INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Public

Application Paper on Combating Money Laundering and Terrorist Financing

November 2021

About the IAIS

The International Association of Insurance Supervisors (IAIS) is a voluntary membership organisation of insurance supervisors and regulators from more than 200 jurisdictions. The mission of the IAIS is to promote effective and globally consistent supervision of the insurance industry in order to develop and maintain fair, safe and stable insurance markets for the benefit and protection of policyholders and to contribute to global financial stability.

Established in 1994, the IAIS is the international standard setting body responsible for developing principles, standards and other supporting material for the supervision of the insurance sector and assisting in their implementation. The IAIS also provides a forum for Members to share their experiences and understanding of insurance supervision and insurance markets.

The IAIS coordinates its work with other international financial policymakers and associations of supervisors or regulators, and assists in shaping financial systems globally. In particular, the IAIS is a member of the Financial Stability Board (FSB), member of the Standards Advisory Council of the International Accounting Standards Board (IASB), and partner in the Access to Insurance Initiative (A2ii). In recognition of its collective expertise, the IAIS also is routinely called upon by the G20 leaders and other international standard setting bodies for input on insurance issues as well as on issues related to the regulation and supervision of the global financial sector.

Application Papers provide supporting material related to specific supervisory material (ICPs or ComFrame). Application Papers could be provided in circumstances where the practical application of principles and standards may vary or where their interpretation and implementation may pose challenges. Application Papers do not include new requirements, but provide further advice, illustrations, recommendations or examples of good practice to supervisors on how supervisory material may be implemented. The proportionality principle applies also to the content of Application Papers.

International Association of Insurance Supervisors
c/o Bank for International Settlements
CH-4002 Basel
Switzerland
Tel: +41 61 280 8090 Fax: +41 61 280 9151
www.iaisweb.org

This document was prepared by the Financial Crime Working Group of the Market Conduct Subcommittee in October 2013 and updated by the Financial Crime Task Force in November 2021 in consultation with IAIS Members.

This document is available on the IAIS website (www.iaisweb.org).

Contents

Acronyms

AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism
CDD	Customer due diligence
DNFBP	Designated non-financial businesses and profession
FATF	Financial Action Task Force
FIU	Financial intelligence unit
ICP	Insurance Core Principle
ML	Money laundering
PF	Proliferation (of weapons of mass destruction) Financing
PEP	Politically exposed person
RBA	Risk-based approach
STR	Suspicious transaction report
TF	Terrorist financing
TFS	Targeted financial sanctions
UNSCR	United Nations Security Council Resolution

1 Introduction

1. The purpose of this Application Paper is to provide information and advice on how money laundering (ML) and terrorist financing (TF) can occur within the life insurance sector and on measures to mitigate the associated risks. While Insurance Core Principle (ICP) 22 on *Anti-money laundering and combating the financing of terrorism* (AML/CFT) and the accompanying standards and guidance apply to insurance supervisors, this paper is directed to life insurers and intermediaries.[1] This paper establishes neither new standards nor expectations. It is intended to provide an additional resource to firms in the implementation of their AML/CFT programme and is intended to be neither exhaustive nor prescriptive.

2. The insurance sector[2] and other sectors of the financial services industry are potentially at risk of being misused for ML/TF. Criminals look to "legitimise" proceeds of criminal activity by disguising the source, changing the form, or moving funds to a place where they are less likely to attract attention and, therefore, may use the financial sector, including the insurance sector, to do so. Persons involved in organising terrorist acts or terrorist organisations look for ways to finance terrorist acts, terrorists or terrorist organisations. The products and transactions of insurers and intermediaries can potentially provide the opportunity to launder money or to finance terrorism. The insurance sector should, therefore, apply AML/CFT preventive measures commensurate with their risks and report suspicious transactions.

3. The IAIS is an Observer Organisation of the Financial Action Task Force (FATF)[3] and accordingly endorses the FATF Recommendations, which are recognised as the international standards on combating ML/TF and proliferation of weapons of mass destruction. IAIS ICP 22 (Anti-Money Laundering and Combating the Financing of Terrorism) is intended to be consistent with the FATF Recommendations and, consistent with the definition of "financial institution" established by FATF, applies to the underwriting, placement and administration of life insurance and other investment-related insurance policies.

4. The FATF Recommendations embody a risk-based approach (RBA) to AML/CFT. By adopting a RBA, supervisors, insurers and intermediaries should be able to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified, and to enable themselves to make decisions on how to allocate their own resources in the most effective way. The FATF has published a paper entitled "Guidance for a Risk-Based Approach – Life Insurance Sector" (Guidance), which aims to support the implementation of the RBA specifically for the life insurance sector. Although FATF guidance papers are non-binding, the methodology for conducting a FATF mutual evaluation of a country's implementation of the

[1] In this paper, intermediaries include agents, who act primarily on behalf of insurers, and brokers, who act primarily on behalf of customers, consistent with ICP 18.0.13.

[2] The insurance sector includes insurers, reinsurers and intermediaries across many and diverse insurance contexts. Unless specifically stated otherwise, in this Application Paper references to "insurance sector", "insurers" and "intermediaries" means "life insurance sector", "life insurers" and "life insurance intermediaries."

[3] The FATF is an inter-governmental body, established to set international standards for AML/CFT. The FATF standards are comprised of its individual recommendations together with interpretive notes and the applicable definitions in the FATF glossary. In this Application Paper, the term FATF Recommendations encompasses all of these components of the FATF standards. Where a reference is made to a specific FATF Recommendation, it also encompasses any Interpretive Note associated with that recommendation.

FATF Recommendations recognises that assessors may consider FATF guidance papers as background information on how countries can implement specific requirements.

