# FINANCIAL CRIME MODULE

| MODULE | FC (Financial Crime) |
|---|---|

# Table of Contents

| MODULE | FC (Financial Crime) |
|---|---|

## Table of Contents

## FC-A.1 Purpose

### *Executive Summary*

FC-A.1.1 This Module applies, to relevant insurance 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), that are relevant to insurance licensees; it also implements IAIS guidance in this area. (Further information on these can be found in Chapter FC-9.) The Module also contains measures relating to the combating of fraud in the insurance sector.

FC-A.1.2 The Module requires insurance firms and insurance brokers 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 (see Part B, Supplementary Information, Appendix FC(iv)), to assist licensees to monitor transactions and fulfil their reporting obligations under Bahrain law. Because they represent negligible money laundering/terrorism financing risk, these requirements do not apply to insurance consultants nor, in some circumstances, to insurance managers.

FC-A.1.3 This Module also covers measures in place to combat fraud: these apply to all insurance licensees. Chapter FC-10 sets out basic requirements regarding measures to deter, detect and report instances of fraud and attempted fraud.

### *Legal Basis*

**FC-A.1.4** **This Module contains the Central Bank of Bahrain's (the 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 insurance licensees (including their approved persons).**

FC-A.1.5 For an explanation of the CBB's rule-making powers and different regulatory instruments, see Section UG-1.1.

## FC-A.2 Module History

FC-A.2.1 This Module was first issued by the BMA in April 2005, together with the rest of Volume 3 (Insurance). 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 3 was updated in January 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-A.1; FC-2; FC-3; FC-5; FC-6.1; FC-6.2; FC-6.5 | 01/07/05 | Inclusion of a revised and renamed Customer Due Diligence Chapter (including a new non-face-to-face business Section). Renamed Suspicious Transaction Reporting Chapter, with minor clarifications to the text. Changes to layout of FC-5 and clarifications to the text. Correction of minor typographical and cross-referencing errors. |
| FC | 01/10/05 | New Chapter on Non-Cooperative Countries/Territories, and UN notifications. Section on charities removed, since not applicable to insurance licensees. Extensive drafting changes to remainder of text, to improve clarity and ensure consistency across different CBB Rulebooks; but no other changes of substance. |
| FC-1.2 | 01/01/06 | Clarified in FC-1.2.11 that the verification for item (a) applies to the identity of the ultimate provider of funds. |
| FC-3.1.7 | 01/04/06 | Clarified and added guidance Paragraph dealing with residency requirements of MLRO. |
| FC-4.3.1 | 01/07/06 | Updated contact information for Compliance Directorate. |
| FC-A.1.4 | 01/2007 | New Rule introduced, categorising this Module as a Directive |
| FC-1.6.3 | 01/2007 | Clarified simplified due diligence rules for transactions under BD6,000. |
| FC-3.3.5A and FC-3.3.7 | 01/2007 | Allowed for a transition period for the external auditor's report required under SubParagraph FC-3.3.1(d) and clarified when all reports are due. |
| FC-4.3.1 | 01/2007 | Updated new e-mail address for Compliance Directorate. |
| FC-1.7.2(d) | 10/2007 | Clarified the record retention period for introduced business in line with Article 60 of the CBB Law |
| FC-2.2.3, 2.2.6, 4.2.5, 6.1.1,6.1.2, 6.1.3 | 10/2007 | Clarified the record retention period for various transactions to be in line with Article 60 of the CBB Law |
| FC-3.3.2 | 10/2007 | Clarified the appointment of external auditors for the purposes of the report required under Paragraph FC-3.3.1 (d) |
| FC-10.1.11 | 10/2007 | Added reference to new Guidance paper on fraud issued by the IAIS. |
| FC-3.3.7 | 04/2008 | Clarified to whom in the CBB should the reports required under Paragraph FC-3.3.1 be submitted to. |
| FC-1.7.2, 2.2.3, 2.2.6, 4.2.5, 6.1.1,6.1.2, 6.1.3 | 04/2008 | Reduced retention requirements of records to five years to be consistent with AML Law and other Volumes of the CBB Rulebook |
| Table of Contents | 07/2008 | Added Supplementary Documents to Part B. |

## FC-A.2 Module History (continued)

FC-A.2.3 (continued)

