ANTI-MONEY LAUNDERING AND COMBATING OF FINANCIAL CRIME MODULE

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML: Table of Contents

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML: Table of Contents (continued)

APPENDICES (included in Volume 6 (Capital Markets), Part B)

CBB Reporting Forms

Supplementary Information

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-A: Introduction

AML-A.1 Purpose

Executive Summary

AML-A.1.1 This Module is a comprehensive framework of rules and guidance aimed at combating money laundering and terrorist financing and applies to all Capital Market Service Providers. 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 Capital Market Service Providers. It also helps implement IOSCO guidance in this area. The Module also contains measures relating to the combating of fraud in the capital market.

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

Legal Basis

AML-A.1.3 **This Module contains the Central Bank of Bahrain ('CBB') Directive (as amended from time to time) regarding the combating ~~of financial crime~~ money laundering and terrorism financing, and is issued under the powers available to the CBB under Article 38 of the Central Bank of Bahrain and Financial Institutions Law 2006 ('CBB Law'). The Directive in this Module is applicable to all Capital Market Service Providers.**

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

AML-A.2 Module History

Evolution of Module

AML-A.2.1 This Module was first issued in October 2010. Any material changes that have subsequently been made to this Module are annotated with the calendar quarter date in which the change is made; Chapter UG-3 provides further details on Rulebook maintenance and version control.

AML-A.2.2 Prior to the introduction of this Module, the CBB had issued various regulatory instruments containing requirements covering different aspects of financial crime. The CBB issued Ministerial Order No. 1 of 2004 with Respect to Directives Relating to the Prevention & Prohibition of Money Laundering at the Bahrain Stock Exchange (BSE) and this Order was applicable to the BSE, issuers of Securities, brokerage firms and offices, registration offices, issue underwriters, establishments accredited with receiving money relating to the subscription of Securities, custodians of Securities, banks accredited for clearance of transactions carried out at the BSE, dealers in Securities, and all other entities concerned with dealing in Securities.

AML-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
AML-A.1.3	07/2011	Clarified legal basis.
AML-7.1	07/2011	Clarified the Rules dealing with substantial shareholdings.
AML-4.2.3	10/2014	Updated method of submitting STRs.
AML-4.4	10/2014	Updated relevant authorities information.
AML	07/2016	Updated to reflect February 2012 update to FATF Recommendations.
AML-4.2.3	07/2016	Updated instructions for STR.
AML-1.2.9A	01/2017	Added guidance paragraph on CR printing
AML-1.1.2A	10/2017	Added new paragraph on the verification of identity and source of funds.
AML-1.1.2B	10/2017	Added new paragraph on the verification of identity and source of funds.
AML-1.2.7	10/2017	Amended paragraph.
AML-1.2.8A	10/2017	Added new paragraph on legal entities or legal arrangements CDD.
AML-2.2.10 – AML-2.2.11	10/2017	Amended paragraphs on On-going CSS and Transaction Monitoring.
AML-3.1.4A	10/2017	Added paragraph on combining the MLRO or DMLRO position with any other position within the licensee.
AML-B.2.4	01/2018	Amended paragraph.
AML-1.8.1	01/2018	Amended paragraph.
AML-1.10.1	01/2018	Deleted sub-paragraph (a).
AML-4.2.6	01/2018	Amended paragraph.
AML-9.1.4	01/2018	Amended paragraph.
AML-9.2.2	01/2018	Deleted paragraph.

AML-A.2 Module History (continued)

Module Ref.	Change Date	Description of Changes
AML-1.1.2	07/2018	Deleted Sub-paragraph (a).
AML-1.10.2	07/2018	Amended Paragraph deleting cross reference.
AML-1.10.3	07/2018	Deleted Paragraph.
AML-1.10.9	07/2018	Deleted Paragraph.
AML-1.10.1	01/2019	Amended references.
AML-3.3.2	01/2019	Amended references.
AML-3.3.4 – AML-3.3.5	01/2019	Amended references.
AML-1.2.9A	10/2019	Amended reference.
AML-1.9.2	10/2019	Amended authority name.
AML-3.1.8	10/2019	Amended authority name .
AML-3.2.1	10/2019	Amended authority name .
AML-4.2.3	10/2019	Amended authority name .
AML-4.4.2	10/2019	Amended authority name .
AML-7.1.2	10/2019	Deleted Paragraph.
AML-9.2.1AA	10/2019	Added a new Paragraph on Terrorist Financing.
AML-B.1.1	01/2020	Added " crypto-asset licensees".
AML-B.1.3	01/2020	Deleted Paragraph.
AML-B.3	01/2020	Deleted Section.
AML-C	01/2020	Added new Chapter "Risk Based Approach".
AML-1	01/2020	Rename the Chapter to "Customer Due Diligence".
AML-1.1.1	01/2020	Amended Paragraph on procedures approval.
AML-1.1.2	01/2020	Added sub-paragraph (i).
AML-1.1.14 – AML-1.1.16	01/2020	Added new paragraphs on "Suspicious Wallet Addresses".
AML-1.2.1	01/2020	Added sub-paragraph (n).
AML-1.2.5	01/2020	Added new sub-paragraph (f).
AML-1.3.4	01/2020	Added new paragraph.
AML-1.4.7	01/2020	Added new paragraph.
AML-1.5.4	01/2020	Deleted paragraph.
AML-1.9	01/2020	Rename the section to "Shell financial Institutions".
AML-1.9.1	01/2020	Amended paragraph.
AML-1.11	01/2020	Added new section "Enhanced Due Diligence for Correspondent Accounts"
AML-2.2.1	01/2020	Amended Paragraph.
AML-2A	01/2020	Added new chapter.
AML-3.1.5	01/2020	Amended Paragraph.
AML-3.1.5A	01/2020	Added Paragraph.
AML-3.1.7	01/2020	Amended sub-Paragraph (a).

AML-A.2 Module History (continued)

Module Ref.	Change Date	Description of Changes
AML-3.3.2	01/2020	Amended Paragraph.
AML-3.3.5	01/2020	Amended Paragraph on report submission date.
AML-3.3.2A – AML-3.3.2E	01/2020	Added Paragraphs.
AML-6.1.1A – AML-6.1.1C	01/2020	Added Paragraphs.
AML-8.1.1	01/2020	Deleted Paragraph.
AML-8.1.1A	01/2020	Added Paragraph.
AML-11.1.2	01/2020	Added paragraph.
AML-5.1.6A	01/2021	Added a new Paragraph on requirements to hire new employees.
AML-A.1.3	2021	Amended Paragraph to replace financial crime with money laundering and terrorism financing.
AML-C	2021	Replaced Introduction with risk-based approach (RBA).
AML-1.1	2021	Amendments to general requirements to introduce additional rules for non-resident customers, amendments to customers onboarded prior to full completion of customer due diligence, digital onboarding etc.
AML-1.2	2021	Amendments to recognise E-KYC and electronic documents law.
AML-1.3	2021	Amendments to introduce additional guidance in enhanced due diligence requirements.
AML-1.4	2021	Amendments to introduce detailed requirements for digital onboarding and related requirements.
AML-1.5.2	2021	Amendments relating to digital onboarding of Bahraini PEPs.
AML-1.10.8A	2021	Amended Paragraph.
AML-3.3.1B	2021	Amended Paragraph.

Superseded Requirements

AML-A.2.4 This Module supersedes the following provisions contained in Circulars or other regulatory instruments:

Circular/other references	Provision	Subject
Resolution No. 1 of 2004	All	In respect of the Directives Relating to the Prevention and Prohibition of Money Laundering at the Bahrain Stock Exchange

AML-A.3 Interaction with Other Modules

AML-A.3.1 All Capital Market Service Providers must comply with all the other relevant Modules in Volume 6 in addition to other applicable laws, rules and regulations.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-B: Scope of Application

AML-B.1 Scope of Application

AML-B.1.1 **This Module contains the CBB's Directive relating to Anti-Money Laundering and Combating of Financial Crime and is issued under the powers available to the CBB under Article 38 of the CBB Law. The Directive under this Module is applicable to all Capital Market Service Providers and relevant Persons, including but not limited to issuers of Securities or any Person acting on their behalf, licensed exchanges, licensed market operators, licensed clearing houses, depositories, investment firms, collective investment undertakings, business trusts, listed companies, crypto-asset licensees, any Person acting for or on behalf of listed companies, Persons accredited with receiving money relating to the subscription of Securities, custodian of Securities, settlement banks, dealers in Securities, share registrars, lead managers, underwriters, professional advisors, listing agents, auditors, financial analysts, credit rating agencies and any other Person concerned with dealing in Securities, irrespective of whether such Person is a Capital Market Service Provider or not. These rules are issued by way of a legally-binding Directive.**

AML-B.1.2 Capital Market Service Providers that are subsidiaries of an overseas based group may apply additional AML/CFT policies and procedures, provided they satisfy the minimum requirements contained in this Module.

AML-B.1.3 [This Paragraph was deleted in January 2020].

AML-B.1.4 The requirements of this Module are in addition to and supplement 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 Capital Market Service Providers). All Capital Market Service Providers are therefore under the statutory obligations of that Law, in addition to the more specific requirements contained in this Module. Nothing in this Module is intended to restrict the application of the AML Law (a copy of which is contained in Part B of Volume 6 Capital Markets), 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').