5. The Guidance is directed both to supervisors and to the private sector (life insurers and intermediaries). It underlines that the development of the ML/TF risk assessment is a key starting point for the application of a RBA by life insurers and intermediaries, and should be commensurate with the nature, size and complexity of their business. The Guidance recognizes that the intensity and depth of risk mitigation measures, including customer[4] due diligence (CDD) checks, depend on the ML/TF risks. The Guidance highlights the importance of the internal controls of insurance entities, emphasizing that in all cases the "tone from the top" (ie the involvement of senior management) plays a central role in effective RBA implementation. The Guidance also affirms the obligation of life insurers and intermediaries to report all suspicious transactions.

6. This Application Paper is based on ICP 22, taking into account the FATF Recommendations and the Guidance. ICP 22 expresses neither an expectation nor requirement that a jurisdiction include non-life business within the scope of its AML/CFT supervisory framework. Accordingly, the guidance herein is provided for life insurers and life intermediaries. If a particular jurisdiction has included the non-life sector within its AML/CFT framework, portions of this Application Paper may be helpful for affected firms.[5]

7. The FATF Recommendations include obligations to identify and assess the risks of potential breaches, non-implementation or evasion of the targeted financial sanctions (TFS) related to proliferation financing (PF), as contained in FATF Recommendation 7, and to take action to mitigate these risks. This Application Paper includes, where relevant, reference to the general TFS-related obligations under the FATF Recommendations.

8. Insurers and intermediaries should operate within their respective country's AML/CFT framework. Per FATF Recommendation 1, this framework may reflect decisions, based on proven low risk and consistent with the country's assessment of its ML/TF risks, to allow for simplified measures or exemptions in certain actions which apply some of the FATF Recommendations in that country.

2 Money laundering, terrorist financing and targeted financial sanctions in insurance

2.1 Concepts

9. ML is the processing of the proceeds of crime to disguise their illegal origin. Once these proceeds are successfully "laundered", the criminal is able to enjoy these monies without attracting attention to the underlying activity or the persons involved.

10. TF is the financing of terrorist acts, terrorists or terrorist organisations. ICP 22 states that TF is the wilful provision or collection of funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used in full or in part, to carry out terrorist acts by a terrorist organisation or by an individual terrorist, or to support terrorists or terrorist organisations. Funds that are used to finance terrorist

[4] In this Application Paper, "customer" in some cases specifically refers to a policyholder, and in other cases, refers to the broader business relationship, encompassing a policyholder, beneficiaries and their respective beneficial owners and should be interpreted according to context.

[5] Similarly, ICP 22.0.7 notes that depending upon its assessment of the ML/TF risks posed by the non-life sector, a jurisdiction may consider and apply ICP 22 in whole or in part to that sector as well.

activities may be derived either from criminal activity or may be from legal sources and the nature of the funding sources may vary according to the type of terrorist organisation.

11. Information on trends and techniques used for ML/TF is collected and communicated by the FATF through its Methods and Trends publications.

12. The application of a risk-based approach to TF has both similarities and differences compared to ML. They both require a process for identifying and assessing risk. However, given the characteristics of TF, the risks may be more difficult to assess and the mitigation strategies may be challenging due to considerations such as the relatively low value of transactions involved in TF or the fact that funds can come from legal sources.

13. It is the responsibility of the insurer or intermediary to report any suspicious activity to the jurisdiction's Financial Intelligence Unit (FIU) if it suspects, or has reasonable grounds to suspect, that funds are the proceeds of criminal activity or are related to TF, rather than to determine the type of underlying criminal activity, or intended terrorist purpose. It is the role of the FIU to receive and analyse suspicious transaction reports (STRs)[6] and to disseminate, where appropriate, the results of their analysis to law enforcement authorities for further investigation. While the identification of potential suspicious transactions can be advanced by the RBA, reporting suspicious transactions, once identified, is mandatory and not risk-based.

14. PF is the provision of financial services for the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. Where particular individuals or organisations are the subject of TFS on TF or PF, the obligation on companies to comply with such TFS is not subject to a RBA. Violations of such sanctions may result in a criminal offence or regulatory sanctions if funds or financial services are made available to a target or its agent. Additionally, according to FATF Recommendation 1, insurers and intermediaries should identify and assess their "PF risk", referring strictly and only to the potential breach, non-implementation or evasion of TFS obligations, and take effective action to mitigate their PF risks on a risk-sensitive basis including screening of policyholders, beneficiaries and beneficial owners[7] on an ongoing basis.

2.2 Vulnerabilities in insurance

15. When assessing ML/TF risks, the focus of sector participants should be on the ability and likelihood of a money launderer or terrorist financier to use a particular financial product to store and move funds through the financial system for illicit purposes. Vulnerability depends on factors such as (but not limited to) the complexity and terms of the contract, distribution, method of payment (eg cash or bank transfer) and contract law. Generally, the ML/TF risk associated with the life insurance sector is lower than that associated with other financial products (eg loans and payment services) or other sectors (eg banking, gambling, precious stones and metal dealers). Indeed, many life insurance products are not sufficiently flexible to be the first vehicle of choice for money launderers. However, as with other financial services products, there is a risk that the funds used to purchase life insurance may be the proceeds of crime. There is also a potential risk that funds withdrawn from life insurance contracts could be used to fund terrorism.

[6] Some jurisdictions use the terminology "suspicious activities report".

[7] In this Application Paper, the term "beneficial owner" has the same meaning as defined under the FATF Glossary. Accordingly, "beneficial owner" refers to the natural person(s) who ultimately owns or controls a policyholder or beneficiary that is a legal person or arrangement and/or the natural person on whose behalf a transaction is being conducted.

