auditor or a consultancy firm approved by the CBB.**

FC-4.3 Compliance Monitoring (continued)

FC-4.3.2A In order for a consultancy firm to be approved by the CBB for the purposes of Paragraph FC-4.3.2, such firm should provide the CBB's Compliance Directorate with:

(a) A sample AML/CFT report prepared for a financial institution;
(b) A list of other AML/CFT related work undertaken by the firm;
(c) A list of other audit/review assignments undertaken, specifying the nature of the work done, date and name of the licensee; and
(d) An outline of any assignment conducted for or in cooperation with an international audit firm.

FC-4.3.2B The firm should indicate which personnel (by name) will work on the report (including, where appropriate, which individual will be the team leader) and demonstrate that all such persons have appropriate qualifications in one of the following areas:

(a) Audit;
(b) Accounting;
(c) Law; or
(d) Banking/Finance.

FC-4.3.2C **Conventional bank licensees must ensure that the personnel conducting the review are qualified, skilled and have adequate experience to conduct such a review. At least two persons working on the report (one of whom should be the team leader) must have:**

(a) A minimum of 5 years professional experience dealing with AML/CFT issues; and
(b) Formal AML/CFT training.

FC-4.3.2D Submission of a curriculum vitae for all personnel to be engaged on the report is encouraged for the purposes of evidencing the above requirements.

FC-4.3.2E Upon receipt of the above required information, the CBB Compliance Directorate will assess the firm and communicate to it whether it meets the criteria required to be approved by the CBB for this purpose. The CBB may also request any other information it considers necessary in order to conduct the assessment.

FC-4.3.3 **The reports listed under Paragraph FC-4.3.1B must be submitted to the licensee's Board, for it to review and commission any required remedial measures, and copied to the licensee's senior management.**

FC-4.3 Compliance Monitoring (continued)

FC-4.3.4 The purpose of the annual compliance review is to assist a licensee's Board and senior management to assess, amongst other things, whether internal and external reports are being made (as required under Chapter FC-5), and whether the overall number of such reports (which may otherwise appear satisfactory) does not conceal inadequate reporting in a particular segment of the licensee's business (or, where relevant, in particular branches or subsidiaries). Conventional bank licensees should use their judgement as to how the reports listed under Paragraph FC-4.3.1B (a) and (b) should be broken down in order to achieve this aim (e.g. by branches, departments, product lines, etc).

FC-4.3.5 **Conventional bank licensees must instruct their appointed firm to produce the report referred to in Paragraph FC-4.3.1B (c) and (d). The report must be submitted to the Compliance Directorate at the CBB by the 30th of June of the following year. The findings of this review must be received and acted upon by the licensee.**

FC-4.3.6 [This Paragraph was deleted in January 2022].

FC-5.1 Internal Reporting

FC-5.1.1 Conventional bank licensees must implement procedures to ensure that staff who handle customer business (or are managerially responsible for such staff) make a report promptly to the MLRO if they know or suspect that a customer (or a person on whose behalf a customer may be acting) is engaged in money laundering or terrorism financing, or if the transaction or the customer's conduct otherwise appears unusual or suspicious. These procedures must include arrangements for disciplining any member of staff who fails, without reasonable excuse, to make such a report.

FC-5.1.2 Where conventional bank licensees' internal processes provide for staff to consult with their line managers before sending a report to the MLRO, such processes must not be used to prevent reports reaching the MLRO, where staff have stated that they have knowledge or suspicion that a transaction may involve money laundering or terrorist financing.

FC-5.2 External Reporting

FC-5.2.1 Conventional bank licensees must take reasonable steps to ensure that all reports made under Section FC-5.1 are considered by the MLRO (or his duly authorised delegate). Having considered the report and any other relevant information the MLRO (or his duly authorised delegate), if he still suspects that a person has been engaged in money laundering or terrorism financing, or the activity concerned is otherwise still regarded as suspicious, must report the fact promptly to the relevant authorities. Where no report is made, the MLRO must document the reasons why.