AML-B.2 Overseas Subsidiaries and Branches

AML-B.2.1 **Capital Market Service Providers must apply the requirements in this Module to all their branches and subsidiaries operating both in the Kingdom of Bahrain and in foreign jurisdictions. Where local standards differ, the higher standard must be followed. Capital Market Service Providers must pay particular attention to procedures in branches or subsidiaries in countries that do not or insufficiently apply the FATF Recommendations and do not have adequate AML/CFT procedures, systems and controls (see also Section AML-9.1).**

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

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

AML-B.2.4 **Financial groups 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;

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

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

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

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-B: This Section was deleted in January 2020

AML-B.3 [This Section was deleted in January 2020].

AML-C.1 ~~Introduction~~ Risk Based Approach

~~AML-C.1.1 The Risk Based Approach (RBA) is central to the effective implementation of the FATF Recommendations. The focus on risk is intended to ensure a Capital Market Service Provider is able to identify, assess and understand the money laundering, and terror financing and proliferation financing (ML/TF/PF) risks to which it is exposed to and take the necessary AML/CFT/CPF control measures to mitigate them.~~

~~AML-C.1.2 The Rules and Guidance in this Section seek to:~~

~~(a) Assist the Capital Market Service Provider to design and implement AML/CFT/CPF control measures by providing a common understanding of what the RBA encompasses; and~~

~~(b) Outline the recommended steps involved in applying the RBA. In the event a Capital Market Service Provider has developed its own RBA, the adopted RBA must be able to achieve the outcomes intended under this Section.~~

~~AML-C.1.3 The RBA:~~

~~(a) Recognizes that the ML/TF/PF threats to a Capital Market Service Provider vary across customers, geographies, products and services, transactions and distribution channels;~~

~~(b) Allows the Capital Market Service Provider to apply procedures, systems and controls to manage and mitigate the ML/TF/PF risks identified; and~~

~~(c) Facilitates the Capital Market Service Provider to allocate its resources and internal structures to manage and mitigate the ML/TF/PF risk identified.~~

~~AML-C.1.4 The RBA provides an assessment of the threats and vulnerabilities of the Capital Market Service Provider from being used as a conduit for ML/TF/PF. By regularly assessing the Capital Market Service Provider's ML/TF/PF risks, it allows the CMSP to protect and maintain the integrity of its business and the financial system as a whole.~~

AML-C.1.5 **Capital Market Service Providers 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.**

AML-C.1 ~~Introduction~~ Risk Based Approach

AML-C.1.6 Capital Market Service Providers must perform enhanced measures where higher ML/TF/PF risks are identified to effectively manage and mitigate those higher risks.

AML-C.1.7 Capital Market Service Providers must maintain and regularly review and update the documented risk assessment. The risk management and mitigation measures implemented by a Capital Market Service Provider must be commensurate with the identified ML/TF/PF risks.

AML-C.1.8 Capital Market Service Providers must allocate adequate financial, human and technical resources and expertise to effectively implement and take appropriate preventive measures to mitigate ML/TF/PF risks.

AML-C.2 Risk Assessment

~~AML-C.2.1~~ ~~A Capital Market Service Provider must ensure that its policies and procedures to identify, assess, monitor, manage and mitigate ML/TF/PF risks are commensurate with the nature, scale and complexities of its activities.~~

~~AML-C.2.2~~ ~~A Capital Market Service Provider must take steps to identify, assess and understand their ML/TF/PF risks in relation to its:~~

~~(a) Customers;~~

~~(b) The countries or jurisdictions its customers are from or in;~~

~~(c) The countries or jurisdictions the Capital Market Service Provider operates in; and~~

~~(d) The products, services, transactions or delivery channels of the Capital Market Service Provider.~~

~~AML-C.2.3~~ ~~In assessing ML/TF/PF risks referred to in AML-C.2.2, a Capital Market Service Provider is required to have the following processes in place:~~

~~(a) Documenting its risk assessments and findings;~~

~~(b) considering all the relevant risk factors before determining what is the level of overall risk profile and the appropriate level and type of mitigation to be applied;~~

~~(c) Keeping the assessment up-to-date through a periodic review conducted at least annually; and~~

~~(d) Having appropriate and clearly defined mechanisms to provide risk assessment information to the CBB.~~

~~AML-C.2.4~~ ~~A Capital Market Service Provider must conduct additional risk assessments as may be required by the CBB, which may include expanding relevant risk factors or increasing the frequency of reviews.~~

AML-C.2 Risk Assessment (continued)

~~*Customer Risk Profile*~~

~~AML-C.2.5~~ ~~A Capital Market Service Provider must implement and maintain appropriate policies and procedures to conduct risk assessment of its customers during the establishment of the business relationship as well as throughout the course of that relationship. Capital Market Service Providers 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.~~

~~AML-C.2.6~~ ~~While there is no agreed upon set of risk factors and no single methodology to apply these risk factors in determining the ML/TF/PF risk of customers, a Capital Market Service Provider must establish an appropriate set of risk factors which, among others, include:~~

~~(a) Country risk: Customers with residence in or connection with high risk jurisdictions;~~

~~(b) Customer risk: type of customers e.g. resident or non-resident, occasional or one-off, legal person structure, status as PEP, occupation;~~

~~(c) Products, services and transactions risk: services that inherently provide more anonymity, ability to pool underlying customers/funds or cash-based or face-to-face or non face-to-face or domestic or cross-border; and~~

~~(d) Delivery/distribution channel risk: The distribution channel for products may alter the risk profile of a customer. This may include sales through online, postal or telephone channel where a non-face-to-face account opening approach is used. Distribution or sale of products through intermediaries may also increase risk as the business relationship between the customer and the Capital Market Service Provider becomes indirect.~~

AML-C.2.7 Capital market service providers 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.

AML-C.2 Risk Assessment (continued)

AML-C.2.8 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.

AML-C.2.9 The risk assessment must be properly documented, regularly updated and communicated to the capital market service provider'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 capital market service provider 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.

AML-C.2.10 Capital market service providers 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;

AML-C.2 Risk Assessment (continued)

g) The distribution channels, including the extent to which the Capital market service provider deals directly with the customer and the extent to which it relies (or is allowed to rely) on third parties to conduct CDD and the use of technology; and

h) Internal audit, external audit or regulatory inspection findings.

Country/Geographic risk

AML-C.2.11 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

AML-C.2.12 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;

AML-C.2 Risk Assessment (continued)

(h) Customer is a PEP or customer's family members, or close associates are PEPs (including where a beneficial owner of a customer is a PEP);
(i) Customer resides in or whose primary source of income originates from high-risk jurisdictions;
(j) Customer resides in countries considered to be uncooperative in providing beneficial ownership information; customer has been mentioned in negative news reports from credible media, particularly those related to predicate offences for AML/CFT/CPF or to financial crimes;
(k) Customer's transactions indicate a potential connection with criminal involvement, typologies or red flags provided in reports produced by the FATF or national competent authorities;
(l) Customer is engaged in, or derives wealth or revenues from, a high-risk cash-intensive business;
(m) The number of STRs and their potential concentration on particular client groups;
(n) Customers who have sanction exposure; and
(o) Customer has a non-transparent ownership structure.

Product/Service/Transactions risk

AML-C.2.13 An overall risk assessment should include determining the potential risks presented by product, service, transaction or the delivery channel of the Capital market service providers. A Capital market service provider 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.

AML-C.2.14 Determining the risks of product, service, transaction or the delivery channel offered to customers may include a consideration of their attributes, as well as any associated risk mitigation measures. Products and services that may indicate a higher risk include:
(a) Private banking;
(b) Anonymous transactions (which may include cash);
(c) Non-face-to-face business relationships or transactions;
(d) Payment received from unknown or un-associated third parties;
(e) Products or services that may inherently favour anonymity or obscure information about underlying customer transactions;
(f) The geographical reach of the product or service offered, such as those emanating from higher risk jurisdictions;
(g) Products with unusual complexity or structure and with no obvious economic purpose;
(h) Products or services that permit the unrestricted or anonymous transfer of value (by payment or change of asset ownership) to an unrelated third party, particularly those residing in a higher risk jurisdiction; and

AML-C.2 Risk Assessment (continued)

(a) Use of new technologies or payment methods not used in the normal course of business by the conventional bank licensee.

Distribution channel risk

AML-C.2.15 A customer may request transactions that pose an inherently higher risk to the conventional bank licensee. Factors that may be considered as indicators of higher risk include:

(a) A request is made to transfer funds to a higher risk jurisdiction/country/region without a reasonable business purpose provided; and

(b) A transaction is requested to be executed, where the licensee is made aware that the transaction will be cleared/settled through an unregulated entity.

AML-C.2.16 Capital market service providers 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 Capital market service provider. Capital market service providers 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.

AML-C.3 Risk Management and Mitigation

AML-C.3.1 A Capital Market Service Provider must:

(a) Develop and implement policies, which are approved by the Board of Directors and procedures and controls, which are approved by senior management, to enable the Capital Market Service Provider to effectively manage and mitigate the risks that have been identified by the Capital Market Service Provider or notified to it by the CBB;

(b) Monitor the implementation of those policies, procedures and controls and enhance them if necessary; and

(c) Perform enhanced measures where higher risks are identified, to effectively manage and mitigate those higher risks.

AML-C.3.2 The risk management and mitigation measures implemented by a Capital Market Service Provider must be commensurate with the risk profile of a particular customer or type of customer.