| Module Ref. | Change Date | Description of Changes |
|---|---|---|
| FC-1.1.3 | 07/2009 | Provided guidance for insurance brokers on definition of 'customers'. |
| FC-3.1.10, 3.2.1, 4.2.3, 4.3.1 | 04/2010 | Updated name and e-mail of relevant authority to Financial Intelligence Unit. |
| FC-A.1.4 | 01/2011 | Clarified legal basis |
| FC-3.1.9 | 10/2011 | Clarified requirements for MLRO. |
| FC-3.3 | 10/2011 | Amended Section to allow for CBB-approved consultancy firm to do required sample testing and report under Paragraph FC-3.3.1. |
| FC-3.3.5 and FC-3.3.6 | 01/2012 | Amended to reflect the addition of approved consultancy firm. |
| FC-4.2.3 | 10/2014 | Updated method of submitting STRs. |
| FC-4.3 | 10/2014 | Updated relevant authorities information. |
| FC | 10/2015 | Updated to reflect February 2012 update to FATF Recommendations. |
| FC-1.5.1 | 07/2016 | Aligned definition of PEPs as per FATF Recommendations. |
| FC-1.5.4 | 07/2016 | Definition of PEPs is already included in Glossary so this guidance paragraph was deleted. |
| FC-4.2.3 | 07/2016 | Updated instructions for STR. |
| FC-1.2.9A | 01/2017 | Added guidance paragraph on CR printing |
| FC-7.2.1AA | 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-1.2.7 | 10/2017 | Amended paragraph. |
| FC-1.2.8A | 10/2017 | Added new paragraph on legal entities or legal arrangements CDD. |
| FC-2.2.10 – FC-2.2.11 | 10/2017 | Amended paragraphs on On-going CDD and Transaction Monitoring. |
| FC-3.1.6A | 10/2017 | Added paragraph on combining the MLRO or DMLRO position with any other position within the licensee. |
| FC-B.3.4 | 01/2018 | Amended paragraph. |
| FC-1.5.5 | 01/2018 | Added new paragraph. |
| FC-1.5.6 | 01/2018 | Added new paragraph. |
| FC-1.6.1 | 01/2018 | Deleted sub-paragraph (f). |
| FC-1.7.1 | 01/2018 | Amended paragraph. |
| FC-4.2.6 | 01/2018 | Amended paragraph. |
| FC-7.1.4 | 01/2018 | Amended paragraph. |
| FC-7.2.2 | 01/2018 | Deleted paragraph. |
| FC-1.1.2 | 07/2018 | Deleted sub-paragraph (g). |
| FC-1.2.1 | 07/2018 | Amended guidance deleting the threshold. |
| FC-1.6.3 | 07/2018 | Deleted Paragraph. |
| FC-1.6.9 | 07/2018 | Deleted Paragraph. |
| FC-1.6.10 | 07/2018 | Deleted Paragraph. |
| FC-1.6.1 | 01/2019 | Amended references. |
| FC-3.3.2 - FC-3.3.5 | 01/2019 | Amended references. |
| FC-3.3.5A | 01/2019 | Deleted paragraph. |
| FC-3.3.7 | 01/2019 | Amended references. |
| FC-6.1.2 | 01/2019 | Amended references. |
| FC-3.1.10 | 10/2019 | Amended authority name. |
| FC-3.2.1 | 10/2019 | Amended authority name. |
| FC-4.2.3 | 10/2019 | Amended authority name. |
| FC-4.3.2 | 10/2019 | Amended authority name. |
| FC-7.2.1AA | 10/2019 | Defined 'without delay'. |

FC-A.2.4 Guidance on the implementation and transition to Volume 3 (Insurance) is given in Module ES (Executive Summary)

## FC-A.2 Module History (continued)

FC-A.2.3 (continued)

| Module Ref. | Change Date | Description of Changes |
|---|---|---|
| FC-1.1.1 | 01/2020 | Amended Paragraph on procedures approval. |
| FC-1.2.1 | 01/2020 | Added a new sub-Paragraph. |
| FC-3.3.5 | 01/2020 | Amended Paragraph on report submission date. |
| FC-3.3.7 | 01/2020 | Amended Paragraphs references. |
| FC-2.1.4 & FC-2.1.5 | 04/2020 | Added new Paragraphs on KPIs compliance with AML/CFT requirements. |
| FC-5.1.6A | 01/2021 | Added a new Paragraph on requirements to hire new employees. |
| FC-5.1.6A | 07/2021 | Amended Paragraph on requirements to hire new employees. |
| FC-A.1.4 | 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 | Amended Section 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 | Amended Section to include E-KYC and electronic documents law requirements. |
| FC-1.3 | 01/2022 | Amended Section on enhanced due diligence requirements for customers identified as having higher risk profile. |
| FC-1.4 | 01/2022 | Amended Section to introduce detailed requirements for digital onboarding and related requirements. |
| FC-1.5.2 | 01/2022 | Amended Paragraph on onboarding non-Bahraini PEPs using digital ID applications. |
| FC-1.5A | 01/2022 | Added a new Section on Enhanced Due Diligence: Charities, Clubs and Other Societies |
| FC-1.6.8A | 01/2022 | Added a new Paragraph on not applying simplified CDD in situations where the licensee has identified high ML/TF/PF risks. |
| FC-2.2.5 | 01/2022 | Amended Paragraph. |
| FC-3.3.1B | 01/2022 | Amended Paragraph. |
| FC-3.3.2 | 01/2022 | Amended Paragraph. |
| FC-3.3.5 | 01/2022 | Amended Paragraph. |
| FC-3.3.6 | 01/2022 | Deleted Paragraph. |
| FC-3.3.7 | 01/2022 | Deleted Paragraph. |
| FC-5.1.6A | 01/2022 | Deleted Paragraph. |

## FC-B.1 License Categories

**FC-B.1.1** **Chapters FC-1 to FC-9 apply to all insurance firms and insurance brokers. These Chapters also apply to insurance managers where they manage a captive insurer. Chapters FC-1 to FC-9 do not apply to insurance consultants.**

FC-B.1.2 Chapters FC-1 to FC-9 apply, as specified in Paragraph FC-B.1.1, to all insurance firms, insurance brokers and, where they manage a captive insurer, insurance managers, irrespective of whether they are a Bahraini insurance licensee or an overseas insurance licensee. Overseas insurance licensees, and Bahraini insurance licensees that are subsidiaries of an overseas group, may apply additional AML/CFT policies and procedures, provided they satisfy the minimum requirements contained in this Module.