FC-5.2.2 To take reasonable steps, as required under Paragraph FC-5.2.1, conventional bank licensees must:

(a) Require the MLRO to consider reports made under Section FC-5.1.1 in the light of all relevant information accessible to or reasonably obtainable by the MLRO;

(b) Permit the MLRO to have access to any information, including know your customer information, in the conventional bank licensee's possession which could be relevant; and

(c) Ensure that where the MLRO, or his duly authorised delegate, suspects that a person has been engaged in money laundering or terrorist financing, a report is made by the MLRO which is not subject to the consent or approval of any other person.

FC-5.2.3 Reports to the relevant authorities made under Paragraph FC-5.2.1 must be sent to the Financial Intelligence Directorate at the Ministry of Interior and the CBB's Compliance Directorate using the Suspicious Transaction Report Online System (Online STR system). STRs in paper format will not be accepted.

FC-5.2.4 Conventional bank licensees must report all suspicious transactions or attempted transactions. This reporting requirement applies regardless of whether the transaction involves tax matters.

FC-5.2 External Reporting (continued)

FC-5.2.5 Conventional bank licensees must retain all relevant details of STRs submitted to the relevant authorities for at least five years.

FC-5.2.6 In accordance with the AML Law, conventional bank licensees, their Directors, officers and employees:

(a) Must not warn or inform ('tipping off') their customers, the beneficial owner or other subjects of the STR when information relating to them is being reported to the relevant authorities; and

(b) In cases where conventional bank licensees form a suspicion that transactions relate to money laundering or terrorist financing, they must take into account the risk of tipping-off when performing the CDD process. If the conventional bank licensee reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and must file an STR.

FC-5.3 Contacting the Relevant Authorities

FC-5.3.1 Reports made by the MLRO or his duly authorised delegate under Section FC-5.2 must be sent electronically using the Suspicious Transaction Reporting Online System (Online STR system).

FC-5.3.2 The relevant authorities are:

Financial Intelligence Directorate (FID)
Ministry of Interior
P.O. Box 26698
Manama, Kingdom of Bahrain
Telephone: + 973 17 749397
Fax: + 973 17 715502
E-mail: bahrainfid@moipolice.bh

Director of Compliance Directorate
Central Bank of Bahrain
P.O. Box 27
Manama, Kingdom of Bahrain
Telephone: 17 547107
Fax: 17 535673
E-mail: Compliance@cbb.gov.bh

FC-6.1 General Requirements

FC-6.1.1 **A conventional bank licensee must take reasonable steps to provide periodic training and information to ensure that staff who handle customer transactions, or are managerially responsible for such transactions, are made aware of:**

(a) Their responsibilities under the AML Law, this Module, and any other relevant AML / CFT laws and regulations;
(b) The identity and responsibilities of the MLRO and his deputy;
(c) The potential consequences, both individual and corporate, of any breach of the AML Law, this Module and any other relevant AML / CFT laws or regulations;
(d) The conventional bank licensee's current AML/CFT policies and procedures;
(e) Money laundering and terrorist financing typologies and trends;
(f) The type of customer activity or transaction that may justify an internal STR;
(g) The conventional bank licensee's procedures for making internal STRs; and
(h) Customer due diligence measures with respect to establishing business relations with customers.

FC-6.1.2 **The information referred to in Paragraph FC-6.1.1 must be brought to the attention of relevant new employees of conventional bank licensees, and must remain available for reference by staff during their period of employment.**

FC-6.1.3 **Relevant new employees must be given AML/CFT training within three months of joining a conventional bank licensee.**

FC-6.1.4 **Conventional bank licensees must ensure that their AML/CFT training for relevant staff remains up-to-date, and is appropriate given the licensee's activities and customer base.**

FC-6.1.5 The CBB would normally expect AML/CFT training to be provided to relevant staff at least once a year.

FC-6.1.6 **Conventional bank licensees 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 conventional bank licensees.**

FC-6.1.6A **[This Paragraph was deleted in January 2022].**

FC-7.1 General Requirements

CDD and Transaction Records

FC-7.1.1 Conventional bank licensees must comply with the record-keeping requirements contained in the AML Law. Conventional bank licensees must therefore retain adequate records (including accounting and identification records), for the following minimum periods:

(a) For customers, in relation to evidence of identity and business relationship records (such as application forms, account files and business correspondence, including the results of any analysis undertaken (e.g. enquiries to establish the background and purpose of complex, unusual large transactions)), for at least five years after the customer relationship has ceased; and

(b) For transactions, in relation to documents (including customer instructions in the form of letters, faxes or emails) enabling a reconstitution of the transaction concerned, for at least five years after the transaction was completed.