AML-C.3.3 Upon the initial acceptance of the customer, a Capital Market Service Provider must regularly review, especially when there is a change in the customer risk profile, and update the customer's risk profile based on their level of ML/TF/PF.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-1: Customer Due Diligence Requirements

AML-1.1 General Requirements

Verification of Identity and Source of Funds

AML-1.1.1 Capital Market Service Providers 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 Capital Market Service Provider's senior management and must be strictly adhered to.

AML-1.1.2 Capital Market Service Providers must implement the customer due diligence measures outlined in Chapter AML-1 when:

(a) [This Sub-paragraph was deleted in July 2018];
(b) Establishing business relations with a new or existing customer;
(c) A change to the signatory or beneficiary of an existing account or business relationship is made;
(d) Customer documentation standards change substantially;
(e) The Capital Market Service Provider has doubts about the veracity or adequacy of previously obtained customer due diligence information;
(f) A significant transaction takes place (as per rule AML-2.2.3);
(g) There is a material change in the way that an account is operated or in the manner in which the business relationship is conducted;
(h) There is a suspicion of Money Laundering or terrorist financing; or
(i) Carrying out accepted crypto-assets transfers and/or wire transfers irrespective of value and/or amount.

AML-1.1.2A Capital Market Service Providers must understand, and as appropriate, obtain information on the purpose and intended nature of the business relationship.

AML-1.1.2B Capital Market Service Providers must conduct ongoing due diligence on the business relationship, including:

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

AML-1.1 General Requirements (continued)

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

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

AML-1.1.3 For the purposes of this Module, 'customer' includes counterparties such as financial markets counterparties, except where Capital Market Service Providers are acting as principals where simplified due diligence measures may apply. These simplified measures are set out in section AML-1.10.

AML-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 AML-1.2. Enhanced requirements apply under certain high-risk situations: these requirements are contained in sections AML-1.3 to AML-1.7 inclusive. Additional requirements apply where a Capital Market Service Provider is relying on a professional intermediary to perform certain parts of the customer due diligence process: these are detailed in section AML-1.8. Simplified customer due diligence measures may apply in defined circumstances: these are set out in section AML-1.10.

Verification of Third Parties

AML-1.1.5 **Capital Market Service Providers must obtain a signed statement, in hard copy or through digital means from all new customers (or for one-off transactions above the BD6,000 threshold) confirming whether or not the customer is acting on his ~~their~~ own behalf or not. This undertaking must be obtained prior to conducting any transactions with the customer concerned.**

AML-1.1 General Requirements (continued)

AML-1.1.6 Where a customer is acting on behalf of a third party, the Capital Market Service Provider 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 Capital Market Service Provider 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.

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

AML-1.1.8 Where capital market services are provided to a minor or other person lacking full legal capacity, the normal identification procedures as set out in this Chapter must be followed. In the case of minors, Capital Market Service Providers must additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open business relations, the Capital Market Service Provider must establish the identity of that third party, as well as the person conducting the business.

AML-1.1 General Requirements (continued)

Anonymous and Nominee Accounts

AML-1.1.9 Capital Market Service Providers must not establish or keep anonymous accounts or accounts in fictitious names. Where Capital Market Service Providers 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 Capital Market Service Provider and verified by it in accordance with the requirements specified in this Chapter.

Timing of Verification

AML-1.1.10 Capital Market Service Providers must not commence a business relationship or undertake a~~n occasional~~ transaction (above the threshold) with a customer before completion of the relevant customer due diligence ('CDD') measures specified in Chapter AML-1. Capital Market Service Providers 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 ~~face-to face contact, providing~~ provided that no disbursement of funds takes place until after the requirements of this Chapter have been fully met.

AML-1.1 General Requirements (continued)

Incomplete Customer Due Diligence

AML-1.1.11 **Where a Capital Market Service Provider is unable to comply with the requirements specified in Chapter AML-1, it must consider whether to terminate the relationship or not proceed with the transaction. If it proceeds with the transaction (to avoid tipping off the customer), it should additionally consider whether it should file a Suspicious Transaction Report.**

AML-1.1.12 See also Chapter AML-4, which covers the filing of Suspicious Transaction Reports.

AML-1.1.13 The CBB will monitor the application of these requirements to Capital Market Service Providers' existing customer base.

Suspicious Wallet Addresses

AML-1.1.14 **A crypto-asset licensee must establish and implement policies for identification of wallet addresses that are suspected of ML/TF (suspicious wallet addresses).**

AML-1.1.15 **A crypto-asset licensee must not establish or continue business relationship with or transact with suspicious wallet addresses referred to in Paragraph-1.1.14.**

AML-1.1.16 **Where a crypto-asset licensee identifies or becomes aware of a suspicious wallet address, it must immediately file a Suspicious Transaction Report (STR) and also notify the CBB.**

Non-Resident Accounts

AML-1.1.17 **Capital Market Service Providers that establish a business relationship or transact or deal with non-resident customers must have documented criteria for acceptance of business with such persons. For non-resident customers, licensees must ensure the following:**

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

AML-1.1 General Requirements (continued)

AML-1.1.18 Capital Market Service Providers that establish a business relationship or transact or deal with non-resident customers must have documented approved policies in place setting out the products and services which will be offered to non-resident customers. Such policy document must take into account a comprehensive risk assessment covering all risks associated with the products and services offered to non-residents. The licensee must also have detailed procedures to address the risks associated with the dealings with non-resident customers including procedures and processes relating to authentication, genuineness of transactions and their purpose.

AML-1.1.19 Capital Market Service Providers must not accept non-residents customers from high risk jurisdictions subject to a call for action by FATF.

AML-1.1.20 Capital Market Service Providers 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 AML-1.1.19; and
(c) Countries that are the subject of any other sanctions.

AML-1.1.21 Capital Market Service Providers that deal with non-resident customers, other than with financial institutions, listed companies and governmental authorities in FATF countries referred to in AML-1.10.1, 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.

AML-1.1.22 Capital Market Service Providers 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.

AML-1.1 General Requirements (continued)

AML-1.1.23 Capital Market Service Providers 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.

AML-1.1.24 Capital Market Service Providers must ensure that only the official/government documents are accepted for the purpose of information in Subparagraphs AML-1.2.1 (a) to (f) in the case of non-resident customers.

AML-1.1.25 Customers residing outside Bahrain, are subject to the enhanced customer due diligence measures outlined in Section AML-1.3. Capital market service providers must not establish a business relationship or transact or deal with natural persons residing outside the GCC through a digital onboarding process.

AML-1.2 Face-to-Face Business

Natural Persons

AML-1.2.1 If the customer is a natural Person, Capital Market Service Providers must identify the person's identity and obtain the following information before providing capital market services, as described in paragraph AML-1.1.2:

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

AML-1.2.1A Capital Market Service Providers 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 AML-1.2.1 (k) above.

AML-1.2.2 See the Guidance Notes (filed under Supplementary Information in Part B of Volume 6) for further information on source of funds (rule AML-1.2.1 (l)) and CDD requirements for Bahrain residents (rule AML-1.2.1 (c) & (f)).

AML-1.2 Face-to-Face Business (continued)

AML-1.2.3 Capital market Service Providers 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, ~~by taking~~ obtaining a copy of a current valid official original identification document (e.g. birth certificate, passport, national identity card, CPR or Iqama ~~residence permit number~~);

(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.

AML-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 Capital Market Service Provider must certify the copy, by writing on it the words 'original sighted', together with the date and his name and signature. Equivalent measures must be taken for electronic copies.

AML-1.2.5 Identity documents which are not obtained by an authorised official of the Capital Market Service Provider in original form (e.g. due to a customer sending a copy by post following an initial meeting) must instead be certified (as per rule AML-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;
(f) An official of another licensed financial institution or of an associate company of the licensee.

AML-1.2 Face-to-Face Business (continued)

AML-1.2.6 The individual making the certification under rule AML-1.2.5 must give clear contact details (e.g. by attaching a business card or company stamp). The Capital Market Service Provider 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)

AML-1.2.7 If the customer is a legal entity or a legal arrangement such as a company or trust, the Capital Market Service Provider must obtain and record the following information from original identification documents, databases, or websites, in hard copy or electronic form, identify the customer and to take reasonable measures to verify its identity,:

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

AML-1.2 Face-to-Face Business (continued)

AML-1.2.8 The information provided under rule AML-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) Partnership agreement;
(c) Board resolution seeking the capital market services (only necessary in the case of private or unlisted companies);
(d) Identification documentation of the authorised signatories of the account (certification not necessary for companies listed in a GCC/FATF state);
(e) Copy of the latest financial report and accounts, audited where possible (audited copies do not need to be certified);
(f) List of Persons authorised to do business on behalf of the company and in the case of the opening of an account, a Board resolution (or other applicable document) authorising the named Persons to operate the account (resolution only necessary for private or unlisted companies); and
(g) Memorandum and Articles of Association.

AML-1.2.8A For customers that are legal persons, Capital Market Service Providers 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.

AML-1.2 Face-to-Face Business (continued)

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

AML-1.2.9A For the purpose of Subparagraph AML-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".

AML-1.2.10 The documentary requirements in rule AML-1.2.8 above do not apply in the case of listed companies from countries which are members of FATF/GCC: see section AML-1.8 below. Also, the documents listed in rule AML-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.

AML-1.2.11 **Capital Market Service Providers must also obtain and document the following due diligence information. These due diligence requirements must be incorporated in the Capital Market Service Providers' new business procedures:**

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

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

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

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

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

(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 Capital Market Service Provider has reasonable grounds for questioning the authenticity of the information supplied by a customer, conduct additional due diligence to confirm the above information.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-1: Customer Due Diligence Requirements

AML-1.2 Face-to-Face Business (continued)

AML-1.2.12 For the purposes of rule AML-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, if they are listed); 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.