FC-B.1.3 The Rules and Guidance in 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 (including financial services firms such as insurance licensees). All insurance licensees are 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 3 (Insurance), 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.1.4** **Chapter FC-10, dealing with insurance fraud, applies to all insurance licensees.**

## FC-B.2 Types of Insurance Business

**FC-B.2.1** **This Module applies to all types of insurance contracts, including general and long-term insurance, as well as to reinsurance and captive insurance business.**

FC-B.2.2 International experience shows that all types of insurance (including general insurance and reinsurance) have been used as channels for illegal activities. However, the CBB also recognises that in the case of pure reinsurance transactions, these risks may exist to a lesser extent. Consequently, upon application by the licensee, the CBB will consider, on an individual basis, exemptions from specific requirements of this Module, in relation to the reinsurance activities of licensees. Normally, the CBB will consider granting such exemptions where the reinsurer concerned deals only with licensed insurance entities, that are subject to AML/CFT standards equivalent to those in this Module.

## FC-B.3 Overseas Subsidiaries and Branches

**FC-B.3.1** **Insurance licensees must apply the requirements in this Module to all their branches and subsidiaries, including those operating in another jurisdiction. Where local standards differ, the higher standard must be followed. Insurance licensees must pay particular attention to procedures in branches and subsidiaries in countries that do not or insufficiently apply the FATF Recommendations and Special Recommendations and do not have adequate AML/CFT procedures, systems and controls (see also Section FC-7.1).**

**FC-B.3.2** **Where another jurisdiction's laws or Regulations prevent an insurance 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.3.3 In such instances, the CBB will review alternatives with the insurance 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 insurance licensee may be required by the CBB to cease the operations of the subsidiary or branch in the foreign jurisdiction in question.

**FC-B.3.4** **Financial groups (e.g. an insurance firm with its subsidiaries) 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;**
**(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** An insurance 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** An insurance 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** An insurance license 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** Insurance 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** An insurance 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 insurance 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 may 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 Risk Assessment (continued)

**FC-C.2.4** An insurance 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;
(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;
(h) Internal audit, external audit or regulatory inspection findings; and
(i) beneficiary of a life insurance policy.

## FC-C.2 Risk Assessment (continued)

### *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.

### *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;

## FC-C.2 Risk Assessment (continued)

(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 insurance 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.2.8 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) Anonymous transactions (which may include cash);
(b) Non-face-to-face business relationships or transactions;
(c) Payment received from unknown or un-associated third parties;
(d) Products or services that may inherently favour anonymity or obscure information about underlying customer transactions;
(e) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions;
(f) Products with unusual complexity or structure and with no obvious economic purpose;
(g) 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
(h) Use of new technologies or payment methods not used in the normal course of business by the insurance licensee.

***Distribution Channel Risk***

FC-C.2.9 A customer may request transactions that pose an inherently higher risk to the insurance 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 An insurance 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 licensee. Licensee 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.

## FC-1.1 General Requirements

*Verification of Identity and Source of Funds*

**FC-1.1.1** Insurance 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** Insurance licensees must implement the customer due diligence measures outlined in this Chapter when:

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

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

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

(a) Scrutinizing of 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
(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 General Requirements

**FC-1.1.2C** **An insurance licensee must also review and update the customer's risk profile based on their level of ML/TF/PF risk upon onboarding the customer 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 a particular customer or type of customer.**

FC-1.1.3 For the purposes of this Module, 'customer' includes counterparties such as reinsurers and financial markets counterparties, as well as persons insured by the licensee. However, in the case of group insurance policies (such as group life or medical), the requirements in this Module need not be applied to all policyholders: see Paragraph FC-1.2.13. For insurance brokers, 'customer' refers to policyholders.

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-1.5 inclusive. Simplified customer due diligence measures may apply in defined circumstances: these are set out in Section FC-1.6.

FC-1.1.5 Where an insurance licensee is dealing with an intermediary such as a broker, reliance may be placed on customer identification undertaken by the intermediary, if certain conditions are satisfied: please refer to Chapter FC-1.7.

## FC-1.1 General Requirements (continued)

*Verification of Third Parties*

**FC-1.1.6** Insurance 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-1.1.7** Where a customer is acting on behalf of a third party, the insurance 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 insurance 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-1.1.8** Insurance licensees must establish and verify the identity of the customer and (where applicable) the party/parties on whose behalf the customer is acting. In the case of insurance policies, the identity of the beneficiaries must also be separately identified and verified, and the relationship between the insured party and the beneficiaries must be ascertained. Verification must take place in accordance with the requirements specified in this Chapter.

**FC-1.1.9** If claims, commissions, and other monies are to be paid to persons (including partnerships, companies, etc.) other than the policyholder, then the identity of the proposed recipient of these monies must also be verified in accordance with the requirements specified in this Chapter.

**FC-1.1.10** Where a policy is 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 subscribes to a policy, the licensee must establish the identity of that third party as well as the intended policyholder.