16. ML/TF risks in the insurance industry may be found in life insurance and, albeit with generally an even lower risk compared to other life insurance products, annuity products. Such products allow a policyholder to place funds into the financial system and potentially disguise their criminal origin or finance illegal activities. Examples of life insurance products or product features that might be potentially at risk of being misused for ML/TF purposes (without prejudice to exposure to other ML/TF risk factors such as transaction, distribution, geographical or customer risk) include:

- Unit-linked or with profit single premium contracts;
- Single premium life insurance policies that store cash value;
- Endowment policies;
- Products with acceptance of very high value or unlimited value payments or large volumes of lower value payment;
- Acceptance of non-traceable payments such as cash, money orders, cashier cheques or virtual assets;[8]
- Acceptance of frequent payments outside a normal premium or payment schedule;
- Allowance of withdrawals at any time or early surrender, with limited charges or fees;
- Products that accept high amount lump sum payments, coupled with liquidity features;
- Products with provisions that allow a policy to be cancelled within a stipulated timeframe and the premiums paid to be refunded;
- Products that allow for assignment without the insurer being aware that the beneficiary of the contract has been changed until such time as a claim is made;
- Products with features or services that make it possible for customers to use the product in a way that is inconsistent with its purpose (for example, an insurance policy intended to provide long-term investment opportunity but that allows frequent or low fee deposit/withdrawal transactions);
- Customer is neither the payer nor recipient of the funds;
- Products with features that allow loans to be taken against the policy (particularly if frequent loans can be taken and/or repaid with cash);
- Acceptance to be used as collateral for a loan and/or written in a discretionary or other increased risk trust;
- Negotiability, for example, the product can be traded on a secondary market or used as collateral for a loan;
- Payment source or recipient of funds are outside of the jurisdiction (eg, insurer in jurisdiction A and payment source in jurisdiction B); and

[8] The FATF Glossary defines a virtual asset as a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes, and specifies that virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are covered elsewhere in the FATF Recommendations.

- Significant, unexpected or unexplained change in customer's pattern of payment, withdrawal or surrender.

17. When a life insurance policy matures or is surrendered, funds become available to the policyholder or other beneficiaries. The beneficiary to the contract may be changed before maturity or surrender, so that the payments are made by the insurer to a new beneficiary. A money launderer or terrorist financier may attempt to achieve their objective by nominating their conspirator as a beneficiary of a life insurance policy. According to FATF Recommendation 10, companies should take appropriate CDD measures, as soon as the beneficiary is named or designated, to enable the verification of the identity of the beneficiary of life insurance and other investment-related insurance policies at the time of the payout but before the funds are disbursed.

18. Also, a life insurance policy might be used as collateral to purchase other financial instruments. In such circumstances, insurers and intermediaries should request explanations and additional information as soon as they learn about this use.

19. Reinsurance is not included within the FATF Glossary's definition of "financial institutions" to which its standards apply. As described in the Guidance, as a matter of good practice, through their regular commercial due diligence, life reinsurers should seek to transact only with life insurers that have adequate AML/CFT programmes in place. The commercial due diligence process may include gathering information (including information from lead underwriters and reinsurance intermediaries, such as brokers) related to the ceding life insurers' AML/CFT programmes prior to entering into contracts. A reinsurer that suspects, or has reasonable grounds to suspect, that funds are proceeds of criminal activity or related to terrorist financing should use the STR process, when available, to advise the FIU. If such a process is not available, the reinsurer should advise an appropriate law enforcement authority.

20. Specific case examples of ML/TF are outlined in Annexes 1 and 2.

21. When assessing vulnerabilities in the life insurance sector to PF risks, insurers and intermediaries should ensure their understanding of their potential exposure to persons, entities or their agents designated under the relevant PF United Nations Security Council Resolutions (UNSCRs).

3 The risk-based approach

22. The FATF Recommendations require the adoption of a RBA to combating ML/TF. By adopting a RBA, supervisors, insurers and intermediaries are able to ensure that measures to prevent or mitigate ML/TF are commensurate with the risks identified. This will allow resources to be allocated in the most efficient way. A RBA should be applied also to identification, assessment and mitigation of PF risks, referring strictly and only to the potential breach, non-implementation or evasion of TFS obligations.

23. Adopting a RBA involves recognising the existence of ML/TF risk, undertaking an assessment of risk, understanding it and developing strategies, supported by appropriate resources, proportionate to the size and complexity of the business, to manage and mitigate the identified risks.

24. Insurers and intermediaries should develop ML/TF risk profiles for all their business relationships. To achieve this, they should identify and assess the risks associated with their

products (including services and transactions), geography (countries[9] or geographic areas), customers and delivery channels. In certain cases, business relationships may be assessed to be lower risk. All relevant risk factors should be considered in a holistic manner before determining the level of overall risk and the appropriate level and type of mitigation to be applied to each business relationship. Such risk assessments should be documented, as appropriate, and kept up to date. Risk assessments are not static. They will change over time, depending on how circumstances develop and how risks evolve.

25. Strategies to manage and mitigate the identified ML/TF risks in insurers and intermediaries are typically aimed at preventing the activity from occurring through a mixture of prevention (eg appropriate CDD measures), detection (eg monitoring and suspicious transaction reporting), and record-keeping so as to facilitate investigations by relevant authorities.

26. A RBA implies that appropriate policies, controls and procedures, approved by senior management, should be designed and implemented based on, and commensurate with, identified and assessed risk. These policies and procedures should be built on the strategic policies of the insurer's Board, including consideration of assessed risk profiles based on all appropriate risk factors. Higher risk business relationships and transactions should be subject to enhanced procedures and other measures, such as enhanced CDD checks and enhanced transaction monitoring. Similarly, in situations where risks are lower, simplified or reduced controls may be applied. The implementation of policies, procedures and controls should be monitored and enhanced by the insurer or intermediary as necessary.