AML-1.2.13 In cases where a Capital Market Service Provider is providing investment management services to a regulated mutual fund, and is not responsible for receiving investors' funds (being paid into the fund), it may limit its CDD to confirming that the administrator of the fund is subject to FATF-equivalent customer due diligence measures (see section AML-1.7 for applicable measures). Where there are reasonable grounds for believing that investors' funds being paid into the fund are not being adequately verified by the administrator, then the Capital Market Service Provider should consider terminating its relationship with the fund.

AML-1.3 Enhanced Customer Due Diligence: General Requirements

AML-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 capital market service provider 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.**

AML-1.3.2 Capital market service providers 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, capital market service providers 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 AML-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 Capital Market Service Provider);
(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.

AML-1.3 Enhanced Customer Due Diligence: General Requirements

AML-1.3.3 In addition to the general rule contained in rule AML-1.3.1 above, special care is required in the circumstances specified in sections AML-1.4 to AML-1.8 inclusive.

AML-1.3.4 Additional enhanced due diligence measures for non-resident account holders may include the following:
(a) References provided by a regulated bank from a FATF country;
(b) Certified copies of bank statements for a recent 3-month period; or
(c) References provided by a known customer of the bank licensee.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-1: Customer Due Diligence Requirements

AML-1.4 Enhanced Customer Due Diligence: Non Face-to-Face Business and New Technologies

AML-1.4.1 **Capital Market Service Providers must establish specific procedures for verifying customer identity where no face-to-face contact takes place.**

AML-1.4.2 **Where no face-to-face contact takes place, Capital Market Service Providers must take additional measures (to those specified in section AML-1.2), in order to mitigate the potentially higher risk associated with such business. In particular, Capital Market Service Providers 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.

AML-1.4.3 There are a number of checks that can provide a Capital Market Service Provider 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; ~~and~~
(c) Salary details appearing on recent bank statements
(d) Independent verification of employment (e.g.: through the use of a national E-KYC application, or public position held;
(e) Carrying out additional searches (e.g. internet searches using independent and open sources) to better inform the customer risk profile;
(f) Carrying out additional searches focused on financial crime risk indicator (i.e. negative news);
(g) Evaluating the information provided with regard to the destination of fund and the reasons for the transaction;
(h) Seeking and verifying additional information from the customer about the purpose and intended nature of the transaction or the business relationship; and
(i) Increasing the frequency and intensity of transaction monitoring.

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

AML-1.4.4 Capital market services provided using digital channels ~~via post, telephone~~ or internet pose greater challenges for customer identification and AML/CFT purposes. Capital Market Service Providers 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 AML-C.2. ~~Capital Market Service Providers must also ensure that they comply with any e-commerce laws and/or CBB Modules issued from time-to-time. Specifically,~~ Capital Market Service Providers which provide screen based trading or online services to their customers must set-up programmes or systems to highlight unusual transactions to enable the Capital Market Service Providers to report all such transactions.

New Products, Practices and Technologies

AML-1.4.5 Capital Market Service Providers 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.

AML-1.4.6 For purposes of Paragraph AML-1.4.5, such a risk assessment must take place prior to the launch of the new products, business practices or the use of new or developing technologies. Capital Market Service Providers must take appropriate measures to manage and mitigate those risks.

AML-1.4.7 Capital Market Service Providers, while complying with the requirements of Paragraphs AML-1.4.5 and AML-1.4.6, must pay special attention to new products, new business practices, new delivery mechanisms and new or developing technologies that favor anonymity.

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

Enhanced Monitoring

AML-1.4.8 **Customers on boarded digitally must be subject to enhanced on-going account monitoring measures.**

AML-1.4.9 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

AML-1.4.10 **Capital Market Service Providers 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.**

AML-1.4.11 **Capital Market Service Providers 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.

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

AML-1.4.12 Capital Market Service Providers that intends 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;

(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.

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

AML-1.4.13 Capital Market Service Providers 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.

AML-1.4.14 Capital Market Service Providers must ensure that the information referred to in Paragraph AML-1.2.1 is collected in adherence to privacy laws and other applicable laws of the country of residence of the customer.

AML-1.4.15 Capital Market Service Providers must ensure that the information referred to in Subparagraphs AML-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 AML-1.4.17 below) or by use of the methods mentioned in Paragraph AML-1.2.3 and /or AML-1.4.3 as appropriate.

AML-1.4 Enhanced Customer Due Diligence: Non Face-to-Face Business and New Technologies

AML-1.4.16 Capital Market Service Providers must also obtain the customer's explicit consent to record the session and capture images as may be needed.

AML-1.4.17 Capital Market Service Providers must verify the information in Paragraph AML-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 licensee.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-1: Customer Due Diligence Requirements

AML-1.4 Enhanced Customer Due Diligence: Non Face-to-Face Business and New Technologies

AML-1.4.18 For the purposes of Paragraph AML-1.4.17, 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.

AML-1.4.19 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.

AML-1.4.20 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

AML-1.4.21 Where Capital Market Service Providers 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 AML-B.2.1.

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

AML-1.5.1 Capital Market Service Providers 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. Capital Market Service Providers must utilise publicly available databases and information to establish whether a customer is a PEP.

AML-1.5.2 Capital Market Service Providers 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. Capital Market Service Providers must not accept a non-Bahraini PEP as a customer based on customer due diligence undertaken using digital ID applications.

AML-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).

AML-1.5.3A In cases of higher risk business relationships with such persons, mentioned in Paragraph AML-1.5.1, Capital Market Service Providers must apply, at a minimum, the measures referred to in (b), (d) and (e) of Paragraph AML-1.5.3.

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

AML-1.5.3C For the purpose of Paragraph AML-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.

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

AML-1.5.4 [This Paragraph was deleted in January 2020].

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

AML-1.6.1 **Capital market 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. For clubs and societies registered with the General Organisation for Youth and Sports (GOYS), Capital Market Service Providers must contact GOYS to clarify whether the account may be opened in accordance with the rules of GOYS.**

AML-1.6.2 Capital Market Service Providers are reminded that clubs and societies registered with GOYS may only have one account with banks in Bahrain.

AML-1.6.3 **Charities should be subject to enhanced transaction monitoring by Capital Market Service Providers. Capital Market Service Providers should develop a profile of anticipated account activity (in terms of payee countries and recipient organizations in particular).**

AML-1.6.4 **Capital Market Service Providers must provide a monthly report of all payments and transfers of BD3,000 (or equivalent in foreign currencies) and above, from accounts held by charities registered in Bahrain. The report must be submitted to the CBB's Compliance Unit (see section AML-4.4 for contact address), giving details of the amount transferred, account name, number and beneficiary name account and bank details. Capital Market Service Providers must ensure that such transfers are in accordance with the spending plans of the charity (in terms of amount, recipient and country).**

AML-1.6.5 **Article 20 of Decree Law No. 21 of 1989 (issuing the Law of Social and Cultural Societies and Clubs and Private Organisations Operating in the Area of Youth and Sport and Private Institutions) provides that Capital Market Service Providers may not accept or process any incoming or outgoing wire transfers from or to any foreign country on behalf of charity and non-profit organisations licensed by the Ministry of Social Development, until an official letter by the Ministry authorising the receipt or remittance of the funds has been obtained by the concerned Capital Market Service Provider.**

AML-1.6.6. **The receipt of a Ministry letter mentioned in rule AML-1.6.5 above does not exempt the concerned Capital Market Service Provider from conducting normal CDD measures as outlined in other parts of this Module.**

AML-1.7 Enhanced Due Diligence: 'Pooled Funds'

AML-1.7.1 Where Capital Market Service Providers receive pooled funds managed by professional intermediaries (such as investment and pension fund managers, stockbrokers and lawyers or authorized money transferors), they must apply CDD measures contained in section AML-1.8 to the professional intermediary. In addition, Capital Market Service Providers must verify the identity of the beneficial owners of the funds where required as shown in rules AML-1.7.2 and AML-1.7.3 below.

AML-1.7.2 Where funds pooled in an account are not co-mingled (i.e. where there are 'sub-accounts' attributable to each beneficiary), all beneficial owners must be identified by the Capital Market Service Provider and their identity verified in accordance with the requirements in section AML-1.2.

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

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

AML-1.7.4 For accounts held by intermediaries from foreign jurisdictions, the intermediary must be subject to requirements to combat Money Laundering and terrorist financing consistent with the FATF Recommendations and the intermediary must be supervised for compliance with those requirements. The Capital Market Service Provider must obtain documentary evidence to support the case for not carrying out customer due diligence measures beyond identifying the intermediary. The Capital Market Service Provider must satisfy itself that the intermediary has identified the underlying beneficiaries and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.

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

AML-1.8 Introduced Business from Professional Intermediaries

AML-1.8.1 A Capital Market Service Provider must only accept customers introduced to it by other Capital Market Service Providers, financial institutions or intermediaries, if it has satisfied itself that the introducer concerned is subject to FATF-equivalent measures and customer due diligence measures. Where Capital Market Service Providers delegate part of the customer due diligence measures to an introducer, the responsibility for meeting the requirements of Chapters 1 and 2 remains with the Capital Market Service Provider, not the introducer.