## FC-1.1 General Requirements (continued)

*Anonymous and Nominee Accounts*

**FC-1.1.11** **Insurance licensees must not establish or keep anonymous policies or policies in fictitious names. Where insurance 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 insurance licensee and verified by it in accordance with the requirements specified in this Chapter.**

*Timing of Verification*

**FC-1.1.12** **Insurance licensees must not commence a business relationship or undertake a transaction with a customer before completion of the relevant customer due diligence ('CDD') measures specified in this Chapter. 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 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 until after the requirements of this Chapter have been fully met.**

*Incomplete Customer Due Diligence*

**FC-1.1.13** **Where an insurance licensee is unable to comply with the requirements specified in this Chapter, it must consider whether to terminate the relationship or not proceed with the transaction. If funds have been received, these must be returned to the counterparty in the same method as originally received. If it proceeds with the transaction (to avoid tipping off the customer), it should additionally consider whether it should file a suspicious transaction report.**

FC-1.1.14 See also Chapter FC-4, 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.

## FC-1.1 General Requirements (continued)

*Non-Resident Accounts*

**FC-1.1.14A** Insurance licensees that transact or deal with non-resident customers who are natural persons must have documented criteria for acceptance of business with such persons. For non-resident customers, insurance 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; and
(f) Test that the persons are contactable without unreasonable delays.

**FC-1.1.14B** Insurance licensees that transact or deal with non-resident customers who are natural persons 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-1.1.14C** Insurance licensees must not accept non-residents customers from high risk jurisdictions subject to a call for action by FATF.

**FC-1.1.14D** Insurance 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-1.1.12B; and
(c) Countries that are the subject of any other sanctions.

## FC-1.1 General Requirements (continued)

**FC-1.1.14E** Insurance licensees that deal with non-resident customers, other than with financial institutions, listed companies and governmental authorities in FATF countries referred to in FC-1.6.1, 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-1.1.14F** Insurance 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-1.1.14G** Insurance 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-1.1.14H** Insurance licensees must ensure that only the 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-1.1.14I** Customers residing outside Bahrain, are subject to the enhanced customer due diligence measures outlined in Section FC-1.3. Licensees must not transact or deal with natural persons residing outside the GCC through a digital onboarding process.

***Existing Customers***

**FC-1.1.15** **[This Paragraph was deleted in October 2015.]**

FC-1.1.16 [This Paragraph was deleted in October 2015.]

## FC-1.2 Face-to-face Business

***Natural Persons***

**FC-1.2.1** If the customer is a natural person, the insurance licensee 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 Bahraini or GCC residents only) 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 policy, and nature and volume of anticipated business dealings with the insurance licensee;
k) Signature of the customer(s);
l) Source of funds for payment of premium; and
m) Reason for opening the account.

**FC-1.2.1A** Insurance 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 3 (Insurance), for a Guidance Note on source of funds.

## FC-1.2 Face-to-face Business

**FC-1.2.3** The insurance licensee must verify the information in Paragraph FC-1.2.1 (a) to (f), by the following methods below; 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);

(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 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-1.2.4** 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 insurance 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 insurance 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 policy, and nature and volume of anticipated business dealings with the insurance licensee; and
(k) Source of funds for payment of premium.

## 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 insurance services (only necessary in the case of private or unlisted companies);
(f) Identification documentation of the authorised signatories of the insurance contract;
(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 insurance contract and a Board resolution (or other applicable document) authorising the named signatories or their agent to receive any proceeds from the insurance contract or to modify the terms of the contract (resolution only necessary for private or unlisted companies).

**FC-1.2.8A** For customers that are legal persons, Insurance 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
(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 Face-to-face business (continued)

**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-1.6 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** **Insurance 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 provider of funds and 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, and for trustees in the case of trusts);**

**(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;**

**(f) In the case of trusts or similar arrangements, establish the identity of the settlor(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 Face-to-face business (continued)

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** **In the case of group insurance policies (such as group life or medical insurance), customer identification may be limited to the principal shareholders and Directors of the contracting company.**

## 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. If the insurance licensee determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it must take enhanced measures which must include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.**

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 insurance 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-1.5 inclusive.

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

**FC-1.4.1** **Insurance 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, insurance 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, insurance 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 an insurance 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) Requiring a premium payment to be made from an account in the customer's name at a bank having equivalent CDD standards;

(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-1.4.4** **Financial services provided using digital channels or internet pose greater challenges for customer identification and AML/CFT purposes. Insurance 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. The risk assessments must be consistent with the requirements in Section FC-C.2.**

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

**FC-1.4.5** Insurance 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. Insurance licensees must take appropriate measures to manage and mitigate those risks.

***Enhanced Monitoring***

**FC-1.4.7** Customers onboarded 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.

***Licensee's digital ID applications***

**FC- 1.4.9** Insurance 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 Enhanced Customer Due Diligence: Non face-to-face Business and New Technologies

**FC-1.4.10** Insurance 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** Insurance 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;

(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;

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

(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** Insurance 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** Insurance 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

**FC-1.4.14** Insurance 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** Insurance 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 insurance licensee.

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

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 insurance 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.3.1.**

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

**FC-1.5.1** Insurance 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. Licensees must utilise publicly available databases and information to establish whether a customer is a PEP.

**FC-1.5.2** Insurance 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, insurance licensees must apply the measures referred to in Subparagraphs FC-1.5.3 (b), (d) and (e).

