مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

GUIDANCE FOR THE INSURANCE SECTOR

October 31, 2022

Contents

1. Introduction

1.1. Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations*, as amended, charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding, and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed insurers, agents, and brokers of their statutory obligations under the legal and regulatory framework in force in the UAE. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for licensed insurers, agents, and brokers to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, such as outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators identified by the FATF and leading jurisdictional authorities. These are not exhaustive and do not set limitations on the measures to be taken by licensed insurers, agents, and brokers in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, licensed insurers, agents, and brokers should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with licensed insurers, agents, and brokers expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all insurance and re-insurance companies, agents, and brokers that are licensed and supervised by the CBUAE.

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

1.3. Legal Basis

This Guidance builds upon the provisions of the following AML/CFT related laws and regulations:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combating the Financing of Terrorism ("CFT") and Financing Illegal Organisations as amended by Federal Decree Law No. (26) of 2021 ('AML-CFT Law");
- Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation for Federal Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations, as amended by Cabinet Decision No. (24) of 2022 ("AML-CFT Decision");
- Insurance Authority's Board of Directors' Decision No. (19) of 2020 Concerning the Guidance Manual for Insurance Companies and Related Professions to Submitting the Data, Information, & Supervisory Reports.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
DNFBP	Designated non-financial business or profession
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FFR	Fund Freeze Report
FIU	Financial intelligence unit
LFI	Licensed financial institution
ML	Money laundering
PEP	Politically exposed person
PNMR	Partial Name Match Report
SAR	Suspicious activity report
SDD	Simplified due diligence
STR	Suspicious transaction report
TF	Terrorist financing
UN	United Nations
UNSC	United Nations Security Council
UNSCR	UN Security Council Resolution

2. Understanding and Assessing the ML/FT Risks

2.1. Overview of Insurance Sector Activities and Participants

The insurance sector offers a range of products and services to individuals and companies designed to provide a guarantee of compensation for specified loss, damage, illness, or death and facilitate financial planning and risk management in the face of uncertain future events. At the most general level, insurance products can be divided into two categories:

- **Insurance of persons and funds accumulation (hereafter referred to as "life and other investment-related insurance")**, which provides *long-term* coverage against the risk of a future loss, such as death, and may serve as an alternative long-term savings or investment vehicle (e.g., to be paid out upon retirement); and
- **Property and liability insurance (hereafter referred to as "general insurance")**, which provides *shorter-term* coverage against the risk of specific losses, such as damage to property, illness and associated medical expenses, or personal or corporate liability.

Both types of insurance may be offered in the UAE by conventional and Takaful insurance companies. The classes and types of the above-mentioned insurance categories are defined by Articles 3 and 4 of the Executive Regulation[2] of the Federal Law No. (6) of 2007 on the Establishment of the Insurance Authority & Organization of Its Operations as amended by Federal Law No. 3 of 2018 ("Insurance Law")).

Under Article 2.16 of the AML-CFT Decision as amended, **only life insurance and other investment-related insurance products are subject to the UAE's AML/CFT legal and regulatory framework.** It is therefore critical that each licensed insurer, re-insurer, agent, and broker undertakes a comprehensive assessment of its ML/FT risks, including especially the risks associated with its life insurance and other investment-related insurance product offerings, and that it designs and implements an AML/CFT compliance program that is commensurate with those risks.

Insurance sector participants include **operators** in the insurance sector, which sell or facilitate the sale of insurance products and must be licensed by the CBUAE, and **customers** who own, pay for, and/or are covered by or the beneficiaries of insurance products.

Principal insurance sector operators, as defined by the Insurance Law, include:

- **Insurers**, defined as any insurance company incorporated in the UAE or foreign company licensed to carry out insurance operations in the UAE according to the provisions of the Insurance Law, including Takaful insurance companies.
    - *Note: An insurer can issue insurance policies to consumers, or to other insurers or **re-insurers**, in exchange for payment of a premium.*
- **Re-insurers,** defined as any re-insurance company incorporated in the UAE of foreign re-insurance company licensed to carry out insurance operations inside the UAE or a foreign re-insurance company outside the UAE.
    - *Note: Reinsurers are insurers that issue insurance policies to customers that are themselves insurers or reinsurers. Reinsurance includes both "treaty" agreements, which*

[2] Insurance Authority – The Board of Directors' Resolution No2 of 2009 on Issuance of the Executive Regulation of the Federal Law No6 f 2007 on Establishment of the Insurance Authority and Organization of the Insurance Operations (Published in the Official Gazette No504 on 31/01/2010).

cover broad groups of policies issued by the primary insurer, as well as "facultative" agreements, which cover specific policies or risks, negotiated on an ad hoc basis.

- **Insurance agents**, defined as any natural or legal person approved and authorized by the insurance company to carry out insurance operations on its behalf or on behalf of any branch thereof.
    - *Note: All insurance agents are "tied" agents, meaning they have a contractual agreement to underwriting and sell insurance products exclusively on behalf of a single insurer. Persons who are contractually free to sell insurance on behalf of multiple insurers or as a freestanding intermediary between insurers and consumers are referred to as insurance brokers, as defined below.*
- **Insurance brokers**, defined as any legal person who independently intermediates in insurance and re-insurance operations between the insurance or re-insurance seeker on one side and any insurance or re-insurance company on the other side and receives for his efforts commission from the insurance company or the re-insurance company with which the insurance or re-insurance has been accomplished.
    - *Note: Insurance brokers can be authorized by multiple insurers to sell insurance products to consumers (or other insurers or reinsurers) on their behalf or to execute insurance sales as freestanding intermediaries between insurers and consumers, in either case in exchange for payment of a commission from the insurer.*

Under the Insurance Law and supporting Insurance Authority Board Resolutions[3], insurance operators also include:

- Health insurance **third-party administrators**, defined as legal persons licensed by the CBUAE to perform health insurance third party administration in accordance with the provisions of the related instructions (e.g. manage health insurance programs and pay health insurance claims on behalf of an insurer);
- **Insurance producers**, defined as natural or legal persons licensed by the CBUAE to practice the profession of marketing insurance policies through ordinary means or electronic means;
- **Price comparison websites** (also referred to as **"insurance aggregators")**, defined as legal persons registered by the CBUAE to provide insurance premium price comparison services using the Internet;
- **Consultants**, defined as natural or legal persons who study the insurance requirements for his customers, give advice in respect of the suitable insurance coverage, assist in preparing the insurance claims along with conducting the other duties specified in the regulation and receive their fees from his customers;[4]
- **Actuaries**, defined as persons who estimate values of the insurance contracts, documents and the related accounts; and

[3] Including Insurance Authority Board Resolution No. 9 of 2011 Concerning the Instructions for Licensing Health Insurance Third Party Administrators and Regulation and Control of their Business, Insurance Authority Board of Directors' Decision No. 12 of 2018 Concerning the Regulation on Licensing and Registration of Insurance Consultants and Organization of their Operations, Insurance Authority Board of Directors' Resolution No. 27 of 2020 Concerning the Instructions for Licensing Insurance Producers, and Insurance Authority Board of Directors' Resolution No. 18 of 2020 Concerning the Electronic Insurance Regulations.

[4] Unlike agents and brokers, consultants are not authorized to complete insurance sales (or to "bind coverage") on behalf of an insurer.

- **Loss and damage adjusters**, defined as persons who examine the damages occurred to the subject matter of the insurance, and assess them.

However, as these participants are not involved or play a very limited role in selling or facilitating the sale of insurance products, and as per Article 2 of the AML-CFT Decision, they are not included under Section 1.2. Applicability of this Guidance.