4 Identification and assessment of risks

27. A RBA starts with the identification and assessment of the inherent ML/TF risks that have to be managed. This inherent risk assessment for a company should take into account the relevant attributes of the company's customers, countries or geographic areas, products and services, transactions and delivery channels. It should also be informed by any relevant findings of the national risk assessment. The company should then assess the effectiveness of its existing controls to manage these risks to arrive at a residual risk assessment. This exercise should be used to identify any appropriate actions necessary to enhance deficient controls so as to conform with the risk profile of the company.

28. Assessing inherent ML/TF risks in business activities involves:

- Analysing ML/TF risks in relation to customers, business relationships, countries or geographic areas, products (including services and transactions) and delivery channels, and whether or not the activities in which the risks arise are considered material in value;
- Assigning appropriate risk levels to, and ranking the relative seriousness of, the identified risks; and
- Highlighting the higher risks.

To appropriately assess inherent risks across the four key dimensions discussed hereunder, insurers and intermediaries may consider the characteristics described in paragraphs 29-32.

29. Customer-related risk refers to the risk that the insurer or intermediary is doing business with a customer that is not adequately identified or may be involved in ML/TF.

[9] While the ICPs refer to "jurisdictions", this application paper also uses "countries" for consistency with the FATF Recommendations, where appropriate.

Illustrative examples of inherent risk factors to consider from a customer perspective include the ease with which customers can be identified, the involvement of third parties, the source of the customer's wealth and funds, and whether a customer is a politically exposed person (PEP)[10] or a designated person with respect to TFS.

30. From a geographic perspective, the general consideration is whether a market's or customer's geographic location or connections will enhance vulnerability to ML/TF. This requires an initial exercise to determine a country's vulnerability against factors such as being identified in FATF statements as having a weak AML/CFT regime, being identified by credible sources as having significant levels of organised crime, corruption, or other criminal activity or being subject to sanctions, embargoes, or similar measures issued by international organisations (such as the United Nations). When assessing its geographic risk, a company should consider the geographic touchpoints of both its own operations and direct customers, as well as the role and positioning of any intermediaries it uses.

31. Product-related risk needs to consider both the design features of the company's products as well as the vulnerability of a product to abuse by a third party or to unintended use based on the methods of transactions available (ie, service and transaction-related risk). Design features of the product are important – for example, complex products with potentially multiple investment accounts and/or products with returns linked to the performance of an underlying financial asset (universal life, wrapper insurance) are at the high risk end of the spectrum. Conversely, products that pay a lump sum, or a regular payout or annuity, to the beneficiary in the event of the death of the insured (individual term life) are comparatively at the low risk end of the spectrum of insurance products. It is also important to recognise that certain characteristics of life insurance products may make them attractive to individuals seeking to hide income, commit tax fraud and evade tax or tax reporting requirements.

32. Delivery channel-related risk refers to the vulnerability of the delivery channel to ML/TF based on attributes that may make it easier to obscure customer identity or the source of funds. Illustrative examples include whether or not sales are conducted face-to-face, and how much the company relies on third party distributors or outsourcing. Consideration may also be given to whether payments are received via an intermediary that may obscure the source of payment.

[10] The FATF Glossary provides the following definitions of PEPs:

"*Foreign PEPs* are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.
Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories."

Local legislation may provide definitions of PEPs based on the FATF's definitions above. Insurers and intermediaries should apply definitions of PEPs provided in the legislation of jurisdictions in which they operate.

33. Insurers that use third party intermediaries to distribute their products should carefully and explicitly assess the potential risks posed by these intermediaries. For example, the size and sophistication of the intermediary may have a bearing on the sophistication of the intermediary's own AML/CFT programme. The jurisdiction in which the intermediary operates or is regulated should also be considered, as legislative and supervisory approaches differ. The insurer should also consider the role of the intermediary in handling customers' funds, both for premium and claims payments. All these factors may have a bearing on the insurer's own risk profile.

34. In the case of insurers or intermediaries that are part of a group, risk assessments of a subsidiary should take into account the group-wide risk appetite and framework, where relevant. Depending on the circumstance and local jurisdictional requirements, the parent company should perform a consolidated risk assessment for the entire group. Such risk assessment should take into account the geographic situations of each relevant insurance entity and, if any, the legal obstacles preventing foreign entities from applying AML/CFT group-wide procedures, including exchange of information within the group.

35. The results of the inherent risk assessment should be used as the basis for the assessment of the existence and effectiveness of the company's internal controls (policies and procedures) to arrive at the residual ML/TF risk of the company. In turn, this should inform the ongoing development or enhancement of the AML/CFT programme and the allocation of resources that are commensurate with levels of ML/TF risks in the various activities of the insurer or intermediary. Insurers and intermediaries should regularly refresh their assessment of inherent and residual ML/TF risks, to enable them to continuously tailor or amend control measures, as necessary, as their risk levels change and evolve over time.

36. The outcome of the insurer's or intermediary's risk assessment should be a rational, well-organised and well-documented analysis of inherent and residual risk within each risk category and in combinations of categories that arise in the activities of the insurer or intermediary. The outcome should be documented in such a way that it can be shared with a regulator.

37. The risk assessment methodology should itself be documented, and as with all documented policies and procedures, the insurer or intermediary should periodically review its risk assessment methodology and update it, as necessary.

38. According to FATF Recommendation 1, insurers and intermediaries should also identify, assess and take effective action to mitigate their PF risks. This risk assessment should be conducted in a similar manner to the ML/TF risk assessment described above. Mitigation measures must include being able to freeze the assets of persons covered under TFS related to proliferation and also ensuring that funds are not made available to such persons.

5 Customer risk assessment

39. As a key component of its operational controls to manage and mitigate the extent of its potential exposure to the risk of ML/TF, the insurer or intermediary needs to assess the risk of every customer relationship, both as part of its onboarding process and at appropriate times throughout the relationship. The outcome of the customer risk assessment is a customer risk rating. Factors that will need to be considered include, but are not limited to, the identity of the customer and any beneficial owner, the customer's residence including, where appropriate, tax residency, citizenship, place of incorporation or place of business, and the nature of the business relationship.