**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')

FC-1.5.4 [This Paragraph was deleted in July 2016 as definition is included under Part B in the Glossary.]

**FC-1.5.5** **In relation to life insurance policies, insurance licensees must take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This must occur, at the latest, at the time of the pay-out.**

**FC-1.5.6** **Where higher risks are identified, senior management must be informed before the pay-out of the policy proceeds, in order to conduct enhanced scrutiny on the whole business relationship with the policyholder, and to consider making a suspicious transaction report.**

## FC-1.5A Enhanced Due Diligence: Charities, Clubs and Other Societies

**FC-1.5A.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. Charities should be subject to enhanced monitoring by insurance licensees.

**FC-1.5A.2** For the purpose of Paragraph FC-1.5A.1, for clubs and societies registered with the Ministry of Youth and Sport Affairs, insurance licensees must contact the Ministry to clarify whether a policy may be issued in accordance with the rules of the Ministry. In addition, in the case of sport associations registered with the Bahrain Olympic Committee (BOC), insurance licensees must contact BOC to clarify whether the policy may be issued in accordance with the rules of BOC.

## FC-1.6 Simplified Customer Due Diligence

**FC-1.6.1** Insurance licensees may apply simplified customer due diligence measures, as described in Paragraphs FC-1.6.2 to FC-1.6.8, 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 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 with 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 that 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; or

(f) [This Subparagraph was deleted in January 2018].

(g) The transaction is a long-term insurance contract, either taken out in connection with a pension scheme relating to the customer's employment or occupation, or contains a no surrender clause and cannot be used as security for a loan.

**FC-1.6.2** For customers falling under the categories (a) to (e) specified in Paragraph FC-1.6.1, 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.

## FC-1.6 Simplified Customer Due Diligence (continued)

**FC-1.6.3** **[This Paragraph was deleted in July 2018].**

**FC-1.6.4** **Insurance licensees wishing to apply simplified due diligence measures as allowed for under Paragraph FC-1.6.1 must retain documentary evidence supporting their categorisation of the customer.**

FC-1.6.5 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-1.6.6** **For customers coming under Paragraph FC-1.6.1 (e), 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-1.6.7 [This Paragraph was deleted in January 2007].

**FC-1.6.8** **Simplified customer due diligence measures must not be applied where a 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-1.6.8A** **Simplified customer due diligence measures must not be applied in situations where the licensee has identified high ML/TF/PF risks.**

**FC-1.6.9** **[This Paragraph was deleted in July 2018].**

FC-1.6.10 [This Paragraph was deleted in July 2018].

## FC-1.7 Introduced Business from Professional Intermediaries

**FC-1.7.1** Insurance licensees may only accept customers introduced to them by other financial institutions or intermediaries, if they have satisfied themselves that the financial institution or intermediary concerned is subject to FATF-equivalent measures and customer due diligence measures. Where an insurance licensee delegates part of the customer due diligence measures to another financial institution or intermediary, the responsibility for meeting the requirements of this Chapter remains with the insurance licensee, not the third party.

**FC-1.7.2** Insurance 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 is able to provide all relevant data pertaining to the customer's identity, the identity of the policyholder and beneficiary of the policy and, where applicable, the party/parties on whose behalf the customer is acting; also, the introducer has confirmed that the 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 insurance licensee and that these documents will be kept for at least five years after the policy relationship has ended.

## FC-1.7 Introduced Business from Professional Intermediaries (continued)

**FC-1.7.3** The insurance 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 insurance licensee must also require the introducer to perform periodic reviews to verify whether the jurisdiction is in compliance with the FATF Recommendations.

**FC-1.7.4** Should the insurance 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 or not accept or continue the business relationship.

## FC-2.1 General Requirements

**FC-2.1.1** **Insurance 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 Where the insurance licensee is an unincorporated entity, the annual review and approval should be undertaken by the most senior person with oversight responsibilities for the licensee, such as its General Manager or managing partner.

FC-2.1.3 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-2.1.4** **Insurance 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-5.4.3).**

FC-2.1.5 In implementing the policies, procedures and monitoring tools for ensuring compliance with Paragraph FC-2.1.4, insurance licensees should consider the following:

(a) The business policies and practices should be designed to reduce incentives for staff to expose the insurance 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** **Insurance 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 Insurance 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 patter of a customer's account activity.

***Automated Transaction Monitoring***

**FC-2.2.3** **Insurance licensees must consider the need to include automated transaction monitoring as part of their risk-based monitoring systems. 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 insurance licensee for five years after the date of the transaction.**

FC-2.2.4 The CBB would expect larger insurance licensees to include automated transaction monitoring as part of their risk-based monitoring systems. See also Chapters FC-3 and FC-6, 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** **In instances where an insurance 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, insurance 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-6.1.1 (b)).**

**FC-2.2.7** **Insurance licensees must consider instances where there is a significant, unexpected or unexplained change in the behaviour of policyholders' account (e.g., early surrenders). Insurance licensees must be extra vigilant to the particular risks involved in the buying and selling of second hand endowment policies, as well as the use of single premium unit-linked policies. Insurance licensees must check any reinsurance or retrocession to ensure that monies are paid to bona fide reinsurance entities at rates commensurate with the risks underwritten.**

**FC-2.2.8** **When an existing customer cancels a policy and applies for another, the insurance 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-6, 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** Insurance 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 Insurance 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. Insurance licensees must require all customers to provide up-to-date identification documents in their standard terms and conditions of business.