Principal insurance sector customers include:

- **Policyholders** or **policy owners**, defined as natural persons, legal persons, or legal arrangements who own and maintain the contractual rights of an insurance policy, including powers to inject funds, establish the beneficiary, and exercise early surrender rights. In the case of a group policy, the policyholder is the owner of the master policy.
- **Policy payers**, defined as natural persons, legal persons, or legal arrangements who pay the necessary premium to keep the policy in force.
- **Insured**, defined by the Insurance Law as natural persons, legal persons, or legal arrangements who concluded an insurance contract with the Insurer.
    - *Note: In many cases, the policyholder, policy payer, and insured will be the same person. The insured will also be the person covered by the insurance policy.*
- **Beneficiaries**, defined by the Insurance Law as natural persons, legal persons, or legal arrangements who acquired the rights of the insurance contract at the start or these rights has been legally transferred thereto.
    - *Note: Beneficiaries and other payees are entitled to receive claim payments, distributions, or other payouts under an insurance policy. The payee of a general insurance policy is typically the insured, although certain property insurance policies may specify a third party, such as a lender or lessor with an interest in the covered property, as entitled to all or part of the claim payments on the policy.*[5]

2.2. ML/FT Risks relevant to life insurance and other investment-related insurance products

Criminal actors may use life insurance and other investment-related insurance products to place illicit proceeds into the financial system, especially (though not exclusively) where the insurer or intermediary accepts premium payments in cash. Such products may be purchased with the intention of either holding the insurance policy over its standard duration or canceling coverage before maturity and, where permitted, withdrawing premiums paid less a penalty (a practice known as “early surrender”) so as to free up funds for alternative uses. Illicit actors may also deliberately overpay premiums and request a refund for the amount overpaid to the insurance carrier in order to trigger payout under a policy. Reimbursed premiums, withdrawn

[5] A policyholder’s **insurable interest** is an interest in the value of the subject of insurance, including any item, event, action, or legal or financial relationship whose loss would cause a financial or other hardship. An insurable interest may result from property rights, contractual rights, or potential legal liability.

contributions, and payout proceeds (whether legitimate or fraudulent) can then be deposited into a bank account or used to purchase other financial instruments without necessarily revealing the ultimate origin of the funds.

As noted above, life and other investment-related products are generally considered to present higher ML/FT risk, particularly where they have high cash values upon surrender. The following methods may be employed to launder funds through life insurance and other investment-related insurance products or relationships:

- Assigning policies and payments to third parties, especially through policies (such as secondhand endowment and bearer insurance policies) that allow the policyholder to change the beneficiary before maturity or surrender without the knowledge or consent of the insurer;
- Borrowing against the cash surrender value of permanent life insurance policies or using a policy as collateral to purchase other financial instruments;
- Selling units in investment-linked products, such as annuities;
- Buying products with insurance termination features without concern for the product's investment performance; and
- Establishing fictitious insurance or reinsurance companies or intermediaries in order to place or move illicit proceeds without revealing the true source of funds.

In addition to these vulnerabilities, the insurance sector is also vulnerable to abuse from other types of economic crime, particularly orchestrated fraud. Moreover, even where insurance products or relationships are not directly abused to launder money or perform other illicit transactions, insurance may be purchased by illicit actors to provide an appearance of legitimacy to the underlying, insured activities. As per Article 11.2 of the AML-CFT Decision, **LFIs must consider the customer and the beneficiary of life insurance and family Takaful policies as risk factors when determining the applicability of enhanced due diligence procedures (EDD).**

The remainder of this section presents additional examples of key ML/FT risk factors relevant to the insurance sector for life insurance and other investment-related insurance products, organized by risks related to insurance products, services and transactions, distribution channels and intermediaries, customers, and geographies. These should be considered by insurance sector operators when performing their financial crimes risk assessments (see section 3.1) and determining the risks presented by specific customers or business activities. Individual risks may be heightened in view of the UAE's national and regional circumstances and the composition of the local insurance sector. Where a risk factor is coupled with one or more of the red flag indicators provided in Annex 1 of this Guidance, insurance sector operators should consider assigning additional resources or controls to the area of heightened risk, such as by applying enhanced due diligence ("EDD") or heightened ongoing monitoring.

Insurance operators are expected to perform and document an enterprise ML/FT risk assessment and keep the risk assessment up to date given material changes to their risk profile or legal, regulatory, or supervisory environment. Additional details on the enterprise risk assessment process and the use of risk assessment findings to support a risk-based approach are provided in section 3.1.

2.2.1. Product Risk Factors

Product risk is assessed by identifying how vulnerable a product is to money laundering and terrorist financing based on the product's design. Product risk should be assessed periodically and when significant changes are made to product offerings, including the development of new products, services, or technologies. Product risk is a significant factor in identifying unusual activity.

The following table describes attributes used to assess the vulnerability of product offerings and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Ability to hold funds or transact large sums	Product design that does not hold a balance or cannot be withdrawn against, such as group benefits	Product design that allows funds to be held on behalf of the customer; high-value or unlimited-value premium payments, overpayments, or large volumes of lower-value payments
Customer anonymity or third-party transactions	Product design that only allows transactions from customers with identification, or where all funds flow back to the customer	Product design that allows deposits and payments by third parties or that provides for non-face-to-face transactions (e.g., mobile apps where payment source is unknown)
Liquidity	Product design that does not permit withdrawals or includes significant fees or other penalties for early withdrawals	Product design that has no (or no significant) fees or other penalties for early withdrawal
Time horizon	Products that are typically held for a long period of time, such as years, until retirement or death	Products that are typically held for a shorter time period
Purpose or intended use of the product	Product design makes it easy to identify if products are not being used as intended	Product design makes it difficult to identify if products are not being used as intended

2.2.2. Service and Transaction Risk Factors

Service and transaction risk can be assessed by identifying how vulnerable a product is to use by a third party or unintended use based on the methods of transaction available. Service and transaction risk is influenced by product design. Understanding potential service and transaction risks in the business is a significant factor in recognizing unusual activity at a customer level.

The following table describes attributes used to assess service and transaction risk and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Difficulty in tracing ownership of funds	Preprinted checks, bill payments, and electronic funds transfer (EFT) payments with verified banking records	Cash, bank drafts in bearer form, travelers checks, counter checks (where ownership information is handwritten or typed in a different

		font than the rest of the check), and potentially some digital currencies
The customer is not the payer or recipient of the funds	The funds are moved from or to another financial institution	The third-party paying or receiving funds has not previously been disclosed
Payment source or recipient is based outside of the country	The recipient or payer is the policyholder and is in a low-risk country	The recipient or payer is the policyholder and is in a higher-risk country or is a third party outside the country (making it more difficult to trade or confirm the source of funds)
Number of transactions	The low number of transactions or transaction frequency that is typical for the product	A large number of transactions back and forth with the customer or third parties, especially where it exceeds typical usage for the product
Transactional patterns	Regular and expected customer account activity	Significant, unexpected, and unexplained change in the customer's typical activity, such as early surrenders or withdrawals where such service is offered

2.2.3. Distribution Channel and Intermediary Risk Factors

The distribution channel is the method a customer uses to open a new policy or account. The distribution channel risk is identified by assessing how vulnerable the channel is to money laundering or terrorist financing activities based on attributes that may make it easier to obscure customer identity.

The risk of failing to identify a customer correctly may be higher for distribution channels that use an intermediary or do not require face-to-face contact. Depending on the product, distribution channel risk may be mitigated by using distributors who are also subject to AML/CFT obligations or a pension scheme subscribed through the customer's employer.