AML-1.8.2 Capital Market Service Providers 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 Capital Market Service Provider 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 identity of the customer and beneficial owner of the funds and, where applicable, the party/parties on whose behalf the customer is acting; also, the introducer has confirmed that the Capital Market Service Provider will be allowed to verify the customer due diligence measures undertaken by the introducer at any stage; and

(j) 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 Capital Market Service Provider and that these documents will be kept for at least five years after the business relationship has ended.

AML-1.8.3 The Capital Market Service Provider 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 Capital Market Service Provider must also perform periodic reviews to verify whether the jurisdiction is in compliance with the FATF Recommendations.

AML-1.8 Introduced Business from Professional Intermediaries (continued)

AML-1.8.4 Should the Capital Market Service Provider not be satisfied that the introducer is in compliance with the requirements of the FATF Recommendations, the Capital Market Service Provider must not accept further introductions, or discontinue the business relationship with the introducer.

AML-1.9 Shell Financial Institutions

Accounts with Shell Financial Institutions

AML-1.9.1 Capital Market Service Providers must not establish business relations with shell financial institutions which have no physical presence or 'mind and management' in the jurisdiction in which they are licensed and which are unaffiliated with a regulated financial group. Capital Market Service Providers must not knowingly establish relations with other Capital Market Service Providers or financial institutions that have relations with shell financial institutions.

AML-1.9.2 Capital Market Service Providers must make a Suspicious Transaction Report to the Financial Intelligence Directorate, Ministry of Interior and the Compliance Directorate of the CBB if they are approached by a shell financial institutions or an institution they suspect of being a shell financial institutions.

AML-1.10 Simplified Customer Due Diligence

AML-1.10.1 Capital Market Service Providers may apply simplified customer due diligence measures, as described in paragraphs AML-1.10.2 to AML-1.10.8, if:

(a) [This Subparagraph was deleted in January 2018];

(b) The transaction concerns the sale of a Security listed on a licensed exchange, issued as a result of an initial public offering after January 2006, and the customer already holds an investor number and an allotment letter. Furthermore, the licensed exchange should have advised the broker (by circular) that all necessary customer due diligence information and copies of all original identification documents will be made available upon request without delay;

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

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

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

(f) The customer is the Central Bank of Bahrain ('CBB'), a licensed exchange, or a licensee of the CBB; or

(g) The customer is a Ministry of a GCC or FATF member state government, a company in which a GCC government is a majority shareholder, or a company established by decree in the GCC.

AML-1.10.2 For customers falling under category (b) in rule AML-1.10.1, the customer's name and contact information must be recorded. However, the verification, certification and due diligence requirements (contained in rules AML-1.2.3, AML-1.2.5, AML-1.2.6, AML-1.2.8, AML-1.2.9 and AML-1.2.11), may be dispensed with.

AML-1.10 Simplified Customer Due Diligence (continued)

AML-1.10.3 [This Paragraph was deleted in July 2018].

AML-1.10.4 **For customers falling under categories (c) to (g) in rule AML-1.10.1, the information required under rule AML-1.2.7 (for legal entities) must be obtained. However, the verification, certification and due diligence requirements (contained in rules AML-1.2.3, AML-1.2.5, AML-1.2.6, AML-1.2.8, AML-1.2.9 and AML-1.2.11), may be dispensed with.**

AML-1.10.5 **Capital Market Service Providers wishing to apply simplified due diligence measures as allowed for under categories (c) to (g) of rule AML-1.10.1 must retain documentary evidence supporting their categorization of the customer.**

AML-1.10.6 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.

AML-1.10.7 **Capital Market Service Providers may use authenticated SWIFT messages as a basis for confirmation of the identity of a financial institution under rule AML-1.10.1 (d) and (e) where it is dealing as principal. For customers coming under rule AML-1.10.1 (d) and (e), Capital Market Service Providers 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.**

AML-1.10.8 **Simplified customer due diligence measures must not be applied where a Capital Market Service Provider 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.**

AML-1.10.8A **Simplified customer due diligence measures must not be applied in situations where the licensee has identified high ML/TF/PF risks.**

AML-1.10.9 **[This Paragraph was deleted in July 2018].**

AML-1.11 Enhanced Due Diligence for Correspondent Accounts

AML-1.11.1 This Section, AML1.11, applies to a Capital Market Service Provider when it provides correspondent account services or characteristic similar to correspondent account services.

AML-1.11.2 When providing correspondent account services, Capital Market Service Providers, must gather sufficient information (e.g. through a questionnaire) about their respondent financial institution to understand the nature of the respondent's business. Factors to consider to provide assurance that satisfactory measures are in place at the respondent financial institution includes:

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

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

(c) Where the customers of the respondent financial institution are located;

(d) The respondent financial institution AML/CFT controls;

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

(f) Confirmation that the respondent financial institution has verified the identity of any third party entities that will have direct access to the account without reference to the respondent financial institution (payable through account);

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

AML-1.11 Enhanced Due Diligence for Correspondent Accounts (continued)

(h) Confirmation that the respondent financial institution is able to provide relevant customer identification data on request to the Capital Market Service Providers; and

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

AML-1.11.3 Capital Market Service Providers must implement the following additional measures, prior to opening a correspondent account:

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

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

AML-1.11.4 Where the correspondent account services involve a payable through account, Capital Market Service Providers must be satisfied that:

(a) The respondent financial institution has performed appropriate measures at least equivalent to those specified in Sections AML-1.1 to AML-1.8 (Customer Due Diligence) on the third party having direct access to the payable-through account; and

(b) The respondent financial institution is able to perform ongoing monitoring of its business relations with that third party and is willing and able to provide CDD information to the Capital Market Service Provider upon request.

AML-1.11.5 Capital Market Service Providers must document the basis for their satisfaction that the requirements in Paragraphs AML-1.11.2, AML-1.11.3 and AML-1.11.4 are met.

AML-1.11.6 Capital Market Service Providers must not enter into or continue correspondent account services relationship with another financial institution that does not have adequate controls against money laundering or terrorism financing activities, is not effectively supervised by the relevant authorities or is a shell financial institution. Capital Market Service Providers must pay particular attention when entering into or continuing relationships with respondents located in jurisdictions that have poor KYC standards or have been identified by the FATF as being 'non-cooperative' in the fight against money laundering/terrorist financing.

AML-1.11 Enhanced Due Diligence for Correspondent Accounts (continued)

AML-1.11.7 **Capital Market Service Providers must also take appropriate measures when establishing a correspondent account services relationship, to satisfy themselves that their respondent financial institutions do not permit their accounts to be used by shell financial institutions.**

AML-1.11.8 In the case of correspondent account services relationships, the Capital Market Service Provider generally does not have direct relationships with the customers of the respondent financial institution. Therefore, there is no expectation or requirement for the Capital Market Service Provider to apply CDD on a respondent financial institution's customer, which is, instead the responsibility of the respondent financial institution. Nonetheless, it is consistent with the risk-based approach for the Capital Market Service Provider to have some general sense of the respondent financial institution's customer base as part of ascertaining the risks associated with the respondent financial institution itself.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-2: AML/CFT Systems and Controls

AML-2.1 General Requirements

AML-2.1.1 **Capital Market Service Providers 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 Capital Market Service Provider. The documentation, and the Board's review and approval, must be made available upon request to the CBB.**

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

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

Risk Based Monitoring

AML-2.2.1 **Capital Market Service Providers 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 including transactions in accepted crypto-assets.**

AML-2.2.2 Capital Market Service Providers' risk-based monitoring systems should therefore be configured to help identify:

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

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

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

Automated Transaction Monitoring

AML-2.2.3 **Capital Market Service Providers must consider the need to include automated transaction monitoring as part of their risk-based monitoring systems to spot abnormal or unusual flow of funds. In the absence of automated transaction monitoring systems, all transactions above BD6,000 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 Capital Market Service Providers for five years after the date of the transaction.**

AML-2.2.4 The CBB would expect larger Capital Market Service Providers to include automated transaction monitoring as part of their risk-based monitoring systems. See also Chapters AML-3 and AML-6, regarding the responsibilities of the MLRO and record-keeping requirements. Where the Capital Market Service Provider is not receiving funds – for instance where it is simply acting as agent on behalf of a principal, and the customer is directly remitting funds to the principal – then the Capital Market Service Provider may agree with the principal that the latter should be responsible for the daily monitoring of such transactions.

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

Unusual Transactions or Customer Behaviour

AML-2.2.5 **Where a Capital Market Service Provider's risk-based monitoring systems identify significant or abnormal transactions (as defined in paragraph AML-2.2.2 and rule AML-2.2.3), it must verify the source of funds for those transactions, particularly where the transactions are above the ~~occasional~~ transactions threshold of BD6,000. Furthermore, Capital Market Service Providers must examine the background and purpose to those transactions and document their findings. In the case of one-off transactions where there is no ongoing account relationship, the Capital Market Service Provider must file a Suspicious Transaction Report (STR) if it is unable to verify the source of funds to its satisfaction (see Chapter AML-4).**

AML-2.2.6 **The investigations required under rule AML-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 rule AML-6.1.1 (b)).**

AML-2.2.7 **Capital Market Service Providers must consider instances where there is a significant, unexpected or unexplained change in customer activity.**

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

AML-2.2.9 Once identification procedures have been satisfactorily completed and, as long as records concerning the customer are maintained in line with Chapters AML-1 and AML-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.

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

On-going Monitoring

AML-2.2.10 Capital Market Service Providers 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 capital market service provider'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 AML-1, by undertaking reviews of existing records, particularly for higher risk categories of customers. Capital Market Service Providers must require all customers to provide up-to-date identification documents in their standard terms and conditions of business.