**FC-2.2.11** Insurance 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 insurance licensee must take steps to obtain updated copies as soon as possible.

## FC-3.1 Appointment of MLRO

**FC-3.1.1** **Insurance firms (except captive insurance firms managed by an insurance manager), insurance brokers and insurance managers (that manage a captive insurance firm) must appoint a Money Laundering Reporting Officer ('MLRO'). In the case of insurance managers that manage captive insurance firms, the insurance manager must appoint a MLRO for each of the captive insurance firms under its management.**

FC-3.1.2 Insurance managers may nominate the same individual to act as MLRO for more than one captive insurance firm, providing this person can meet in full the responsibilities of MLRO for each captive insurance firm in question.

**FC-3.1.3** **The position of MLRO is a controlled function and the MLRO is an approved person.**

FC-3.1.4 For details of the CBB's requirements regarding controlled functions and approved persons, see Section AU-1.2. Amongst other things, approved persons require CBB approval before being appointed, which is granted only if they are assessed as 'fit and proper' for the function in question. A completed Form 3 must accompany any request for CBB approval.

**FC-3.1.5** **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-3.1.6 Subject to Paragraph FC-3.1.5, however, the position of MLRO may otherwise be combined with other functions in the insurance 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-3.1.9 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-3.1.6A For purposes of Paragraphs FC-3.1.5 and FC-3.1.6 above, insurance 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 insurance licensee.

**FC-3.1.7** **Insurance licensees must appoint at least one deputy MLRO (or more depending on the scale and complexity of the licensee's operations). The deputy MLRO(s) must be resident in Bahrain unless otherwise agreed with the CBB.**

## FC-3.1 Appointment of MLRO (continued)

FC-3.1.7.A The deputy MLRO should be able to support the MLRO discharge his responsibilities and to deputise for him in his absence. In the case of insurance licensees undertaking significant overseas business, the CBB would normally expect to see one or more deputy MLRO(s) residing in the jurisdiction(s) where the bulk of the customer business is processed. In such cases, the CBB would normally agree to an application for an exemption from the residency requirement in Rule FC-3.1.7.

FC-3.1.8 Insurance licensees should note that although the MLRO may delegate some of his functions, either to other employees of the licensee or even (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-3.1.9** **So that he can carry out his controlled function effectively, insurance 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 insurance 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 insurance licensee to a customer, or any transactions conducted by the insurance 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 insurance licensee; and**

**(g) Is resident in Bahrain.**

## FC-3.1 Appointment of MLRO (continued)

**FC-3.1.10** In addition, insurance licensees must ensure that their MLRO is able to:

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

(b) Respond promptly to any reasonable request for information made by the Financial Intelligence Directorate or the CBB.

**FC-3.1.11** If the position of MLRO falls vacant, the insurance 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-3.2 Responsibilities of the MLRO

**FC-3.2.1** The MLRO is responsible for:

(a) Establishing and maintaining the insurance 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 this Module;

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

(d) Acting as the insurance licensee's main point of contact in respect of handling internal suspicious transactions reports from the licensee's staff (refer to Section FC-4.1) 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-4.2);

(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-3.3.3;

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

(i) Ensuring that the insurance licensee maintains all necessary CDD, transactions, STR and staff training records for the required periods (refer to Section FC-6.1).

## FC-3.3 Compliance Monitoring

***Annual Compliance Review***

**FC-3.3.1** **Insurance 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-3.3.1A Insurance 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-3.3.1B** **An insurance licensee must review the effectiveness of its AML/CFT procedures, systems and controls at least once each calendar year. The review must cover the licensee and its branches and subsidiaries both inside and outside the Kingdom of Bahrain. An insurance 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-4.1, 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-4.2 and, where an insurance 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 licensee's anti-money laundering procedures, systems and controls, and compliance with the AML Law and this Module.**

## FC-3.3 Compliance Monitoring (continued)

**FC-3.3.2** **The reports listed under Paragraph FC-3.3.1B (a) and (b) must be made by the MLRO. The sample testing and report required under Paragraph FC-3.3.1B (c) and (d) must be made by the licensee's external auditor or a consultancy firm approved by the CBB.**

FC-3.3.2A In order for a consultancy firm to be approved by the CBB for the purposes of Paragraph FC-3.3.2, 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-3.3.2B 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-3.3.2C At least two persons working on the report (one of whom would normally expected to be the team leader) should have:

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

FC-3.3.2D 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-3.3.2E 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-3.3 Compliance Monitoring (continued)

**FC-3.3.3** **The items listed under Paragraph FC-3.3.1B 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-3.3.4 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-4), 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). Licensees should use their judgement as to how the reports listed under Paragraph FC-3.3.1B (a) and (b) should be broken down in order to achieve this aim (e.g. by branches, departments and product lines).

**FC-3.3.5** **Insurance licensees must instruct their appointed firm to produce the report referred to in Paragraph FC-3.3.1B (c) and (d). The report must be submitted to 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-3.3.5A [This Paragraph was deleted in January 2019].

FC-3.3.6 [This Paragraph was deleted in January 2022].