The following table describes attributes used to assess the vulnerability of distribution channels and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
The distributor has AML/CFT obligations	The distributor is overseen by a regulatory authority and subject to AML/CFT laws equivalent to or stronger than the insurer	Distributor is not subject to AML/CFT requirements
Payment to an insurer	Customer pays the insurer directly from their account at a bank or securities dealer	The customer pays the distributor, who then pays the insurer

The direct relationship of customer to insurer	Tied agents, brokers, and banking consultants; products distributed directly by insurers	Non-face-to-face relationships[6] with insurers or agents (e.g., trusts or insurance sold by telephone or online without adequate safeguards for confirmation of identity)

2.2.4. Customer Risk Factors

Customer-based risk factors are assessed to evaluate the level of vulnerability to ML/FT threats posed by customers based on their characteristics. Understanding the inherent risks enables an insurer, agent, or broker to identify appropriate mitigating controls and manage residual risks. Customer risk factors combined with business risk factors can be used as criteria for risk scoring to identify high-risk customers. Such risk factors include:

- Customer identity;
- Third-party involvement;
- Customer's source of wealth or funds;
- Customers who are politically exposed persons ("PEPs"), including the direct family members and close known associates of a PEP, and legal entities where at least one beneficial owner is a PEP; and
- Known criminals, terrorists, or persons on sanctions lists.[7]

The following table describes attributes used to assess customer risks and provides lower- and higher-risk examples of each.

Attribute	Lower-risk example	Higher-risk example
Identification	Customer provides identification or can be identified using third-party sources.	Customer has difficulty producing identification, or the authenticity of the identification provided is questionable
Third-party relationships	No third-party involvement	Customer is controlled by a third party, or there are multiple indicators of third-party deposits or payments; customer is controlled by a gatekeeper (such as an accountant, lawyer, or other professional holding accounts or contracts at the insurer) without any interaction with the beneficial owner
Customer's legal form	Customer is a living person or is a large, publicly-traded legal entity with clear ownership and control	Customer is a legal entity with a complex structure where it is difficult to ascertain those who own or control the entity; policyholder

[6] As discussed in section 3.3.1.5 below, relationships in which personal contact between an insurer or agent and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships.
[7] Please see section 3.5 below and also refer to the Executive Office's "*Typologies on the circumvention of Targeted Sanctions against Terrorism and the Proliferation of Weapons of Mass Destruction":* available at https://www.uaeiec.gov.ae/en-us/un-page?p=2#

		and/or beneficiary are companies with nominee shareholders and/or shares in bearer form
Occupation, business type, or another source of wealth or funds	Customer's business type or occupation is in a lower-risk industry	Customer's business or occupation is in a higher-risk industry (such as a cash-intensive business or an industry that has extensive international exposure or is associated with crime typologies) or is associated with a lower income for a high-value deposit without a confirmed source of funds or wealth (such as inheritance or real estate)
Depth and duration of relationship with customer	Customer has a long history with the insurer or its agents and additional information is on file (such as credit underwriting, insurance underwriting, customer due diligence, etc.)	Customer is new to the insurer or insurer has little or no experience with the customer
Customer only holds accounts with lower risk products and services	Customer holds policies or accounts that are registered with the government, such as a registered retirement savings plan	Customer only holds non-registered policies or accounts (e.g., investment or bank accounts with an affiliate)
Political exposure	Customer does not have any ties to politically exposed persons	Customer is considered a politically exposed person, particularly from a foreign jurisdiction
Other screening results	Customer does not have negative news media or media confirms what is known about the customer (such as career confirmation or community engagement)	Customer has ties to or is on a designated sanctions list; has a history of predicate offenses; or is associated with negative news

2.2.5. Geographic Risk Factors

A customer's geographic location or connections may indicate a higher risk for ML/FT activities. To mitigate risk, controls are recommended based on domestic and international geographic risk factors. Where available, data from internal insurer historical case experiences or government data based on crimes applicable to ML or predicate offenses can be used to inform the assessment of domestic geographical risk. Customer risk is higher among customers with connections outside the country, especially connections to higher-risk countries. According to the National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates, the regions and jurisdictions most often involved in criminal activity in relation to the UAE were Pakistan, India, Iran, Bangladesh, China, Russia, South Africa, Nigeria, Somalia, Lebanon, Yemen, Syria, Iraq, Afghanistan, and North Africa. The following table describes attributes used to assess geographic risks and provides each's lower- and higher-risk examples.

Attribute	Lower-risk example	Higher-risk example

Higher-crime regions	Customer does not reside in a region with higher frequency and severity of crimes with ML risk, based on the insurer's own risk assessment (utilizing historical case experiences or government data where appropriate)	Customer resides in a region with high frequency and severity of crimes with ML risk, based on the insurer's own risk assessment (utilizing historical case experiences or government data where appropriate)
History high-risk activity or fraud	Customer does not reside in a region that experiences a higher incidence of high-risk activity or fraud	Customer resides in a region that experiences a higher incidence of high-risk activity or fraud
Foreign tax or physical residency of customer	Countries risk rated as low by the insurer	Countries risk rated as high by the insurer
Foreign ties or transactions	Customer does not have any indicators of foreign residency or transactions outside of country	Customer has requested or performed transactions with ties to high-risk countries, including especially those on the NAMLCFTC's and FATF's lists of high-risk jurisdictions subject to a call for action and jurisdictions under increased monitoring.

3. Mitigating Risks

The sections below discuss how insurance operators can apply preventive measures to identify, assess, manage, and mitigate the risks associated with the insurance sector for life insurance and other investment-related insurance products. This is not a comprehensive discussion of all AML/CFT requirements imposed on insurance sector participants; insurers, agents, and brokers should therefore consult the UAE legal and regulatory framework currently in force.

The controls discussed below should be integrated into each institution's larger AML/CFT compliance program and supported by appropriate governance, training, and independent audit. As discussed in section 3.6 below, insurers are permitted to delegate the performance of specified controls to insurance agents, brokers, banks, or other intermediaries, using either a **third-party reliance** or an **outsourcing** model.

- Under a **third-party reliance** model, insurers may rely on any third-party LFI, such as a bank, insurance agent, or insurance broker, to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, following *the third party's* AML/CFT policies and procedures. In such circumstances, the third party will usually have an existing business relationship with the customer, which is independent of the relationship to be formed by the customer with the relying institution. The third-party reliance model is most commonly employed in the case of insurance brokers, who sell insurance products to consumers on behalf of multiple insurers and therefore typically maintain and apply their own AML/CFT policies and procedures.

- Under an **outsourcing** model, by contrast, insurers may engage a third-party service provider, such as an insurance agent, broker, or other intermediaries, to apply some or all of the AML/CFT preventive measures described in this section on behalf of the delegating institution, following *the insurer's* AML/CFT policies and procedures. In an outsourcing scenario, the third party is subject to the delegating insurer's control regarding the effective implementation of those policies and procedures by the outsourcing entity. The outsourcing model is most commonly employed in the case of tied agents, who sell insurance products to consumers exclusively on behalf of a single insurer and therefore typically follow the insurer's AML/CFT policies and procedures.

Under either model, **the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures** (including maintaining the availability of all relevant data and records), and the arrangement must satisfy the conditions set forth in section 3.6 below**.**

3.1. Risk-Based Approach and Enterprise Risk Assessment

Under article 4 of the AML-CFT Decision, the insurance operator is required to perform, document, and keep up to date an enterprise risk assessment for the purposes of identifying, assessing, and understanding its ML/FT risks for life insurance and other investment-related insurance products, including those arising in relation to its:

- Products;
- Services and transactions;
- Distribution channels and intermediaries;
- Customers; and
- Geographies, in terms of both the jurisdictions or regions in which has operations and the jurisdictions or regions in which its customers are located or do business.

The insurance operator is expected to document the methodology and findings of the risk assessment, considering all relevant risk factors before determining the level of overall risk and the appropriate type and extent of mitigation to be applied. Insurance operators must keep their risks assessments up to date and ensure that identified risks are within the institution's risk appetite and that identified deficiencies are appropriately tracked and remediated. Risk assessments should provide a consolidated assessment of the insurance operator's ML/FT risks across all business units, product lines, and delivery channels, including those of branches, subsidiaries, parent entities, or other affiliates located outside the UAE.

ML/FT risk factors relevant to the insurance sector for life insurance and other investment-related insurance products can be found in section 2.2 above, and red flag indicators for the UAE insurance sector are provided in Annex 1. Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 4[8] for further information.