AML-2.2.11 Capital Market Service Providers 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 Capital Market Service Provider must take steps to obtain updated copies as soon as possible.

AML-2.2.12 Capital Market Service Providers must in addition to rules AML-2.2.10 and AML-2.2.11, maintain information and documents in respect to client transactions such as date of execution, value of transaction, type of Securities and identity of the counterparty.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-2A: Money Transfers and Accepted Crypto-asset Transfers

AML-2A.1 Applicability and CBB's Approach to Transfer of Accepted Crypto-assets

AML-2A.1.1 **The requirements of this Section, AML-2A.1, applies to Capital Market Service Providers (including Crypto-asset licensees as well as third party service providers) if they act as an ordering financial institution, intermediary financial institution or beneficiary financial institution.**

AML-2A.1.2 **A third party service provider that provides accepted crypto-asset transfers and/or electronic transfer of funds (wire transfer) on behalf of a Capital Market Service Provider, irrespective of whether the third party service provider is licensed by the CBB or not, must comply with the requirements of Paragraph AML-2A.1. A Capital Market Service Provider is ultimately responsible for the functioning and activities of the third party service provider and must ensure that the third party service provider meets all regulatory obligations as specified in this Section.**

CBB's Approach to Transfer of Accepted Crypto-assets

AML-2A.1.3 As with financial payment methods, accepted crypto-assets can be used to quickly move (transfer) funds globally and to facilitate a range of financial activities. Similar to mobile or internet based payment services and mechanism, accepted crypto-assets can be used to transfer funds in a wide geographical area with a large number of counterparties.

AML-2A.1.4 **The CBB considers transactions involving transfer of accepted crypto-assets as functionally analogous to wire transfer. Therefore, Capital Market Service Providers (including crypto-asset licensees), whenever their transaction, whether in fiat currency or accepted crypto-assets, involves (i) a traditional wire transfer, or (ii) an accepted crypto-asset transfer, must comply with the requirements of Paragraph AML-2A.2 unless stated otherwise.**

AML-2A.2 Transfer of Accepted Crypto-assets and Wire Transfer

Accepted Crypto-asset Transfer to be Considered as Cross Border Transfer

AML-2A.2.1 Capital Market Service Providers (including crypto-asset licensees) must consider all transfers of accepted crypto-assets as cross-border transfer rather than domestic transfer.

Outward Transfers

AML-2A.2.2 Capital Market Service Providers must include all required originator information and required beneficiary information details with the accompanying transfer of accepted crypto-assets and/or wire transfer of funds they make on behalf of their customers.

AML-2A.2.3 For purposes of this Section, originator information refers to the information listed in Subparagraphs AML-2A.2.7 (a) to (c) and beneficiary information refers to the information listed in Subparagraphs AML-2A.2.7 (d) and (e).

Inward Transfers

AML-2A.2.4 Capital Market Service Providers must:

(a) Maintain records (in accordance with Chapter AML-6 of this Module) of all originators information received with an inward transfer; and

(b) Carefully scrutinize inward transfers which do not contain originator information (i.e. full name, address and account number or a unique customer identification number). Capital Market Service Providers must presume that such transfers are 'suspicious transactions' and pass them to the MLRO for review for determination as to possible filing of STR, unless (i) the ordering financial institution is able to promptly (i.e. within two business days) advise the licensee in writing of the originator information upon the licensee's request (Refer to Paragraph AML-2A.2.5); or (ii) the ordering financial institution and the licensee are acting on their own behalf (as principal).

AML-2A.2 Transfer of Accepted Crypto-assets and Wire Transfer (continued)

AML-2A.2.5 **The period of 2 business days provided to ordering financial institution by the Capital Market Service Provider under Paragraph AML-2A.2.4(b)(i) to furnish the originator information is only applicable while undertaking fund transfer (traditional wire transfer) and must not be used in case of transfer of accepted crypto-assets.**

AML-2A.2.6 **While undertaking accepted crypto-asset transfer, a Capital Market Service Provider must ensure that the ordering financial institution transmits the originator and beneficiary information immediately (Refer to Paragraph AML-2A.2.9).**

Accepted Crypto-asset Transfer and Cross Border Wire Transfer

AML-2A.2.7 **Information accompanying all accepted crypto-asset transfer as well as wire transfer must always contain:**

(a) The name of the originator;

(b) The originator account number (e.g. IBAN or crypto-asset wallet) where such an account is used to process the transaction;

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

(d) The name of the beneficiary; and

(e) The beneficiary account number (e.g. IBAN or crypto-asset wallet) where such an account is used to process the transaction.

AML-2A.2.8 Where a Capital Market Service Provider undertakes a transfer of accepted crypto-asset, it is not necessary for the information referred to in Paragraph AML-2A.2.7 to be attached directly to the accepted crypto-asset transfers itself. The information can be submitted either directly or indirectly.

AML-2A.2.9 **A Capital Market Service Provider while undertaking transfer of accepted crypto-asset must ensure that the required originator and beneficiary information is transmitted immediately and securely.**

AML-2A.2.10 For the purposes of Paragraph AML-2A.2.9, "Securely" means that the provider of the information must protect it from unauthorized disclosure as well as ensure that the integrity and availability of the required information is maintained so as to facilitate recordkeeping and the use of such information by financial institution. The term "immediately" means that the provider of the information must submit the required information simultaneously or concurrently with the transfer itself of the accepted crypto-asset.

AML-2A.2 Transfer of Accepted Crypto-assets and Wire Transfer (continued)

AML-2A.2.11 **The CBB recognises that unlike traditional fiat currency wire transfer, not every accepted crypto-asset transfer involves (or is bookended by) two institutions (crypto-asset entities or financial institution). In instances in which an accepted crypto-asset transfer involves only one financial institution on either end of the transfer (e.g. when an ordering financial institution sends accepted crypto-assets on behalf of its customers, the originator, to a beneficiary that is not a customer of a beneficiary financial institution but rather an individual user who receives the accepted crypto-asset transfer using his/her own distributed ledger technology (DLT) software, such as an unhosted wallet), the financial institution must still ensure adherence to Paragraph AML-2A.2.7 for their customer. The CBB does not expect that financial institutions, when originating an accepted crypto-asset transfer, would submit the required information to individual users who are not financial institutions. However, financial institutions receiving an accepted crypto-asset transfer from an entity that is not a financial institution (e.g. from an individual accepted crypto-asset user using his/her own DLT software, such as an unhosted wallet), must obtain the required originator information from their customer.**

Domestic Wire Transfer

AML-2A.2.12 **Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and the CBB by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.**

AML-2A.2.13 For purposes of Paragraph AML-2A.2.12, the information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from the CBB.

AML-2A.2 Transfer of Accepted Crypto-assets and Wire Transfer (continued)

AML-2A.2.14 It is not necessary for the recipient institution to pass the originator information on to the beneficiary. The obligation is discharged simply by notifying the beneficiary financial institution of the originator information at the time the transfer is made.

Responsibilities of Ordering, Intermediary and Beneficiary Financial Institutions

Ordering Financial Institution

AML-2A.2.15 **The ordering financial institution must ensure that wire transfers as well as accepted crypto-asset transfers contain required and accurate originator information, and required beneficiary information.**

AML-2A.2.16 **The ordering financial institution must maintain all originator and beneficiary information collected in accordance with Paragraph AML-6.1.1.**

AML-2A.2.17 **The ordering financial institution must not execute the wire transfer or accepted crypto-asset transfer if it does not comply with the requirements of Paragraphs AML-2A.2.15 and AML-2A.2.16.**

Intermediary Financial Institutions

AML-2A.2.18 **For cross-border wire transfers and accepted crypto-asset transfers, financial institutions processing an intermediary element of such chains of wire transfers and/or accepted crypto-asset transfers must ensure that all originator and beneficiary information that accompanies a wire transfer and accepted crypto-asset transfer is retained with it.**

AML-2A.2.19 **Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept, for at least five years, by the receiving intermediary institution of all the information received from the ordering financial institution or another intermediary financial institution.**

AML-2A.2 Transfer of Accepted Crypto-assets and Wire Transfer (continued)

AML-2A.2.20 An intermediary financial institution must take reasonable measures to identify cross-border wire transfers and accepted crypto-asset transfer that lack required originator information or required beneficiary information.

AML-2A.2.21 An intermediary financial institution must have effective risk-based policies and procedures for determining:

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

(b) The appropriate follow-up action.

Beneficiary Financial Institution

AML-2A.2.22 A beneficiary financial institution must take reasonable measures to identify cross-border wire transfers as well as accepted crypto-asset transfer that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

AML-2A.2.23 For wire transfers as well as accepted crypto-asset transfer, a beneficiary financial institution must verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Paragraph AML-6.1.1.

AML2A.2.24 A beneficiary financial institution must have effective risk-based policies and procedures for determining:

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

(b) The appropriate follow-up action.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-3: Money Laundering Reporting Officer (MLRO)

AML-3.1 Appointment of MLRO

AML-3.1.1 **Capital Market Service Providers must appoint a Money Laundering Reporting Officer ("MLRO"). The position of the MLRO is a controlled function and the MLRO is an approved Person.**

AML-3.1.2 For details of CBB's requirements regarding controlled functions and approved Persons, see the relevant licensing Module, such as MAE, CSD, or MIR Module. 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.