40. The insurer and intermediary will need to carefully assess all relevant information concerning the customer and their proposed or ongoing business relationship in order to assign them the correct risk rating. To achieve this, the insurer or intermediary will have to collect and/or refresh a range of relevant information[11], and establish a consistent framework for using the information to determine a customer risk rating. Based on the risk rating, the insurer or intermediary can then apply a RBA to decide whether or not to accept or continue (if legally permissible) the business relationship and to determine the appropriate current level of CDD measures and risk mitigation to be applied to the relationship.

41. The sophistication of the customer risk assessment framework should be proportionate to the size and complexity of the business, considering all the key factors of its targeted customers, products, delivery channels and geographic exposure. This means that a simple risk assessment framework might be enough for smaller or less complex insurers or intermediaries, and that where insurers or intermediaries are part of a group, risk assessments should take into account the group-wide risk appetite and framework.

42. Conceptually, the customer risk rating will drive whether the standard CDD measures should be applied to the customer, or whether enhanced measures are recommended due to a higher customer risk rating. There is also the potential of applying simplified CDD measures for customers whose risk rating is determined to be appropriately low.

43. There are many factors that could be considered when creating a customer risk-rating framework. These are comprised of both customer-specific risk factors and business risk factors. Of particular importance to insurers and intermediaries is that the beneficiary of a life insurance policy should be included as a relevant risk factor in determining whether enhanced CDD measures are applicable. A non-exhaustive list, in no particular order of priority, includes:

- Type and background of customer and/or beneficial owner and beneficiaries (are they considered a PEP; are they designated on a sanctions list or do they have known ties to a designated person);
- Relationship between customers and beneficiaries;
- The customer's and/or beneficial owner's and beneficiaries' geographical nexus;
- The geographical nexus of the activities of the customer and/or beneficial owner and beneficiary;
- The nature of the proposed or observed activities in the account;
- The means of payment as well as the type of payment (cash, wire transfer, other);
- The source of funds;
- The source of wealth;
- The frequency and scale of activity;
- The type and complexity of the business relationship;
- Whether or not payments will be made to or received from third parties;
- Whether a business relationship is dormant;
- Any bearer arrangements;

[11] Subject to relevant data protection laws.

- Structure of a legal entity that a customer, policyholder or beneficiary obscures or makes it difficult to identify the ultimate beneficial owner or controlling interests;
- Customer is reluctant to provide identification, exhibits difficulty producing identification, or provides identification documents of questionable authenticity;
- Involvement of a gatekeeper or a third party apparently unrelated to the customer;
- Higher risk business or occupation (such as those that are cash-intensive);
- Mismatch between wealth and income of the customer and proposed premium amounts, deposit amounts or policy limits;
- Customer is associated with negative news which may affiliate the customer with allegations of criminal behaviour; and
- Suspicion or knowledge of ML/TF or other crime.

See also paragraphs 76-77 for higher risk cases where enhanced CDD measures could be applied, and paragraphs 82-85 for lower risk cases where simplified CDD measures could be applied.

44. A customer risk assessment should be conducted at onboarding, on an ongoing basis defined within the framework as a function of the current customer risk rating and whenever an event which could materially affect the risk of the customer relationship ("trigger event") occurs.

6 Overview of customer due diligence

45. Insurers and intermediaries should undertake risk-based CDD measures driven by the customer risk assessment output, including verification of the identity of the customer and beneficial owner:

- When establishing business relationships;
- When there is a suspicion of ML/TF;
- When the insurer or intermediary has doubts about the veracity or adequacy of previously obtained customer identification data; or
- On existing relationships at appropriate times.

46. A first step in setting up a system of CDD is to develop clear, written and risk-based customer acceptance policies and procedures based on inherent and customer risk assessment results. They should prohibit the issuance of insurance policies to customers whose identities cannot be confirmed and, where relevant, the use of anonymous accounts or accounts in fictitious names. Identification and subsequent verification will also prevent anonymity of policyholders, beneficiaries and beneficial owners, and the use of fictitious names.

47. Insurers and intermediaries should identify and freeze without delay the assets of, and otherwise not deal with, any designated entities (eg terrorists, terrorist organisations, entities associated with PF) consistent with their national legislation and the relevant UNSCRs.

48. CDD measures taken by insurers and intermediaries should include:

(a) Identifying the customer (natural and legal persons and legal arrangements) and verifying that customer's identity using reliable, independent source documents, data or information ("identification data");

(b) Identifying the (ultimate) beneficial owner and taking reasonable measures to verify the identity of the beneficial owner such that the insurer or intermediary is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements, this should include understanding by insurers and intermediaries of the ownership and control structure of the customer;

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship and other relevant factors such as those in paragraph 43; and

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship, to ensure that the transactions being conducted are consistent with the insurer's knowledge of the customer and/or beneficial owner, their business and risk profile including, where necessary, the source of funds.

When performing elements (a) and (b), insurers and intermediaries should also verify that any person purporting to act on behalf of the customer and/or beneficial owner is authorised to do so and identifying and verifying the identity of that person using the identification data described in (a).

49. In addition to the CDD measures required for the customer and the beneficial owner, insurers and intermediaries should conduct the following CDD measures on the beneficiaries of life insurance and other investment-related insurance policies as soon as the beneficiaries are identified/designated:

(a) For beneficiaries that are identified as specifically named natural or legal persons or legal arrangements – taking the name of the person;

(b) For beneficiaries that are designated by characteristics or by class (eg spouse or children at the time that the insured event occurs) or by other means (eg under a will) – obtaining sufficient information concerning the beneficiary to satisfy the insurer or intermediary that it will be able to establish the identity of the beneficiary at the time of the payout; and

(c) Such due diligence with respect to a beneficiary who is a legal person or arrangement should include identification of the (ultimate) beneficial owner of the beneficiary.