3.2. New Products, Practices, and Technologies

[8] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

Under Article 23 of the AML-CFT Decision, an insurance operator is required to identify and assess the ML/FT risks for life insurance and other investment-related insurance products that may arise in relation to:

- The development of new products and new business practices, including new delivery mechanisms (such as mobile insurance applications, insurance portals, transaction terminals, and insurance booths); and
- The use of new or developing technologies for both new and preexisting products.

An operator must undertake such risk assessments prior to the launch or use of new products, practices, and technologies and must take appropriate measures to manage and mitigate the identified risks. Operators should pay special attention to new products, practices, or technologies that favor anonymity.

3.3. Customer Due Diligence

3.3.1. *General CDD Measures*

For life insurance and other investment-related insurance products, insurance operators must perform customer due diligence ("CDD") on their customers, defined as natural persons, legal persons, or legal arrangements with whom an insurer, agent, or broker establishes or intends to establish a business relationship to carry out insurance operations, as defined in Articles 4 and 5 of the Insurance Law.

Unless otherwise specified below, the customer of an insurance operator is the existing or prospective **policyholder**, defined as the *natural person, legal person, or legal arrangement* who owns and maintains the contractual rights of the insurance policy. Where the insurer is acting as a reinsurer, the customer will be the insurer (or reinsurer) in whose name the reinsurance policy is issued. Additionally, in the case of group life insurance or other policies, when the insured persons have active powers on the contract (e.g., to inject sums into the contract, establish the beneficiary, or exercise early surrender of the amounts), those persons should be considered equal to customers, and life insurers and relevant intermediaries should therefore conduct CDD on these persons, as well as on their related third parties. In cases where the insured persons have no active powers, their names should be screened against sanctions lists, but they are not considered customers for AML/CFT purposes, and insurers and intermediaries are not required to conduct full CDD checks on them.

Finally, although in most cases the policyholder will also be the party who pays the necessary premium to keep the policy in force, there may be exceptional cases in which the policy payer is an unrelated third party (referred to as a **third-party payer**). In such cases, the insurer—or its agent, under a third-party reliance or outsourcing arrangement, if applicable—should perform the following general CDD measures on *both* the policyholder and the third-party payer.

3.3.1.1. Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, insurance operators are required to identify and verify the identities of all customers. Customers should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, as per Article 4.3 of the AML-CFT Decision, where there is no ML/FT suspicion and ML/FT risks are assessed to be low, an operator may complete the verification of the customer's identity after establishing a business relationship, as set forth in section 3.3.3 below.

When verifying the Emirates ID card either physically, by way of digital or electronic Know Your Customer (e-KYC) solutions, the insurance operator must use the online validation gateway of the Federal Authority for Identity & Citizenship, Customs & Port Security, the UAE-Pass Application or other UAE Government supported solutions, and keep a copy of the Emirates ID and its digital verification record. Where passports, other than the Emirates ID are used in the KYC process, a copy must be physically obtained from the original passport which must be certified (i.e. certified copy) as "Original Sighted and Verified" under the signature of the employee who carries out the CDD process and retained.

Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.1, for further information.

3.3.1.2. Beneficial Owner Identification and Verification

Under Article 9.1 of the AML-CFT Decision, insurance operators are required to identify and verify the identities of all beneficial owners of any legal person customer, defined as all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25 percent or more. Where no individual meets this description, the operator is required to identify and verify the identity of the individual(s) holding the senior management position in the entity. This option should be used only as a last resort, however, and when the operator is confident that no one individual, or small group of individuals, exercises control over the customer.

Under Article 9.2 of the AML-CFT Decision, for legal arrangements, insurance operators must verify the identity of the settlor, the trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement and obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment, or at the time he/she intends to exercise his/her legally acquired rights. The beneficial owner of a legal person or arrangement must be an individual. Another legal person cannot be classified as the beneficial owner of a customer, no matter what percentage it owns. Insurance operators should continue tracing ownership all the way up the ownership chain until it identifies all individuals who own or control at least 25 percent of the operator's customer. If the insurance operator has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the operator should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so for legal person is to identify additional beneficial owners below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10 percent or even the 5 percent level, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

Beneficial owners should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, pursuant to Article 4.3 of the AML-CFT Decision, where there is no ML/FT suspicion and ML/FT risks are assessed to be low, an operator may complete verification after establishing a business relationship, as set forth in section 3.3.3 below.

Please consult also the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.3.1 and 6.3.3, respectively, as well as the *CBUAE's Guidance for LFIs providing services to Legal Persons and Arrangements*[9] for further information.

3.3.1.3. Understanding the Nature of the Customer's Business and the Nature and Purpose of the Business Relationship

Under Article 8 of the AML-CFT Decision, insurance operators are required to understand the nature of the customer's business and the nature and purpose of the operator's relationship with the customer, including the expected uses to which the customer will put the operator's products or services. This step requires the operator to collect information that allows it to create a profile of the customer, including the types and volumes of transactions the customer is expected to engage in, and to assess the risks associated with the relationship. In certain instances, the expected type and volume of transactions are implicit in the specific insurance product being provided, in which case this aspect of the customer's profile can be derived directly from the product choice.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship—together with the ongoing analysis of actual customer behavior and the behavior of relevant peer groups—allows the insurance operator to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. This element of CDD can also serve to inform the operator's risk rating or other risk assessment of the customer for the purposes of performing risk-based ongoing monitoring (see section 3.3.1.4) and determining whether simplified or enhanced due diligence measures may be warranted (see sections 3.3.3 and 3.3.4, respectively).

3.3.1.4. Ongoing Monitoring

Under Article 12 of the AML-CFT Decision, insurance operators are required to subject all customers to ongoing monitoring throughout the business relationship. Ongoing monitoring ensures that the operator's products and services are being used in accordance with the customer profile developed through CDD during onboarding, and that transactions are normal, reasonable, and legitimate.

Insurance operators are required to ensure that the CDD information they hold on all customers is accurate, complete, and up to date. This is particularly crucial in the context of customers that are companies or that engage in business. Operators should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

CDD updates should include a refresh of all elements of initial CDD, and in particular should ascertain that:

- The customer's beneficial owners remain the same;
- The customer continues to have active status with a company registrar;
- The customer has the same legal form and is domiciled in the same jurisdiction; and
- The customer is engaged in the same type of business and in the same geographies.

[9] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

In addition to a review of the customer's CDD file, under Article 7 of the AML-CFT Decision, the operator must also review the customer's transactions to ensure that the transactions conducted are consistent with the information they have about the customer, their type of activity and the risks they pose, including, when necessary, the source of funds. It must determine whether they continue to fit the customer's profile and business and are consistent with the business the customer is expected to engage in when the business relationship was established. This type of transaction review is distinct from the transaction monitoring discussed in section 3.4 below and its purpose is to complement it by identifying behaviors, trends, or patterns that are not necessarily subject to transaction monitoring rules. The techniques used for transaction review will vary depending on the customer. For lower-risk customers, a review of alerts, if any, is likely to be sufficient. For higher-risk customers, a more intensive review may be necessary. For customers with a large volume of transactions, operators may use data analysis techniques.

If the review finds that the customer's behavior or information has materially changed, the operator should risk-rate the customer again. New information gained during this process may cause the operator to determine that EDD is necessary or may bring the customer into the category of customers for which EDD is mandatory (i.e., customers that are PEPs, or owned or controlled by PEPs, the direct family members or associates known to be close to the PEPs; customers that are based in high-risk jurisdictions; etc.).

Operators may consider requiring that the customer update them on any changes in its beneficial ownership or business activities. Even if this requirement is in place, however, operators should not rely on the customer to notify it of a change but should still update CDD on a schedule appropriate to the customer's risk rating.

3.3.1.5. Non-Face-to-Face Relationships

Insurance operators should develop policies and procedures to address any specific risks associated with non-face-to-face customer relationships and transactions undertaken in the course of such relationships. Such policies and procedures should be applied when establishing a new customer relationship and when conducting ongoing monitoring, and should be at least as stringent as those that would be required to be performed if there was face-to-face contact.