**FC-3.3.7** **[This Paragraph was deleted in January 2022].**

## FC-4.1 Internal Reporting

**FC-4.1.1** **Insurance 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 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-4.1.2 Suspicious transaction or conduct may include a claim made in suspicious circumstances, a policy surrendered soon after inception or in circumstances that would otherwise appear contrary to the interests of a reasonable policyholder. If a prospective policyholder does not pursue an application, this may be considered suspicious in itself. Item FC (iv) in Part B of Volume 3 (Insurance) provides further examples of transactions that may be suspicious or unusual.

**FC-4.1.3** **Where insurance 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-4.2 External Reporting

**FC-4.2.1** Insurance licensees must take reasonable steps to ensure that all reports made under Section FC-4.1 are considered by the MLRO (or his duly authorised delegate). Having considered the report and any other relevant information, if the MLRO (or his duly authorised delegate) still suspects that a person has been engaged in money laundering or terrorism financing, or the activity concerned is otherwise still regarded as suspicious, he must report the fact promptly to the relevant authorities. Where no report is made, the MLRO must document the reasons why.

**FC-4.2.2** To take reasonable steps, as required under Paragraph FC-4.2.1, insurance licensees must:

(a) Require the MLRO to consider reports made under Section FC-4.1 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 insurance 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-4.2.3** Reports to the relevant authorities made under Paragraph FC-4.2.1 must be sent to the Financial Intelligence Directorate at the Ministry of Interior and the CBB's Compliance Directorate using the Suspicious Transaction Reporting Online System (Online STR system). STRs in paper format will not be accepted.

**FC-4.2.4** Insurance licensees must report all suspicious transactions or attempted transactions. This reporting requirement applies regardless of whether the transaction involves tax matters.

## FC-4.2 External Reporting (continued)

**FC-4.2.5** Insurance licensees must retain all relevant details of STRs submitted to the relevant authorities, for at least five years.

**FC-4.2.6** In accordance with the AML Law, insurance licensees, their Directors, officers and employees:

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

(b) In cases where insurance 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 insurance 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-4.3 Contacting the Relevant Authorities

**FC-4.3.1** Reports made by the MLRO or his duly authorised delegate under Section FC-4.2 must be sent electronically using the Suspicious Transaction Reporting Online System (Online STR system).

**FC-4.3.2** 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-5.1 General Requirements

**FC-5.1.1** **An insurance 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 insurance 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 insurance licensee's procedures for making internal STRs; and**
**(h) Customer due diligence measures with respect to establishing business relations with customers.**

**FC-5.1.2** **The information referred to in Paragraph FC-5.1.1 must be brought to the attention of relevant new employees of insurance licensees, and must remain available for reference by staff during their period of employment and by the CBB.**

**FC-5.1.3** Relevant new employees must be given AML/CFT training within three months of joining an insurance licensee.

**FC-5.1.4** Insurance 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-5.1.5 The CBB would normally expect AML/CFT training to be provided to relevant staff at least once a year.

**FC-5.1.6** Insurance 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 licensees.

**FC-5.1.6A** **[This Paragraph was deleted in January 2022].**

## FC-6.1 General Requirements

*Policyholder/Transaction Records*

**FC-6.1.1** **Insurance licensees must comply with the record-keeping requirements contained in the AML Law and the CBB Law. Insurance 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 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 enabling a reconstitution of the transaction concerned, for at least ten years after the transaction was completed.**

*Compliance Records*

**FC-6.1.2** **Insurance licensees must retain copies of the reports produced for their annual compliance review, as specified in Paragraph FC-3.3.1B, for at least five years. Licensees must also maintain for five years reports made to, or by, the MLRO made in accordance with Sections FC-4.1 and 4.2, 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-6.1.3** **Insurance 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-6.1.4** **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-6.1.5 Insurance licensees are also reminded of the requirements contained in Chapter GR-1 (Books and Records).

## FC-7.1 Special Measures for Non-Cooperative Countries or Territories ('NCCTs')

**FC-7.1.1** **Insurance 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 insurance licensees from time to time by the CBB.**

**FC-7.1.2** **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-4.2.**

**FC-7.1.3** **Insurance 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-7.1.4 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-7.2 Terrorist Financing

**FC-7.2.1AA** **Insurance licensees must implement and comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. Insurance 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-7.2.1** **Insurance licensees must comply in full with the provisions of the UN Security Council Anti-terrorism Resolution No. 1373 of 2001 ('UNSCR 1373').**

**FC-7.2.2** **[This Paragraph was deleted in January 2018].**

FC-7.2.3 A copy of UNSCR 1373 is included in Part B of Volume 3 (Insurance), under 'Supplementary Information'.

**FC-7.2.4** **Insurance 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; and**
**(b) All claims, whether actual or contingent, which the insurance licensee has on persons and entities which may be the subject of Article 1, Paragraphs (c) and (d) of UNSCR 1373.**

FC-7.2.5 For the purposes of Paragraph FC-7.2.4, '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-7.2.6** **All reports or notifications under this Section must be made to the CBB's Compliance Directorate.**

FC-7.2.7 See Section FC-4.3 for the Compliance Directorate's contact details.