Compliance Records

FC-7.1.2 Conventional bank licensees must retain copies of the reports produced for their annual compliance review, as specified in Paragraph FC-4.3.1B, for at least five years. Conventional bank licensees must also maintain for 5 years reports made to, or by, the MLRO made in accordance with Sections FC-5.1 and 5.2, and records showing how these reports were dealt with and what action, if any, was taken as a consequence of those reports.

Training Records

FC-7.1.3 Conventional bank licensees must maintain for at least five years, records showing the dates when AML/CFT training was given, the nature of the training, and the names of the staff that received the training.

Access

FC-7.1.4 All records required to be kept under this Section must be made available for prompt and swift access by the relevant authorities or other authorised persons.

FC-7.1.5 Conventional bank licensees are also reminded of the requirements contained in Chapter OM-7 (Books and Records).

FC-8.1 Special Measures for Non-Cooperative Countries or Territories ('NCCTs')

FC-8.1.1 **Conventional bank licensees must give special attention to any dealings they may have with entities or persons domiciled in countries or territories which are:**

(a) Identified by the FATF as being 'non-cooperative'; or

(b) Notified to conventional bank licensees from time to time by the CBB.

FC-8.1.2 **Whenever transactions with such parties have no apparent economic or visible lawful purpose, their background and purpose must be re-examined and the findings documented. If suspicions remain about the transaction, these must be reported to the relevant authorities in accordance with Section FC-5.2.**

FC-8.1.3 **Conventional bank licensees must apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries where such measures are called for by the FATF. The type of enhanced due diligence measures applied must be effective and proportionate to the risks.**

FC-8.1.4 With regard to jurisdictions identified as NCCTs or those which in the opinion of the CBB, do not have adequate AML/CFT systems, the CBB reserves the right to:

(a) Refuse the establishment of subsidiaries or branches or representative offices of financial institutions from such jurisdictions;

(b) Limit business relationships or financial transactions with such jurisdictions or persons in those jurisdictions;

(c) Prohibit financial institutions from relying on third parties located in such jurisdictions to conduct elements of the CDD process;

(d) Require financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in such jurisdictions;

(e) Require increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in such jurisdictions; or

(f) Require increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in such jurisdictions.

FC-8.2 Terrorist Financing

FC-8.2.1AA **Conventional bank licensees must implement and comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. Conventional bank licensees must freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267(1999) and its successor resolutions as well as Resolution 2178(2014) or (ii) designated as pursuant to Resolution 1373(2001).**

FC-8.2.1 **Conventional bank licensees must comply in full with any rules or regulations issued by the CBB in connection with the provisions of the UN Security Council Anti-terrorism Resolution No. 1373 of 2001 ('UNSCR 1373'), including the rules in this Chapter.**

FC-8.2.2 **[This Paragraph was deleted in January 2018].**

FC-8.2.3 A copy of UNSCR 1373 is included in Part B of Volume 1 (Conventional Banks), under 'Supplementary Information'.

FC-8.2.4 **Conventional bank licensees must report to the CBB details of:**

(a) Funds or other financial assets or economic resources held with them which may be the subject of Article 1, Paragraphs c) and d) of UNSCR 1373;

(b) All claims, whether actual or contingent, which the conventional bank licensee has on persons and entities which may be the subject of Article 1, Paragraphs c) and d) of UNSCR 1373; and

(c) All assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs, including attempted transactions.

FC-8.2.5 For the purposes of Paragraph FC-8.2.4, 'funds or other financial resources' includes (but is not limited to) shares in any undertaking owned or controlled by the persons and entities referred to in Article 1, Paragraph c) and d) of UNSCR 1373, and any associated dividends received by the licensee.