- *Note: Relationships in which personal contact between an insurer or agent and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships for the purpose of this Guidance.*

Heightened ML/FT risks may arise from establishing business relationships or undertaking transactions according to instructions conveyed by customers over the internet (absent personal contact via video teleconference), post, fax, or telephone. An operator should note that online applications and transactions may pose greater risks than other non-face-to-face business due to the following factors, which taken together may compound the associated ML/FT risks:

- The ease of unauthorized access to the facility, across time zones and locations;
- The ease of making multiple fictitious applications without incurring additional cost or the risk of detection;
- The absence of physical documents; and
- The speed of electronic transactions.

The measures taken by an insurance operator for verifying the identity of customers and beneficial owners in the context of non-face-to-face relationships will depend on the nature and characteristics of the product or service provided and the customer's risk profile. Where verification of identity is performed without face-to-face contact (e.g., electronically), an operator should apply additional checks to manage the risk of impersonation. The additional checks may consist of robust anti-fraud checks that the operator routinely undertakes as part of its existing procedures, which may include as appropriate and feasible:

- Telephone contact with the customer at a residential or business number that can be verified independently;
- Confirmation of the customer's address through an exchange of correspondence or other appropriate method;
- Subject to the customer's consent, telephone confirmation of the customer's employment status with his or her employer's human resource department at a listed business number of the employer;
- Confirmation of the customer's salary details by requiring the presentation of recent bank statements where applicable;
- Provision of certified identification documents by lawyers or notaries public;
- Requiring the customer to make an initial premium payment using a check drawn on the customer's personal account with a bank in the UAE; and
- Video call with the customer.

3.3.1.6. Name Screening

An insurance operator should screen the following parties against relevant ML/FT information sources (such as negative media databases) and internal watchlists (such as lists of customers previously exited for financial crime reasons) prior to a customer's onboarding:

- All customers, regardless of risk rating or risk profile;
- Beneficial owners of legal entity customers;
- Natural persons appointed to act on behalf of the customer (see section 3.3.2.1);
- Directors, partners, and managers of customers that are legal persons;
- Natural persons having executive authority over customers that are legal arrangements; and
- Insured with no active powers on the contract (if any).

With respect to sanctions lists, the parties listed above must be screened prior to a customer's onboarding and on an ongoing basis thereafter (please see section 3.5 below). In addition, *at the time of payout*, an insurer must screen against sanctions lists and should screen against the same other lists and information sources all beneficiaries or other payees and their beneficial owners (where applicable).

The results of screening and assessment by the insurance operator should be documented. Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*[10] for further information.

3.3.1.7. Customer Rejection and Exit

Insurance operators should not deal with any person on an anonymous basis or any person using a fictitious name. Prior to establishing an insurance relationship, if an insurance operator has any reasonable grounds to suspect that the assets or funds of a customer are the proceeds of crime or related to the financing of terrorism, the operator should reject the business relationship and, per Article 17 of the AML-CFT Decision, file a suspicious transaction report ("STR") with the UAE Financial Intelligence Unit ("FIU").

As per article 13 of the AML-CFT Decision, where an insurance operator is unable to undertake the CDD measures described above, or is a confirmed match to a party included on applicable sanctions lists, the insurance operator must:

- Not onboard the customer;
- Exit the relationship if one has been established;
- Not make any payment to a payee or beneficiary under the customer's policy or other insurance relationship; and
- Maintain the related records (Please see Section 3.10 below).

In addition, it should add the customer, its beneficial owners, directors, and managers to internal watchlists. The operator should also determine whether the circumstances warrant the filing of a suspicious transaction report ("STR") or SAR.

3.3.2. Specific CDD Measures for Insurers

In addition to performing general CDD on their customers, insurers are also expected to collect and verify the identities of any natural persons appointed to act on the customer's behalf and are required, under Article 11 of the AML-CFT Decision, to collect and verify the identities of the beneficiaries or other payees of an insurance policy and their beneficial owners (where applicable), as set forth below.

3.3.2.1. Identification and Verification of Natural Persons Appointed to Act on a Customer's Behalf

As per Article 8.2 of the AML-CFT Decision, where a customer appoints one or more natural or legal persons (such as an insurance broker) to act on his, her, or its behalf in establishing a business relationship with an insurer, the insurer must identify and verify the identity of each such natural person in accordance with the same procedures used to identify and verify the identity of a natural person customer. The insurer should also verify the due authority of each natural person appointed to act on behalf of the customer by obtaining, at a minimum:

[10] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

- The appropriate documentary evidence authorizing the appointment of such natural or legal person by the customer to act on his, her, or its behalf; and
- The signature of such a natural or legal person appointed.

As with customers, natural persons appointed to act on a customer's behalf should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, where there is no ML/FT suspicion, and ML/FT risks are assessed to be low, and where the deferral of verification is essential in order not to interrupt the normal course of business operations, an operator may complete the verification of the appointed person's identity after establishing a business relationship, as set forth in section 3.3.3 below.

3.3.2.2. Identification and Verification of Beneficiaries or Other Payees and Their Beneficial Owners

Under Article 11.1 of the AML-CFT Decision, insurers are required to conduct CDD measures, including ongoing monitoring, with respect to any beneficiary of life insurance and other investment insurance insurance products, including life insurance products relating to investments and family Takaful insurance, as soon as the beneficiary is identified or designated. In addition, *as soon as a beneficiary or other payee is designated*, an insurer must perform the following:

- For a beneficiary or payee who is identified as a specifically named natural person, legal person, or legal arrangement, obtain the full name, including any aliases, of such beneficiary or payee; or
- For a beneficiary or payee who is designated by characteristics, class, or other means, obtain sufficient information concerning the beneficiary or payee to satisfy itself that it will be able to establish the identity of such beneficiary or payee at the time of payout.
- *At the time of payout*, insurers must also verify the identities of all beneficiaries or payees and their beneficial owners in accordance with the same procedures used to identify and verify the identity of a natural person customer.

3.3.3. Simplified Due Diligence for Lower-Risk Scenarios

As per Article 4.3 of the AML-CFT Decision, an insurance operator may perform simplified due diligence ("SDD") measures in relation to a customer, a beneficial owner of a customer, a natural person appointed to act on behalf of a customer, or a beneficiary or other payee if it is satisfied that the risks of ML/FT are low. The assessment of low risks should be supported by an adequate analysis of risks by the insurance operator, and the selection of simplified measures should be commensurate with the type and level of risk identified through such risk analysis. In all cases, the operator should document the details of its risk analysis and the nature of the SDD measures employed.

Examples of potentially lower-risk scenarios include, but are not limited to, those in which:

- The customer is a UAE government entity, including UAE state-owned enterprises;
- The customer is an entity listed on a stock exchange and subject to regulatory disclosure requirements relating to adequate transparency with respect to beneficial owners;

- The insurance product does not offer cash payouts except upon the occurrence of specified trigger events;
- The insurance product does not have an early surrender option and cannot be used as collateral; or
- The insurance product is a pension or other scheme where contributions are made via deduction from wages and scheme rules and do not permit the assignment of a member's interest under the scheme.

Additional examples of lower-risk attributes for the insurance sector are provided in section 2.2 above.

Where an insurance operator is satisfied that the ML/FT risks are low, the operator may perform one or more of the following SDD measures, as warranted by the risk analysis:

- Verifying the identity of the customer and any beneficial owner(s) after establishing the business relationship, provided verification is nonetheless completed in a timely fashion (to be documented in the operator's internal procedures) and appropriate controls are in place to manage the ML/FT risks associated with the customer and the relationship prior to verification;[11]
- Reducing the frequency of updates to CDD information;
- Reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
- Developing an understanding of the intended nature and purpose of the customer relationship on the basis of the relationship type and the customer's historical transaction activity, rather than by collecting information regarding the intended nature and purpose of the relationship during onboarding or CDD updating.