AML-3.1.3 **The position of the 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 the MLRO may not be outsourced.**

AML-3.1.4 Subject to rule AML-3.1.3, however, the position of the MLRO may otherwise be combined with other functions in the Capital Market Service Provider, 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. Rule AML-3.1.7 requires that the MLRO is a Director or employee of the Capital Market Service Provider, so the function may not be outsourced to a third party employee.

AML-3.1.4A For purposes of Paragraphs AML-3.1.3 and AML-3.1.4 above, Capital Market Service Providers 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 Capital Market Service Providers.

AML-3.1.5 **Unless exempted by the CBB, a Capital Market Service Providers must appoint deputy MLRO to act for the MLRO in his/her absence. The deputy MLRO must be resident in Bahrain unless otherwise agreed with the CBB.**

AML-3.1.5A Where a Capital Market Service Provider seeks an exemption from appointment of Deputy MLRO, from the CBB, it must provide in writing, to the satisfaction of the CBB, the nature, scale and complexity of their business and the alternative arrangements that the Capital Market Service Provider shall implement when the MLRO is not available to carry out the controlled function.

AML-3.1.6 Capital Market Service Providers should note that although the MLRO may delegate some of his functions, either to other employees of the Capital Market Service Provider or even (in the case of larger groups) to individuals performing similar functions for other group entities, the responsibility for compliance with the requirements of this Module remains with the Capital Market Service Provider and the designated MLRO. The deputy MLRO should be able to support the MLRO discharge his responsibilities and to deputise for him in his absence.

AML-3.1 Appointment of MLRO (continued)

AML-3.1.7 So that he can carry out his functions effectively, Capital Market Service Providers must ensure that their MLRO:

(a) Is a Director or a member of senior management of the Capital Market Service Provider;
(b) Has a sufficient level of seniority within the Capital Market Service Provider, 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 Capital Market Service Provider to that customer, or any transactions conducted by the Capital Market Service Provider on behalf of a customer;
(e) Is provided with timely information needed to identify, analyze and effectively monitor customer accounts;
(f) Has access to all customer due diligence information obtained by the Capital Market Service Provider; and
(g) Is resident in Bahrain.

AML-3.1.8 In addition, Capital Market Service Providers must ensure that their MLRO is able to:

(a) Monitor the day-to-day operation of its policies and procedures relevant to this Module; and
(b) Respond promptly to any reasonable request for information made by the Financial Intelligence Directorate, or the CBB.

AML-3.1.9 If the position of the MLRO falls vacant, the Capital Market Service Provider 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 Capital Market Service Provider 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. Any action taken by the Deputy MLRO will be regarded as having the same authority as if it had been done by the MLRO.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-3: Money Laundering Reporting Officer (MLRO)

AML-3.2 Responsibilities of the MLRO

AML-3.2.1 The MLRO is responsible for:

(a) Establishing and maintaining the Capital Market Service Provider's AML/CFT policies and procedures;

(b) Ensuring that the Capital Market Service Provider complies with the AML Law, any other applicable AML/CFT legislation and this Module;

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

(d) Acting as the Capital Market Service Provider's main point of contact in respect of handling internal Suspicious Transaction Reports from the Capital Market Service Provider's staff (refer to section AML-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 Transaction Reports to the Financial Intelligence Directorate and the Compliance Directorate (refer to section AML-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 AML-5;

(g) Producing annual reports on the effectiveness of the Capital Market Service Provider's AML/CFT controls, for consideration by senior management, as per rule AML-3.3.3 and following-up on the status of any anomaly identified or remedial measure required by the CBB;

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

(i) Ensuring that the Capital Market Service Provider maintains all necessary CDD, transactions, STR and staff training records for the required periods (refer to section AML-6.1).

AML-3.3 Compliance Monitoring

Annual Compliance Review

AML-3.3.1 **Capital Market Service Providers 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.**

AML-3.3.1A Capital Market Service Provider 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.

AML-3.3.1B **A Capital Market Service Provider must review the effectiveness of its AML/CFT procedures, systems and controls at least once each calendar year. The review must cover the Capital Market Service Provider and its branches and subsidiaries both inside and outside the Kingdom of Bahrain. A Capital Market Service Provider 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 AML-4.1, a breakdown of all the results of those internal reports and their outcomes for each segment of the Capital Market Service Provider'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 AML-4.2 and, where a Capital Market Service Provider 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 Capital Market Service Provider's anti-money laundering procedures, systems and controls and compliance with the rules of a licensed exchange and licensed clearing house ~~and~~ or central depository, AML Law and this Module.

AML-3.3 Compliance Monitoring (continued)

AML-3.3.2 **The reports listed under rule AML-3.3.1B (a) and (b) must be made by the MLRO. The sample testing required under rule AML-3.3.1B (c) must be undertaken either by the Capital Market Service Provider's internal audit function its external auditors or a consultancy firm approved by the CBB. The report required under rule AML-3.3.1B (d) must be made by the Capital Market Service Provider's external auditors or a consultancy firm approved by the CBB.**

AML-3.3.2A In order for a consultancy firm to be approved by the CBB for the purposes of Paragraph AML-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.

AML-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.

AML-3.3.2C **Capital Market Service Providers must ensure that the personnel conducting the review are qualified, skilled and have adequate experience to conduct such a review. At least two persons working on the report (one of whom should be the team leader) must have:**
(a) A minimum of 5 years professional experience dealing with AML/CFT issues; and
(b) Formal AML/CFT training.

AML-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.

AML-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.

AML-3.3 Compliance Monitoring (continued)

AML-3.3.3 **The reports listed under rule AML-3.3.1B must be submitted to the Capital Market Service Provider's Board for it to review and commission any required remedial measures and copied to the Capital Market Service Provider's senior management.**

AML-3.3.4 The purpose of the annual compliance review is to assist a Capital Market Service Provider's Board and senior management to assess, amongst other things, whether internal and external reports are being made (as required under Chapter AML-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 Capital Market Service Provider's business (or, where relevant, in particular branches or subsidiaries). Capital Market Service Providers should use their judgement as to how the reports listed under rule AML-3.3.1B (a) and (b) should be broken down in order to achieve this aim (e.g. by branches, departments, product lines, etc).

AML-3.3.5 **Capital Market Service Providers must instruct their external auditor to produce the report referred to in rule AML-3.3.1B (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 Capital Market Service Provider.**

AML-3.3.6 The external auditors may rely upon work performed by the Capital Market Service Provider's internal audit function as part of their procedures for producing the report referred to in rule AML-3.3.5.

AML-4.1 Internal Reporting

AML-4.1.1 Capital Market Service Providers must implement procedures to ensure that staff who handle customer business (or are managerially responsible for such staff) make a report promptly to the MLRO if they know or suspect that a customer (or a Person on whose behalf a customer may be acting) is engaged in Money Laundering or terrorism financing, or if the transaction or the customer's conduct otherwise appears unusual or suspicious. These procedures must include arrangements for disciplining any member of staff who fails, without reasonable excuse, to make such a report.

AML-4.1.2 Where Capital Market Service Providers' 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.

AML-4.2 External Reporting

AML-4.2.1 Capital Market Service Providers must take reasonable steps to ensure that all reports made under section AML-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.

AML-4.2.2 To take reasonable steps, as required under rule AML-4.2.1, Capital Market Service Providers must:

(a) Require the MLRO to consider reports made under Section AML-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 Capital Market Service Provider'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.

AML-4.2.3 Reports to the Relevant Authorities made under rule AML-4.2.1 must be sent to the Financial Intelligence Directorate at the Ministry of the 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.

AML-4.2.4 Capital Market Service Providers must report all suspicious transactions or attempted transactions. This reporting requirement applies regardless of whether the transaction involves tax matters.

AML-4.2 External Reporting (continued)

AML-4.2.5 Capital Market Service Providers must retain all relevant details of STRs submitted to the Relevant Authorities, for at least five years.

AML-4.2.6 In accordance with the AML Law, Capital Market Service Providers, their Directors, officers and employees:

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

(b) In cases where Capital Market Service Providers 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 Capital Market Service Provider 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.

AML-4.3 Reporting to the SRO

AML-4.3.1 The MLRO, whenever he becomes aware or believes, or has reason to believe that a client is involved in a Money Laundering offence, shall in addition to the reporting in section AML-4.2, inform the SRO on which the transaction is taking place, or where the Securities or cash is being held, in which case the SRO must, unless instructed otherwise by a Relevant Authority, stop the execution of the suspicious transaction and any Security deposited with the SRO or other Capital Market Service Provider.

AML-4.4 Contacting the Relevant Authorities

AML-4.4.1 Reports made by the MLRO or his duly authorised delegate under Section AML-4.2 must be sent electronically using the Suspicious Transaction Reporting Online System (Online STR system).

AML-4.4.2 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

AML-5.1 General Requirements

AML-5.1.1 Capital Market Service Providers 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 Capital Market Service Provider'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 report in accordance with section AML-4.1;
(g) The Capital Market Service Provider's procedures for making an internal report as per section AML-4.1; and
(h) Customer due diligence measures with respect to establishing business relations with customers.

AML-5.1.2 The information referred to in rule AML-5.1.1 must be brought to the attention of relevant new employees of Capital Market Service Providers, and must remain available for reference by staff during their period of employment.

AML-5.1.3 Relevant new employees must be given AML/CFT training within three months of joining a Capital Market Service Provider.

AML-5.1.4 Capital Market Service Providers must ensure that their AML/CFT training for relevant staff remains up-to-date, and is appropriate given the Capital Market Service Provider's activities and customer base.

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

AML-5.1.6 Capital Market Service Providers 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 Capital Market Service Providers.