FC-8.2 Terrorist Financing (continued)

FC-8.2.6 **All reports or notifications under this Section must be made to the CBB's Compliance Directorate.**

FC-8.2.7 See Section FC-5.3 for the Compliance Directorate's contact details.

FC-8.3 Designated Persons and Entities

FC-8.3.1 **Without prejudice to the general duty of all conventional bank licensees to exercise the utmost care when dealing with persons or entities who might come under Article 1, Paragraphs (c) and (d) of UNSCR 1373, conventional bank licensees must not deal with any persons or entities designated by the CBB as potentially linked to terrorist activity.**

FC-8.3.2 The CBB from time to time issues to licensees lists of designated persons and entities believed linked to terrorism. Licensees are required to verify that they have no dealings with these designated persons and entities, and report back their findings to the CBB. Names designated by CBB include persons and entities designated by the United Nations, under UN Security Council Resolution 1267 ('UNSCR 1267').

FC-8.3.3 **Conventional bank licensees must report to the relevant authorities, using the procedures contained in Section FC-5.2, details of any accounts or other dealings with designated persons and entities, and comply with any subsequent directions issued by the relevant authorities.**

FC-9.1 Regulatory Penalties

FC-9.1.1 **Without prejudice to any other penalty imposed by the CBB Law, the Decree Law No. 4 or the Penal Code of the Kingdom of Bahrain, failure by a licensee to comply with this Module or any direction given hereunder shall result in the levying by the CBB, without need of a court order and at the CBB's discretion, of a fine of up to BD 20,000.**

FC-9.1.2 Module EN provides further information on the assessment of financial penalties and the criteria taken into account prior to imposing such fines (reference to Paragraph EN-5.1.4). Other enforcement measures may also be applied by CBB in response to a failure by a licensee to comply with this Module; these other measures are also set out in Module EN.

FC-9.1.3 The CBB will endeavour to assist conventional bank licensees to interpret and apply the rules and guidance in this Module. Conventional bank licensees may seek clarification on any issue by contacting the Compliance Directorate (see Section FC-5.3 for contact details).

FC-9.1.4 Without prejudice to the CBB's general powers under the law, the CBB may amend, clarify or issue further directions on any provision of this Module from time to time, by notice to its licensees.

FC-10.1 Guidance Provided by International Bodies

FATF: Recommendations

FC-10.1.1 The FATF Recommendations (see www.fatf-gafi.org) together with their associated interpretative notes and best practices papers issued by the Financial Action Task Force (FATF) provide the basic framework for combating money laundering activities and the financing of terrorism. FATF Recommendations 2, 8-12, 14-21, 26-27, 32-35, 37 and 40 and the AML/CFT Methodology are specifically relevant to the banking sector.

FC-10.1.2 The relevant authorities in Bahrain believe that the principles established by these Recommendations should be followed by licensees in all material respects, as representing best practice and prudence in this area.

Basel Committee: Statement on Money Laundering and Customer Due Diligence for Banks

FC-10.1.3 In December 1988, the Basel Committee on Banking Supervision issued a 'Statement of Principles' followed by the Customer Due Diligence for Banks paper in October 2001 (with attachment dated February 2003 – see www.bis.org/publ/) with which internationally active banks of member states are expected to comply. These papers cover identifying customers, avoiding suspicious transactions, and co-operating with law enforcement agencies.

FC-10.1.4 The CBB supports the above papers and the desirability of all conventional bank licensees adhering to their requirements and guidance.

Other Website References Relevant to AML/CFT

FC-10.1.5 The following lists a selection of other websites relevant to AML/CFT:

(a) The Middle East North Africa Financial Action Task Force: www.menafatf.org ;
(b) The Egmont Group: www.egmontgroup.org ;
(c) The United Nations: www.un.org/terrorism ;
(d) The UN Counter-Terrorism Committee: www.un.org/Docs/sc/committees/1373/ ;
(e) The UN list of designated individuals: www.un.org/Docs/sc/committees/1267/1267ListEng.htm ;
(f) The Wolfsberg Group: www.wolfsberg-principles.com ; and
(g) The Association of Certified Anti-Money Laundering Specialists: www.acams.org .