An insurance operator should not perform SDD measures where:

- A customer or any beneficial owner of the customer is from or in a country or jurisdiction against which the FATF has called for countermeasures;
- A customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the operator for itself or notified to operators generally by local regulatory or supervisory authorities; or
- The operator suspects that ML or FT is involved.

3.3.4. Enhanced Due Diligence for Higher-Risk Scenarios

The AML-CFT Law and the AML-CFT Decision impose specific and enhanced due diligence obligations on insurance operators with respect to two classes of customers or transactions:

- Customers that are politically exposed persons ("PEPs"), which include the direct family members or associates known to be close to the PEPs; and

[11] Such measures may include holding funds in suspense or escrow until verification of identity has been completed or making completion of identity verification a precondition of closing any transaction with or on behalf of the customer.

- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries.

The AML-CFT Law and Decision give special attention to customers in these groups because they are likely to expose operators to a heightened risk of money laundering, terrorism financing, and other illicit finance.

In addition to these classes of customers and transactions, for which EDD is mandatory, operators are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for ML or FT. Examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The customer belongs to a higher-risk industry or sector identified in topical risk assessments, or to an industry or sector identified by the operator as higher-risk for ML or FT;
- The ownership structure of a legal entity customer appears unusual or excessively complex given the nature of the legal entity's business;
- The legal entity customer is a personal asset-holding vehicle;
- The business relationship is conducted under unusual circumstances, such as significant unexplained geographic distance between the operator and the customer;
- The legal entity customer has nominee shareholders or shares in bearer form;
- The customer is a cash-intensive business;
- The customer operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, or inadequate AML/CFT measures, as identified by the FATF;
- The customer operates in or does business with a jurisdiction identified by credible bodies (e.g., reputable international bodies such as Transparency International) as having significant levels of corruption, terrorism financing, or other criminal activity;
- The relationship involves or could involve cash or anonymous transactions;
- The relationship involves or could involve frequent payments received from unknown or unassociated third parties.

Additional examples of higher-risk attributes and red flag indicators for the insurance sector are provided in section 2.2 and Annex 1 of this Guidance respectively.

As per Article 4.2 b) of the AML-CF Decision, where the operator identifies a customer or relationship as presenting higher ML/FT risks, it must apply EDD measures commensurate with those risks. Examples of EDD measures include but are not limited to:

- Obtaining approval from the operator's senior management to establish or continue a business relationship with the customer, including making any payment to a beneficiary or payee;
- Establishing the source of wealth and source of funds of the customer and any beneficial owner of the customer;

- Conducting enhanced monitoring during the course of the business relationship with the customer, including by increasing the degree and nature of transaction monitoring and CDD updating;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar or equivalent CDD standards;
- Using public sources of information (e.g., websites) to gain a better understanding of the reputation of the customer or any beneficial owner of the customer;
- Commissioning external intelligence reports where it is not possible for the operator to easily obtain information through public sources or where there are doubts about the reliability of public information; and
- For high-net-worth individuals, particularly those utilizing higher-risk products or services or characterized by other markers of heightened ML/FT risk:
    - Independently corroborating information obtained on the source of wealth of customers and beneficial owners against documentary evidence or public information sources;
    - Screening operating companies and individual benefactors contributing to the customer's and beneficial owner's wealth or funds; and
    - Scrutinizing transactions relating to customers that have multiple policies with the operator or to customers having a common beneficial owner.

In addition, as noted in section 3.3.1.2 above, if the insurance operator has followed its standard beneficial ownership identification and verification procedures and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the operator should consider intensifying its efforts to identify the beneficial owners. The most common method of doing so is to identify additional beneficial owners below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of beneficial owners at the 10 percent or even the 5 percent level, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

Additional examples of EDD measures are provided in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.4.

3.4. Transaction Monitoring and Suspicious Transaction Reporting

3.4.1. Transaction Monitoring

Under Article 16 of the AML-CFT Decision, insurance operators must monitor activity by all customers to identify behavior that is potentially suspicious and that may need to be the subject of an STR or SAR when conducting operations related to life insurance and other investment-related insurance products. Transactions may be suspicious simply in virtue of their individual characteristics (such as their value, source, destination, or use of intermediaries) or because, together with other transactions, they form a pattern that diverges from expected or historical transactional activity or may otherwise be indicative of illicit activity, including the evasion of reporting or recordkeeping requirements. When monitoring and evaluating

transactions, the operator should take into account all information that it has collected as part of CDD, including the identities of beneficial owners. In addition, higher-risk customers should be subject to more stringent transaction monitoring, with lower thresholds for alerts and more intensive investigation.

Transaction monitoring can include manual monitoring processes and the use of automated and intelligence-led monitoring systems. In all cases, the appropriate type and degree of monitoring should appropriately match the ML/FT risks of the operator's customers, products and services, delivery channels, and geographic exposure, and may therefore vary across an operator's business lines or units, where applicable.

Transaction monitoring programs should also be calibrated to the size, nature, and complexity of each institution. Operators with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. Operators utilizing automated systems should perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. While smaller operators may rely on transaction monitoring systems that are less automated, they should still ensure that these are appropriately executed to address the risks from their day-to-day transactional activity.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening* for further information.

3.4.2. STR Reporting

As required by Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, insurance operators must file without any delay an STR or SAR with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. STR/SAR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system. STR/SAR filings are essential to assisting law enforcement authorities in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an operator suspects that a transaction or funds are linked to a crime, operators should consider filing an STR or SAR in the following situations involving higher-risk customers:

- A potential customer decides against purchasing financial services after learning about the operator's CDD requirements;
- A current customer cannot provide required information (including documentation) about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- The operator is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the operator should not establish the business relationship, or continue an existing business relationship; or
- Other situations that are suspicious or involve activity with no legitimate business or other lawful purpose.

Please consult the CBUAE's *Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*[12] for further information.

3.5. Sanctions Obligations and Freezing Without Delay

The AML-CFT Law and AML-CFT Decision require insurance operators to promptly apply directives issued by the Competent Authorities of the UAE for implementing the decisions issued by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision No. (74) of 2020 sets out the legislative and regulatory framework regarding the Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List. As per Cabinet Decision 74 and in particular its Article 15, **all insurance operators without any exception,** are obliged to apply policies, procedures and controls to implement TFS to those sanctioned and designated in the Local Terrorist List and the UN Consolidated List.

For more information and details on their obligations in relation to their sanctions obligations, insurance operators should consult the Executive Office for Control and Non-Proliferation (former Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's – referred to as the Executive Office) "*Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions*"[13]; the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions* as well as the CBUAE*'s Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening* and any of their amendments or updates thereof. Insurance operators should also consult the CBUAE's and the Executive Office's websites as updated from time to time, and refer to the Executive Office's list of Frequently Asked Questions (FAQ) for the insurance sector.

3.6. Third-Party Reliance and Outsourcing

As noted above, insurers are permitted to delegate the performance of specified controls to insurance agents or other intermediaries, using either a **third-party reliance** or an **outsourcing** model.

- Under a **third-party reliance** model, insurers may rely on any third-party LFI, such as a bank or insurance agent or broker, to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, following *the third party's* AML/CFT policies and procedures. In such circumstances, the third party will usually have an existing business relationship with the customer, which is independent of the relationship to be formed by the customer with the relying institution. The third-party reliance model is most commonly employed in the case of insurance brokers, who sell insurance products to consumers on behalf of multiple insurers and therefore typically maintain and apply their own AML/CFT policies and procedures.
- Under an **outsourcing** model, by contrast, insurers may engage a third-party service provider, such as an insurance agent or other intermediary, to apply some or all of the AML/CFT preventive measures described in this section on behalf of the delegating institution, following *the insurer's* AML/CFT policies and procedures. In an outsourcing scenario, the third party is subject to the delegating insurer's control regarding the effective implementation of those policies and procedures

[12] Available at: https://www.uaeiec.gov.ae/en-us/un-page.
[13] Available at: https://www.uaeiec.gov.ae/en-us/un-page.

by the outsourcing entity. The outsourcing model is most commonly employed in the case of tied agents, who sell insurance products to consumers exclusively on behalf of a single insurer and therefore typically follow the insurer's AML/CFT policies and procedures.