## FC-7.3 Designated Persons and Entities

**FC-7.3.1** **Without prejudice to the general duty of all insurance 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, insurance licensees must not deal with any persons or entities designated by the CBB as potentially linked to terrorist activity.**

FC 7.3.2 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 the CBB include persons and entities designated by the United Nations, under UN Security Council Resolution 1267 ("UNSCR 1267").

**FC-7.3.3** **Insurance licensees must report to the relevant authorities, using the procedures contained in Section FC-4.2, details of any accounts or other dealings with designated persons and entities, and comply with any subsequent directions issued by the relevant authorities.**

## FC-8.1 Regulatory Penalties

**FC-8.1.1** **The requirements in this Module are legally binding. 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-8.1.2 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-5.2.3). Other enforcement measures may also be applied by the 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-8.1.3 The CBB will endeavour to assist insurance licensees to interpret and apply the requirements of this Module. Insurance licensees may seek clarification on any issue by contacting the Compliance Directorate (see Section FC-4.3 for contact details).

FC-8.1.4 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-9.1 Guidance Provided by International Bodies

### *FATF Recommendations*

FC-9.1.1 The Financial Action Task Force (FATF) Recommendations (see www.fatf-gafi.org) (together with their associated interpretative notes and best practices papers) provide the basic framework for combating money laundering activities and the financing of terrorism. FATF Recommendations 9-12, 15-17, 18-21, 26-27, 33-35, 37 and 40 and the AML/CFT Methodology are specifically relevant to the insurance sector.

FC-9.1.2 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.

### *IAIS: Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism*

FC-9.1.3 In January 2002, the International Association of Insurance Supervisors (IAIS) issued *Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities*. This document was updated in October 2004 and was reissued as *Guidance Paper No. 5: Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism* (see www.iaisweb.org/publication ). The Guidance Paper includes a set of measures and procedures, including elements of customer due diligence (CDD), reporting of suspicious transactions and measures affecting the organisation and staff of insurance licensees.

FC-9.1.4 The CBB supports the above papers and the desirability of all insurance licensees adhering to their requirements and guidance.

### *Other Website References Relevant to AML/CFT*

FC-9.1.5 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 .

## FC-10.1 General Requirements

**FC-10.1.1** **Insurance licensees must ensure that they allocate appropriate resources and have in place systems and controls to deter, detect, and record instances of fraud or attempted fraud.**

FC-10.1.2 Fraud may arise from internal sources originating from changes or weaknesses to processes, products and internal systems and controls. Fraud can also arise from external sources, such as claims fraud.

**FC-10.1.3** **Any actual or attempted fraud incident (however small) must be reported to the appropriate authorities (including the CBB) and followed up. Monitoring systems must be designed to measure fraud patterns that might reveal a series of related fraud incidents.**

**FC-10.1.4** **Insurance licensees must ensure that a person is given overall responsibility for the prevention, detection and remedy of fraud, at a senior level of the organisation.**

**FC-10.1.5** **Insurance licensees must ensure the effective segregation of functions and responsibilities, between different individuals and departments, such that the possibility of financial crime is reduced and that no single individual is able to initiate, process and control a transaction.**

**FC-10.1.6** **Insurance licensees must provide regular training to their management and staff, to make them aware of potential fraud risks.**

***Advance Fee Fraud***

FC-10.1.7 In a number of jurisdictions, there have been a number of recent incidents whereby insurance entities have either been the victims of, or have inadvertently provided assistance to, advance fee frauds. Advance fee fraud consists of setting up a fraudulent and almost certainly non-existent financial or banking transaction, the aim of which is to defraud an innocent third party of an up-front payment or deposit which is intended by the third party to be consideration for their involvement in that financial transaction, the receipt of a low interest or interest fee loan or the receipt of some other financial benefit. The types of transactions used as the façade for the frauds vary in detail, some of the most common are investment in financial instruments, self-liquidating loans and loans or other financial benefits. Although these transactions are generally based around banking or securities transactions, it is occasionally the case that the transaction will purport to be guaranteed by insurers.

## FC-10.1 General Requirements (continued)

FC-10.1.8 The most common type of advance fee fraud is for a fraudster to approach a company or sovereign state which has a poor credit rating or which is in some financial difficulty and offer to obtain funding at beneficial rates. Likewise, a potential investor may be approached and offered the opportunity to invest in a transaction with a very high rate of return. In each instance, the borrower or investor will be asked to provide some funds up front to cover the costs of setting up the transaction or by way of a deposit or down payment on fees. Once the fee has been paid, the fraudster will disappear and the transaction will, on further investigation, prove to be fictitious.

FC-10.1.9 Insurance licensees are encouraged to promote the exchange of information amongst themselves with respect to fraud and those committing fraud including, as appropriate, through the use of databases. Licensees should also consider the need to exchange information with the police and other external bodies.

FC-10.1.10 Insurance claims fraud is an offence punishable under the provision of Section 391 of the Penal Code, Decree Act No. (15), of 1976 of the Kingdom of Bahrain.

***Guidance Provided by the IAIS***

FC-10.1.11 In October 2006, the International Association of Insurance Supervisors (IAIS) issued *Guidance Paper on Preventing, Detecting and Remedying Fraud in Insurance* (see www.iaisweb.org/publication). The Guidance Paper has been developed to help the insurance sector prevent and detect cases of fraud. Insurance licensees should assess their own vulnerability and implement effective and efficient policies, procedures and controls to address the risk of fraud.