AML-5.1.6A For the purposes of Paragraph FC-5.1.6, Capital Market Service Providers must obtain a good conduct certificate from the Ministry of Interior prior to hiring any Bahraini employee.

AML-6.1 General Requirements

CDD and Transaction Records

AML-6.1.1 Capital Market Service Providers must comply with the record-keeping requirements contained in the AML Law and in the CBB Law. Capital Market Service Providers must therefore retain adequate records (including accounting and identification records), for the following minimum periods:

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

(b) For transactions, in relation to documents enabling a reconstitution of the transaction concerned, for at least five years after the transaction was completed.

AML-6.1.1 A For the purposes of Subparagraph AML-6.1.1(b), crypto-asset licensees must maintain all records of transactions in such form or manner that individual transactions can be reconstructed swiftly and the records can associate the transactions to a natural person.

AML-6.1.1B Crypto-asset licensees must maintain information obtained through enhanced customer due diligence (refer CRA-7.1.3 of Module CRA), including information relating to the identification of the relevant customers, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of transaction and the amount transferred.

AML-6.1.1C Crypto-asset licensees relying solely on the public information available on the blockchain or other type of distributed ledger underlying the accepted crypto-asset for record keeping in not sufficient for compliance with AML-6.1.1 and AML-6.1.1A. The information available on the blockchain or other type of distributed ledger may enable to trace transactions back to a wallet, though may not readily link the wallet address to the name of the customer and the beneficial owner. Crypto-asset licensees must ensure that additional information necessary to associate the wallet address to a natural person is maintained.

AML-6.1 General Requirements (continued)

Compliance Records

AML-6.1.2 Capital Market Service Providers must retain copies of the reports produced for their annual compliance review, as specified in rule AML-3.3.1, for at least five years. Capital Market Service Providers must also maintain for five years reports made to, or by, the MLRO made in accordance with sections AML-4.1 and AML-4.2, and records showing how these reports were dealt with and what action, if any, was taken as a consequence of those reports.

AML-6.1.3 When required to deliver the original copy of a record concerning any transaction, or a document pertaining thereto before the expiry of the prescribed period, the Capital Market Service Providers shall observe the following:

(a) They shall maintain a complete copy of the delivered record or documents until the end of the period prescribed for maintaining the original records or documents.

(b) They shall maintain a record of the delivered documents.

Training Records

AML-6.1.4 Capital Market Service Providers 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

AML-6.1.5 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.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-7: General Requirements in Relation to Securities

AML-7.1 General Requirements in Respect of Substantial Shareholding

AML-7.1.1 Any Person whose ownership alone or his ownership together with that of his minor children, or any other accounts under his disposal, or the ownership of any of his associate or affiliate companies amounts to 5% or more of any listed Security of a joint stock company, must notify the licensed exchange forthwith, which must in turn notify the CBB of this fact and the CBB may declare the name of the Person who owns such stake.

AML-7.1.2 [This Paragraph was deleted in October 2019].

AML-7.1.3 All persons must obtain CBB prior written approval to execute any order that will bring their ownership alone or their ownership together with their minor children, or the accounts standing under their disposal to 10% or more in any listed security. Any further increase of 1% or more shall also be subject to CBB prior written approval.

AML-7.1.4 Without prejudice to any greater penalty prescribed under the Prevention and Prohibition of the Money Laundering Law or any other law, a breach of the provisions of section AML-7.1 shall result in the cancellation of the transaction, and the Person in breach must bear all costs arising in this connection.

AML-7.2 Requirements for Listing

AML-7.2.1 No local or foreign company shall be listed on a Licensed Exchange, unless their documents of incorporation are complete and satisfy all legal requirements applicable in the Kingdom, or in their countries of incorporation to the extent that these are comparable to this Module, as the case may be.

AML-7.3 Requirements for Offering

AML-7.3.1 No Security shall be offered for public subscription in the Kingdom unless the issuing company is duly incorporated under the laws of the Kingdom, or the laws of its country of incorporation, as the case may be, satisfying all terms and conditions governing the public offering of Securities in the Kingdom, and abiding by the conditions and requirements stipulated under the Commercial Companies Law and the Disclosure Standards in force in the Kingdom.

AML-7.3.2 No Security issued to the bearer shall be offered, listed, traded or deposited on a Licensed Exchange.

AML-7.4 Requirements for Deposit

AML-7.4.1 A Security shall not be accepted in the Central Depository System unless its authenticity is approved by the concerned shares registrar and the client shall provide the Central Depository System with any amendment or change which may occur in such particulars.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-8: Acceptance of Cash

AML-8.1 Acceptance of Cash

AML-8.1.1 [This Paragraph was deleted in January 2020].

AML-8.1.1A A Capital Market Service Provider, whether at the commencement of or during a business relationship, must not accept cash from a customer, whether for investment purpose or as payment for services provided by the Capital Market Service Provider except for payment of one time or non-recurring fees (symbolic fees) with a value not exceeding Two Hundred Bahraini Dinars for the services provided by the Capital Market Service Provider such as account opening fees, fees for providing statements, fees for printing documents and certificates of various types and such other services.

AML-8.1.2 If the value of a transaction is paid for by cheque by a third party other than the purchaser, the identity of such third party shall be verified.

AML-9.1 Special Measures for Non-Cooperative Countries or Territories ('NCCTs')

AML-9.1.1 **Capital Market Service Providers 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 Capital Market Service Providers from time-to-time by the CBB.

AML-9.1.2 **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 AML-4.2.**

AML-9.1.3 **Capital Market Service Providers 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.**

AML-9.1.4 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.

AML-9.2 Terrorist Financing

AML-9.2.1AA **Capital Market Service Providers must implement and comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. Capital Market Service Providers 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).**

AML-9.2.1 **Capital Market Service Providers must comply in full with the provisions of the UN Security Council Anti-Terrorism Resolution No. 1373 of 2001 ('UNSCR 1373').**

AML-9.2.2 **[This Paragraph was deleted in January 2018].**

AML-9.2.3 A copy of UNSCR 1373 is included in Part B of Volume 6 (Capital Markets), under 'Supplementary Information' on the CBB Website.

AML-9.2.4 **Capital Market Service Providers 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 Capital Market Service Provider has on Persons and entities which may be the subject of Article 1, Paragraphs (c) and (d) of UNSCR 1373.

AML-9.2.5 For the purposes of rule AML-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, Paragraphs (c) and (d) of UNSCR 1373, and any associated dividends received by the Capital Market Service Provider.

AML-9.2.6 **All reports or notifications under this section must be made to the CBB's Compliance Directorate.**

AML-9.2.7 See section AML-4.3 for the Compliance Directorate's contact details.

AML-9.3 Designated Persons and Entities

AML-9.3.1 **Without prejudice to the general duty of all Capital Market Service Providers to exercise the utmost care when dealing with Persons or entities who might come under Article 1, Paragraphs (c) and (d) of UNSCR 1373, Capital Market Service Providers must not deal with any Persons or entities designated by the CBB as potentially linked to terrorist activity.**

AML-9.3.2 The CBB from time-to-time issues to Capital Market Service Providers lists of designated Persons and entities believed linked to terrorism. Capital Market Service Providers 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').

AML-9.3.3 **Capital Market Service Providers must report to the Relevant Authorities, using the procedures contained in section AML-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.**

AML-10.1 Regulatory Penalties

AML-10.1.1 **Without prejudice to any other penalty imposed by the CBB Law, the AML Law No. 4 or the Penal Code of the Kingdom of Bahrain, failure by a Capital Market Service Provider 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 BD20,000.**

AML-10.1.2 Module MIE provides further information on the CBB's general approach to enforcement and the criteria taken into account prior to imposing such fines (see section MIE-3.1). Other enforcement measures may also be applied by the CBB in response to a failure by a Capital Market Service Provider to comply with this Module; these other measures are also set out in Module MIE.

AML-10.1.3 The CBB will endeavour to assist Capital Market Service Providers to interpret and apply the requirements of this Module. Capital Market Service Providers may seek clarification on any issue by contacting the Compliance Directorate (see section AML-4.3 for contact details).

AML-10.1.4 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 Capital Market Service Providers.

AML-11.1 Guidance Provided by International Bodies

FATF Recommendations

AML-11.1.1 The Recommendations (see www.fatf-gafi.org) together with their associated interpretative notes and best practices papers issued by the Financial Action Task Force (FATF), provide the basic framework for combating Money Laundering activities and the financing of terrorism.

AML-11.1.2 The Relevant Authorities in Bahrain believe that the principles established by these Recommendations should be followed by Capital Market Service Providers in all material respects, as representing best practice and prudence in this area.

Other Website References Relevant to AML/CFT

AML-11.1.3 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.

MODULE	AML: Anti-Money Laundering & Combating of Financial Crime
CHAPTER	AML-12: Fraud

AML-12.1 General Requirements for the Detection and Prevention of Fraud

AML-12.1.1 **Capital Market Service Providers 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.**

AML-12.1.2 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, for instance through false invoicing or advance fee frauds. Further guidance – and occasional investor alerts – can be found on the CBB's website (www.cbb.gov.bh).

AML-12.1.3 **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.**

AML-12.1.4 **Capital Market Service Providers must ensure that a Person of sufficient seniority is given overall responsibility for the prevention, detection and remedying of fraud within the organisation.**

AML-12.1.5 **Capital Market Service Providers 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.**

AML-12.1.6 **Capital Market Service Providers must provide regular training to their management and staff, to make them aware of potential fraud risks.**