Under either model, the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures.

3.6.1. Third-Party Reliance

Insurers are permitted to rely on third-party LFIs to perform the elements of general CDD described in sections 3.3.1.1 through 3.3.1.3, provided the insurer relying on a third party:

- Immediately obtains the necessary CDD information concerning the elements described in sections 3.3.1.1 through 3.3.1.3;
- Takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay;
- Satisfies itself that the third party is regulated, supervised, or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements in line with FATF standards and local law and regulation; and
- Takes appropriate steps to identify, assess, and understand the ML/FT risks specific to the countries or jurisdictions in which the third party operates.

With respect to the second of these conditions, a best practice is for insurers to obtain a copy of the relevant CDD records or have direct access to the database where such information is held, in order to facilitate ongoing monitoring of the business relationship and, if applicable, the filing of STRs and for a complete assessment record in case of a change of intermediary servicing the policy.

Insurers are not permitted to rely on third parties to conduct ongoing monitoring of business relationships (described in section 3.3.1.4), although they may *outsource* such functions following the guidelines described immediately below.

3.6.2. Outsourcing

In an outsourcing or agency scenario, the outsourced entity applies CDD or other AML/CFT measures on behalf of the delegating insurer, in accordance with the insurer's internal policies and procedures, and is subject to the insurer's control of the effective implementation of those policies and procedure by the outsourced entity. When outsourcing a part of their AML/CFT function, including the distribution of products, an insurer should therefore include any outsourced entity in its own AML/CFT program and internal control processes, and should monitor such an entity for compliance with its internal AML/CFT policies and procedures. Outsourced entities should also be subject to the employee and agent screening and monitoring checks described immediately below.

3.7. Employee, Officer, Agent, and Broker Risk Management

Insurance operators should have in place screening procedures to ensure high standards when hiring employees, appointing officers, or engaging agents or brokers (including but not limited to outsourced entities, as described in section 3.6.2 above). Employee, officer, and agent or broker screening procedures should include:

- Background checks of employment history; and
- Screening against sanctions lists, ML/FT information sources, and internal watchlists.

In addition, insurance operators should conduct credit history checks on a risk basis. The operator should be aware of potential conflicts of interest for staff with AML/CFT responsibilities and should act to reduce or manage such conflicts of interest, for example by reallocating responsibilities or by instituting quality controls and "four-eye" reviews of the conflicted employee's work.

Operators should also monitor on an ongoing basis for possible indicators of suspicious or illicit behavior by employees, such as:

- An employee whose lifestyle cannot be supported by his/her salary, which may indicate receipt of tips or bribes.
- An employee who is reluctant to take a vacation, which may indicate they have agreed or are being forced to provide services to customers in violation of the law or company policy.
- An employee who is associated with an unusually large number of transactions or a transaction in an unusually large amount, which may indicate they have agreed or are being forced to provide services to customers in violation of the law or company policy.

3.8. Training

As with all risks to which the operator is exposed, the AML/CFT training program should ensure that employees are aware of the risks facing the insurance sector for life insurance and other investment-related insurance products, familiar with the obligations of the operator, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the operator's risk and the nature of its operations, and should be clearly documented in the operator's AML/CFT compliance program and associated training policies, procedures, plans, materials, and attendance records.

3.9. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the operator faces and organized in accordance with the "three lines of defense" model. All three lines of defense must report up to and have the active support and oversight of the operator's senior management, defined broadly to include executives, senior leadership, and the Board of Directors.

Under the model, an operator's business units, sales or relationship managers, and other frontline personnel represent the units or functions that create risk and should therefore serve as the **first line of defense** against ML/TF, and other forms of illicit activity. They should scrutinize customers and their related parties at onboarding and performing periodic and risk-based reviews to update customer information and the operator's understanding of the customer's risks.

The operator's AML/CFT compliance function, in turn, constitutes the **second line of defense**, supporting the frontline units' risk management activities through its system of internal controls and related monitoring, reporting, and risk assessment responsibilities. The core of an effective risk-based program is an appropriately experienced AML/CFT compliance officer, located within the second line of defense, who understands the operator's risks and obligations and who has the resources and autonomy necessary to ensure that the operator's program is effective.

Finally, under article 20.6 of the AML-CFT decision, operators must be subject to independent testing by internal or external auditors, who represent the **third line of defense** by providing independent assurance to the Board and executive management on the effectiveness and adequacy of the operator's governance, risk management, and internal controls. Auditors should have sufficient expertise and understanding of ML/FT risks and requirements and should be fully independent of the activities and reporting structure of the functions subject to independent testing.

Additionally, as per article 32 of the AML-CFT decision, operators with overseas branches, subsidiaries, or other affiliates or legal entities must ensure that all entities within the affiliate network are subject to the AML/CFT policies, procedures, and controls that are at least as stringent as those in place at the entity located in the UAE. Likewise, all entities within the affiliate network should be included in the operator's enterprise risk assessment and subject to AML/CFT independent testing and consolidated governance and oversight.

3.10. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, insurance operators must maintain detailed records associated with their ML/FT risk assessment and mitigation measures as well as records, documents, data and statistics for all financial transactions, all records obtained through CDD measures for both the originators and the beneficiaries, account files and business correspondence, copies of personal identification documents, including STRs/SARs and results of any analysis performed. Operators should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. Operators must make the records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five (5) years, from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

Annex 1. Red Flag Indicators for the UAE Life Insurance Sector

The UAE Insurance Authority (now merged with the CBUAE) has issued the following list of red flag indicators when handling life insurance and other investment-related insurance products.[14] These indicators should be incorporated into an insurance operator's AML/CFT policies, procedures, detection scenarios, and other processes for identifying potentially suspicious activity related to life and general insurance products.

1. The purchase of an insurance product does not reflect a customer's known needs (e.g., purpose of the account).
2. The early surrender of an insurance product is taken at a cost to the customer.
3. The surrender of an insurance product is initiated with the refund directed to a third party.
4. The customer exhibits no concern for the investment performance of a purchased insurance product and instead exhibits significant concern for its early surrender terms.
5. The customer purchases insurance products using unusual payment methods, such as cash or cash equivalents, or with monetary instruments in structured amounts.
6. The customer demonstrates reluctance to provide identifying information when purchasing an insurance product.
7. The customer borrows the maximum amount available from their insurance product shortly after purchase.
8. The customer used to purchase low-premium insurance and pay premiums by making regular payments but suddenly purchases insurance that requires a large lump-sum premium payment, for which no reasonable explanations are provided.
9. The customer purchases an insurance product without concern for the coverage or benefits, or the customer only cares about the procedures for the policy loan, cancellation of insurance policy, or changing beneficiary when purchasing an insurance policy that has a high cash value or requires a high lump-sum premium payment.
10. The customer usually pays a premium by making regular payments but suddenly requests to purchase a large-sum policy by paying off premium all at once.
11. The customer purchases insurance products with high cash value successively over a short period of time, and the insurance products purchased do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
12. The customer pays premiums in cash and in several payments marginally below the threshold for declaration but cannot reasonably explain the source of funds. In addition, the transactions do not appear to be commensurate with the customer's status and income or are unrelated to the nature of the customer's business.
13. The customer, after making a large premium payment for a policy purchased, applies for a large policy loan or cancels the policy in a short period of time, for which no reasonable explanations are provided.

[14] Sources: FATF, *Life Insurance Sector: Guidance for a Risk-Based Approach* (October 2018), available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf; and
U.S. Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, "Insurance," available at: https://bsaaml.ffiec.gov/manual/RisksAssociatedWithMoneyLaunderingAndTerroristFinancing/16.