Verification of the identity of the beneficiary should occur at the time of the payout and before the funds are disbursed, based on the information previously gathered under (a) and (b), which should be recorded and maintained in accordance with the record keeping provisions (see paragraphs 144-147). After verifying the identity of the beneficiary, insurers and intermediaries should take additional measures, depending on their assessment of ML/TF risks with respect to the beneficiary, for example, if the beneficiary is a PEP (see paragraph 97).

50. As noted above under "Customer risk assessment", the beneficiary of a life insurance policy should be included as a relevant risk factor by the insurer or intermediary in determining whether enhanced CDD measures are applicable. If the insurer or intermediary determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, then the enhanced CDD measures should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

51. Where an insurer or intermediary is unable to comply with paragraphs 45-47 above:

- It should not open the account, commence business relations or, if consistent with law, should not perform the transaction or should terminate the business relationship; and
- It should also consider making a STR.

7 New customers

7.1 Methods of identification and verification

52. This section does not seek to specify what, in any particular case, may or may not be sufficient evidence to complete verification. It does set out what, as a matter of good practice, may reasonably be expected of insurers and intermediaries in either face-to-face or non-face-to-face interactions. There may be cases where an insurer or intermediary has properly satisfied itself that verification has been achieved by other means, which it can justify to the appropriate authorities as reasonable in the circumstances. This will apply whether the verification is done by the insurer or intermediary, or by a third party on which reliance is being placed (see "Reliance on third parties" section below).

53. Reliable and independent identification data should be obtained from each verification subject. "Reliable and independent" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

54. It is important to note that the implementation of FATF Recommendations is technology neutral. Given the significant recent advances in digital ID technology, architecture, processes and the emergence of consensus-based open-source digital ID technical standards, insurers and intermediaries may consider the adoption of independent digital ID systems. FATF has issued guidance on the use of Digital Identity (Digital ID) ("FATF Guidance on Digital ID"). Insurers and intermediaries should adopt an informed, risk-based approach towards such technologies. Examples of considerations include:

- Understanding the digital ID system's assurance levels, particularly for identity proofing and authentication;
- Ensuring that the assurance levels are appropriate for the ML/TF risks associated with the customer, product, jurisdiction, geographic reach, etc; and
- Ensuring that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals.

7.1.1 Individuals

55. The personal information used to identify the customer may include:

- Full name(s) and alias;
- Date and place of birth;
- Citizenship;

- Current permanent address[12] including postcode/zipcode; and
- Specimen signature or digital signature of the individual.

56. On a risk-sensitive basis, the insurer or intermediary may also collect the following information to complete its customer risk assessment:

- Occupation and name of employer/source of income;
- Details concerning any public or high-profile positions held; and
- Country(ies) of tax residency.

57. It is recognised that different jurisdictions have different identification documents. In order to verify identity, it is suggested that the following documents may be considered to be most reliable:

- Valid passport;
- National identity card; or
- Other government-issued identification document containing a recent photograph.

58. However, some jurisdictions do not have national identity cards and many individuals do not possess passports. Some jurisdictions establish criteria for acceptable verification documents, taking into account local conditions. Identity should always be verified using reliable, independent source documents, data or information.

7.1.2 Legal persons, companies, partnerships, other institutions and arrangements

59. When performing CDD measures in relation to customers or beneficiaries that are legal persons or legal arrangements, the insurer or intermediary should identify and verify the customer or beneficiary, and understand the nature of its business, and its ownership and control structure.

60. The insurer or intermediary should:

(a) Identify the customer or beneficiary and verify its identity – the types of measures that would normally be needed to perform this function satisfactorily would require obtaining and verifying the following information:

- Name, legal form and proof of existence – for example through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable, independent source proving the name, form, unique identifier (if available) and current existence of the customer;
- The powers that regulate and bind the legal person or arrangement (eg the memorandum and articles of association of a company as well as the names of the relevant persons having a senior management position in the legal person or arrangement (see also paragraph 55)); and
- The address of the registered office and main place of business.

(b) Identify the beneficial owners of the customer or beneficiary and take reasonable measures to verify the identity of such persons through the following information:

[12] In this context “current permanent address” means the verification subject’s actual residential address, as it is an essential part of identity.

- For legal persons:
  - (i) The identity of the natural persons (if any – as ownership interests can be so diversified that there are no natural persons (whether acting alone or together) exercising control of the legal person or arrangement through ownership), who ultimately have a controlling ownership interest in a legal person;
  - (ii) To the extent that there is doubt under (i) as to whether the person(s) with the controlling ownership[13] interest are the beneficial owner(s) or where no natural person exerts control through ownership interests, the identity of the natural persons (if any) exercising control of the legal person or arrangement through other means; and
  - (iii) Where no natural person is identified under (i) or (ii) above, insurers and intermediaries should identify and take reasonable measures to verify the identity of the relevant natural person who holds the position of senior managing official.
- For legal arrangements:
  - (i) That are trusts: the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries/class of beneficiaries and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership); and
  - (ii) That are other types of legal arrangements: the identity of persons in equivalent or similar positions.

61. Where the customer or the owner of the controlling interest is a company listed on a stock exchange and is subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of that company. The relevant information or data may be obtained from a public register, from the customer or from other reliable sources. This provision could also apply to mutual insurance companies and fraternal benefit societies that are subject to similarly rigorous levels of regulatory oversight as insurers listed on a stock exchange.

62. When dealing with the identification and verification of companies, trusts and other legal entities, the insurer should be aware of vehicles, corporate or otherwise, that are known to be at higher risk of misuse for illicit purposes. Such information should be available from the country's national risk assessment of ML/TF risks presented by the different types of legal persons created in the country.