Annex 2. Synopsis

Purpose of this Guidance	Purpose	The purpose of this Guidance is to assist the understanding of risks and effective performance by CBUAE licensed insurers, agents, and brokers of their AML/CFT obligations.
	Applicability	This Guidance applies to all insurance and re-insurance companies, agents, and brokers that are licensed and supervised by the CBUAE.
Understanding and Assessing ML/FT Risks	Overview of Insurance Sector Activities and Participants	Under Article 2.16 of the AML-CFT Decision, as amended, only direct insurance and re-insurance operations with **respect to insurance of persons and funds accumulation** (referred to as 'life insurance and other investment-related insurance products' hereafter) are subject to the UAE's AML/CFT legal and regulatory framework, with the exception of the targeted financial sanctions' requirements applicable for all insurance operators. Insurance sector participants include **operators** in the insurance sector, which sell or facilitate the sale of insurance products and must be licensed by the CBUAE, and **customers**, who own, pay for, and/or are covered by or the beneficiaries of insurance products. • **Operators** principally include **insurers**, **re-insurers**, **insurance agents**, and **insurance brokers**. Operators also include consultants, actuaries, loss and damage adjusters, third-party administrators, insurance producers, and price comparison websites (or "insurance aggregators"), although due to their reduced risk exposure these operators are not subject to the Guidance with the exception of the requirements relating to targeted financial sanctions. • **Customers** principally include **policyholders** (or "policy owners), **policy payers**, **insureds**, and **beneficiaries**.
	ML/FT Risks relevant to life insurance and other investment-related insurance products	• Criminal actors may use life insurance and other investment-related insurance products to place illicit proceeds into the financial system, especially (though not exclusively) where the insurer or intermediary accepts premium payments in cash. • Reimbursed premiums, withdrawn contributions, and payout proceeds (whether legitimate or fraudulent) can be deposited into a bank account or used to purchase other financial instruments without necessarily revealing the ultimate origin of the funds. • Life and other investment-related products are generally considered to present higher ML/FT risk, particularly where they have high cash values upon surrender (e.g. assigning policies and payments to third parties, borrowing against the cash surrender value of permanent life insurance policies, selling units in investment-linked products or buying products with insurance termination features without concern for the product's investment performance).
	Product Risk Factors	Higher-risk products can include those: whose design allows the insurance operator to hold funds or transact large sums on behalf of the customer; provides for customer anonymity or third-party transactions; has no (or very small) fees or penalties for early withdrawal; allows the product to be held for a shorter period of time; and makes it difficult to identify if products are not being used as intended.
	Service and Transaction Risk Factors	Higher-risk services and transactions can include those: for which it is difficult to trace the ownership of funds; where the customer is not the payer or recipient of the funds; where the payment source or recipient is based outside the country; or involving a large number or transactions back and forth or significant, unexpected, and unexplained changes in the customer's typical activity.
	Distribution Channel and Intermediary Risk Factors	Higher-risk distribution channels can include those: involving a distributor or other intermediary that is not subject to AML/CFT requirements; where the customer pays a distributor, who then pays the insurer; or where the customer has a purely non-face-to-face relationship with insurers or agents (e.g., insurance sold online without adequate safeguards to confirm identity).
	Customer Risk Factors	Higher-risk customers can include those: with incomplete or questionable identification; who are controlled by third parties; that are legal entities with a complex structure; in high-risk industries; making high-value transactions without a confirmed source of funds or wealth; who are new to the insurer; who only hold non-registered policies or accounts; who are politically exposed persons; or who are sanctioned, have ties to sanctioned persons, or are associated with negative news.
	Geographic Risk Factors	Higher-risk geographies can include: regions with high frequency and severity of crimes with ML risk; regions that experience a higher incidence of high-risk activity or fraud; countries risk-rated as high by the insurer; or countries on the NAMLCFTC's or FATF's lists of high-risk jurisdictions or FATF's list of jurisdictions under increased monitoring.

Mitigating Risks	Risk-Based Approach and Enterprise Risk Assessment	Any insurance operator is required to perform, document, and keep up to date an enterprise risk assessment for the purposes of identifying, assessing, and understanding its ML/TF risks for life insurance and other investment-related insurance products and to ensure that identified risks are within the institution's risk appetite and that identified deficiencies are appropriately tracked and remediated.
	New Products, Practices, and Technologies	An insurance operator is required to identify, assess, and take steps to mitigate the ML/TF risks for life insurance and other investment-related insurance products that may arise in relation to: (i) the development of new products and new business practices, including new delivery mechanisms; and (ii) the use of new or developing technologies for both new and preexisting products. The operator must undertake such risk assessments prior to the launch or use of the new products, practices, and technologies and must take appropriate measures to manage and mitigate the identified risks
	Customer Due Diligence ("CDD")	For life insurance and other investment-related insurance products, all insurance operators must perform general CDD on their customers, including customer identification and verification, beneficial ownership identification and verification, understanding the nature of the customer's business and the nature and purpose of the relationship, ongoing monitoring, and name screening. • Additionally, insurance operators are expected to collect and verify the identities of: (i) any natural persons appointed to act on the customer's behalf and (ii) the beneficiaries or other payees of an insurance policy and their beneficial owners. • In low-risk scenarios, insurance operators may perform certain simplified due diligence ("SDD") measures, such as verifying the customer's or beneficial owner's identity after establishing the business relationship, unless there is a suspicious of ML/TF. • In higher-risk scenarios, insurance operators must perform enhanced due diligence ("EDD") measures, such as establishing the source of wealth or funds or conducting enhanced monitoring during the course of the business relationship.
	Transaction Monitoring and STR Reporting	When conducting operations related to life insurance and other investment-related insurance products, Insurance operators must monitor activity by all customers to identify behavior that is potentially suspicious. Insurance operators must file without any delay an STR or SAR with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult CBUAE's *Guidance for Licensed Financial Institutions (LFI) on Transaction Monitoring and Sanctions Screening* as well as CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting*.
	Sanctions Obligations and Freezing without delay	All insurance operators without any exception, are obliged to apply policies, procedures and controls to implement TFS to those sanctioned and designated in the Local Terrorist List and the UN Consolidated List. Please consult the Executive Office for Control and Non-Proliferation (previously known as the Executive Office of the Committee for Goods and Materials Subjected to Import and Export Control's – referred to as the Executive Office) "*Guidance on TFS for Financial Institutions and designated non-financial business and professions*"; the CBUAE's *Guidance for LFIs on the Implementation of Targeted Financial Sanctions* as well as the CBUAE's *Guidance for LFIs on Transaction Monitoring Screening and Sanctions screening*. Insurance operators should also consult the CBUAE's and the Executive Office's websites as updated from time to time (in particular the Executive Office's list of FAQ for the insurance sector).
	Third-Party Reliance and Outsourcing	Insurers are permitted to delegate the performance of specified controls to insurance agents or other intermediaries, using either a third-party reliance model (whereby a third-party licensed financial institution carries out CDD measures following its own AML/CFT policies and procedures) or an outsourcing model (whereby insurers engage a third-party service provider to apply all or some of the insurer's own AML/CFT policies and procedures). Under either model, the insurer retains ultimate responsibility for the implementation of applicable AML/CFT preventive measures.
	Employee, Officer, Agent, and Broker Risk Management	Insurance operators should have in place screening procedures to ensure high standards when hiring employees, appointing officers, or engaging agents or brokers. Operators should also monitor on an ongoing basis for possible indicators of suspicious or illicit behavior.
	Training	An operator's AML/CFT training program should ensure that employees are aware of the risks facing the insurance sector for life insurance and other investment-related insurance products, are familiar with the obligations of the operator, and are equipped to apply appropriate risk-based controls.
	Governance and Independent Audit	The preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the operator faces and organized in accordance with the "three lines of defense" model, comprising business unites, a compliance function, and an independent audit function.