63. Sufficient verification should be undertaken to ensure that the individuals purporting to act on behalf of an entity are authorised to do so.

64. In all transactions undertaken on behalf of an employer-sponsored pension or savings scheme, the insurer or intermediary should, at a minimum, undertake verification of the

[13] The FATF Methodology describes controlling ownership as follows "A controlling ownership interest depends on the ownership structure of the company. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25%)."

principal employer and trustees (if any) of the scheme. Verification of the principal employer should be conducted in accordance with the procedures for verification of institutional applicants for business. Verification of any trustees of the scheme will generally consist of an inspection of the relevant documentation, which may include:

- The trust deed and/or instrument and any supplementary documentation;
- A memorandum of the names and addresses of current trustees (if any);
- Extracts from public registers; and
- References from professional advisers or investment managers.

65. As legal controls vary between jurisdictions, particular attention may need to be given to the place of origin of such documentation and the background against which it is produced.

66. Insurers and intermediaries should maintain their records with respect to their CDD on legal persons and legal arrangements in such a way as to enable competent authorities to access, in a timely fashion, adequate, accurate and current information on the beneficial ownership and control of legal persons and legal arrangements and, in particular the settlor, the trustee and the beneficiaries of express trusts.

7.2 Timing of identification and verification

67. According to FATF Recommendation 10, insurers and intermediaries should undertake CDD measures before or during the course of establishing a business relationship. More specifically, insurers are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship. This means that (the owner/controller of) the policyholder needs to be identified and their identity verified before, or at the moment when, the insurance contact is concluded. Valid exceptions are mentioned in the following paragraphs.

68. Where a policyholder and/or beneficiary is permitted to utilise the business relationship prior to verification, insurers and intermediaries should adopt risk management procedures concerning the conditions under which this may occur. These procedures should include measures such as a contractual limitation on the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship.

69. FATF Recommendation 10 recognises that identification and verification of the identity of the customer and beneficial owner may (if permitted) take place after the establishment of the business relationship provided that:

- This occurs as soon as reasonably practicable;
- It is essential not to interrupt the normal conduct of business; and
- The ML/TF risks are effectively managed.

70. Where the insurer or intermediary has already commenced the business relationship and is unable to comply with the verification requirements, according to FATF Recommendation 10, it should not conduct further transactions or should terminate the business relationship (if legally permissible) and consider making a STR. An insurer or intermediary that has not commenced business relations or has not performed a transaction, and is unable to comply with the verification requirements, should not commence business relations or should not perform the transaction and should consider making a STR.

71. Examples of situations where a business relationship could be used prior to verification are:

- Group pension schemes;
- Non-face-to-face customers (such as those using internet, telemarketing, or other electronic means of communication);
- Premium payment made before the application has been processed and the risk accepted; and
- Using a policy as collateral.

72. Measures to restrict the services available and prohibit any further transactions on the contracts in question could be considered as a preferred alternative. For example, where permitted, a contract could be "frozen" and the payment would only be made to the beneficiary once full and proper CDD measures have been successfully conducted.

7.3 Initial screening of and risk rating of customers

73. Once the identity of customers, beneficiaries and beneficial owners with respect to the insurance contract has been established, the insurer or intermediary should conduct due diligence on a risk-sensitive basis by referencing the standard information gathered from the counterparty together with other relevant available information, according to their customer risk assessment framework. Screening customers, beneficiaries and beneficial owners against internal and external publicly available information may uncover that they are or have associations with known fraudsters or money launderers (possibly available from industry databases), PEPs, or designated persons or entities listed on applicable sanctions lists (such as those published by the United Nations).

74. Insurers and intermediaries should use appropriate available sources of information when considering whether or not to accept the ML/TF risk associated with the contract, bearing in mind that compliance with TFS related to TF and PF is not subject to the RBA.

8 Enhanced customer due diligence in higher risk cases

8.1 Enhanced customer due diligence measures

75. According to FATF Recommendation 10, insurers and intermediaries should conduct enhanced CDD measures, consistent with the risks identified with respect to all higher risk categories of products (including services and transactions), geography, customers and delivery channels.

Examples of enhanced CDD measures that could be applied for higher-risk business relationships include:

- Obtaining additional information on the customer (eg occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the customer;
- Obtaining information on the reasons for intended or performed transactions;

- Obtaining senior management approval to commence or continue the business relationship;
- Conducting enhanced ongoing monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination; and
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

8.2 Higher risk cases

76. Examples of situations where customer or business relationship risk could be higher include the following:

- The business relationship is conducted in unusual circumstances (eg significant unexplained geographic distance between the insurer or intermediary and the customer);
- The business is cash intensive;
- Customers are non-residents;
- Legal persons or arrangements that are personal asset holding vehicles;
- Companies have nominee shareholders or shares in bearer form; and
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

77. Examples of situations where the product, service, transaction or delivery channel risk factors could be higher include:

- Large cash or other forms of anonymous transactions;
- Non-face-to-face business relationships or transactions (ie the carrying out of an insurance contract, without the simultaneous physical presence of the insurer or intermediary and the consumer, by making exclusive use of one or more of the internet, telemarketing, or other electronic means of communication up to and including the time at which the contract is concluded) without adequate safeguards for confirmation of identification or to mitigate the risks of identity fraud (see also Paragraph 78);
- Payments received from unknown or un-associated third parties;
- Where there is a change of beneficiary in a life policy, after the establishment of the business relationship, particularly in the case of a third party beneficiary, when it would be difficult to establish the link with the policyholder. In some cases, the third party may not even be aware of the existence of the policy that it is entitled to benefit from. Those situations involving third parties can be considered as presenting high risk in particular if the beneficiary is a legal person or arrangement, or a category or class of persons;
- Where the insurer or the intermediary may also have difficulty in identifying the person on whose behalf the business relationship or transaction is being conducted (eg policyholder different from the insured person and beneficiary and with no apparent relationship to them, or third party payer on the contract with no apparent relationship with the policyholder);

- Viatical arrangements: Where a policyholder becomes seriously or terminally ill, they may decide to transfer the entitlement to the benefits of a life insurance policy after their death to a third party in order to receive funds before their death. In some jurisdictions, there are "viatical" companies that purchase and sell these entitlements. In these cases, similar risks exist as described under "bearer policies". In light of the inherent risks, where viatical arrangements are allowed in a jurisdiction, supervisory overview or regulation is strongly recommended. An insurer that needs to pay funds to a viatical company should perform enhanced CDD as specified above including the identification and verification of the viatical company and its beneficial owners;
- Bearer policies: Bearer policies are insurance contracts that require the insurer to pay funds to the person(s) holding the policy document or to whom the entitlement to the benefit(s) is endorsed without needing to seek the consent of the insurer. This type of policy does not exist in every jurisdiction but, where it does, it could serve as a financial instrument that can easily be transferred from person to person without the endorsees being identified. Identification and verification by the insurer would only occur at the policy's maturity when the benefits are being claimed. From the point of view of AML and CFT, the use of bearer policies is strongly discouraged, not least because of the importance of performing enhanced CDD combined with the inherent uncertainties in being able to undertake CDD on the beneficiaries; and
- Insurers and intermediaries should have measures in place to deal with high risk situations (ie as presented by high risk products such as bearer policies and instruments). The FATF states in Recommendation 24 that measures should be taken as regards products favouring anonymity such as bearer shares and warrants, by prohibiting them or immobilizing them in a registry held by a regulated entity, or requiring shareholders to notify the company and the company to register them. In that regard, insurers and intermediaries should have a mechanism in place to identify the beneficial owner of bearer policies and should take appropriate measures as prescribed by their regulation. At a minimum, they should consider the business relationship involving such products as presenting high risk and apply enhanced CDD measures commensurate to that risk.

78. With respect to non-face-to-face business relationships or transactions indicated in the preceding paragraph, the FATF Guidance on Digital ID acknowledges that non-face-to-face customer identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place may present a standard level of risk, and may even be lower-risk. In assessing the risk that a particular non-face-to-face transaction poses, insurers and intermediaries should give consideration to what digital ID systems (if any) are employed for the transaction.

8.3 Higher risk countries

79. According to FATF Recommendation 10, insurers and intermediaries should apply enhanced CDD to business relationships and transactions with natural persons, legal persons and arrangements, and financial institutions from countries for which this is called for by the

FATF.[14] The type of enhanced CDD measures applied should be effective and proportionate to the risks.

80. In specific circumstances, countries may be asked by the FATF to impose appropriate countermeasures. Countries may also apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks. In this regard, insurers and intermediaries should have put in place effective measures to be informed when countries pose high/higher risks, such as:

- Countries identified by credible sources such as mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems;
- Countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity; and
- Countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organizations operating within them.

9 Simplified customer due diligence in lower risk cases

81. According to FATF Recommendation 10, insurers and intermediaries should normally apply the full range of CDD measures to the customer, including the requirement to identify the beneficiary, when establishing the business relationship. However, if the risk of ML or TF is lower (based on an adequate analysis of the risks by the insurer or intermediary, or by the country) it could be reasonable for insurers and intermediaries to apply, subject to national legislation and guidelines, simplified CDD measures when entering into business relationship or when the product is issued.

82. Examples of where the customer risk factor could be lower are:

- Financial institutions and designated non-financial business and professions (DNFBPs) – where they are subject to requirements to combat ML/TF consistent with the FATF Recommendations, and are effectively supervised or monitored in

[14] For instance, jurisdictions may be publicly identified in one of the two FATF public documents that are issued three times a year.

The first public document, the *FATF's Public Statement*, identifies:

1) jurisdictions that have strategic AML/CFT deficiencies and to which counter-measures apply.

2) jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies.

In the second FATF public document, *Improving Global AML/CFT Compliance: On-going Process*, the FATF identifies jurisdictions with strategic AML/CFT deficiencies that have provided a high-level political commitment to address the deficiencies through implementation of an action plan developed with the FATF.

More information can be obtained from the FATF website: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/

accordance with the FATF Recommendations to ensure compliance with those requirements;

- Public companies listed on a stock exchange and subject to regulatory disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company; and
- Public administrations or enterprises.

83. Examples of circumstances where the product, service, transaction or delivery channel risk factor could be lower are:

- Products that only pay out at death and/or in the event of disability as long as the beneficiary does not change;
- Transactions involving low amounts, such as life insurance policies where the annual premium is less than USD/€ 1000 or a single premium of less than USD/€ 2500;
- Insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;
- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme (eg small insurance premiums); and
- Financial products or services that provide appropriately defined and limited services to certain types of customers to increase access for financial inclusion purposes.

84. Examples of situations where the country risk factor could be lower are where:

- Countries are identified by credible sources such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and
- Countries are identified by credible sources as having a low level of corruption or other criminal activity.

85. In making a risk assessment, insurers and intermediaries could, when appropriate, also take into account possible variations in ML/TF risk between different regions or areas within a country.

86. The simplified CDD measures should be commensurate with the lower risk factors. This does not, however, automatically mean that the same customer is lower risk for all types of CDD measures (eg the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (eg if account transactions rise above a defined monetary threshold);[15]

[15] In the context of facilitating financial inclusion, it is important to support progressively or concurrently, improved access to the larger range of needed financial services, including tailored life insurance products. The FATF's "Guidance on AML/CFT measures and financial inclusion" highlights that financial inclusion objectives have led a number of countries to design a so-called "progressive" or "tiered" CDD

- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinising transactions based on a reasonable monetary threshold; and
- Not collecting specific information or not carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

87. However, FATF Recommendation 10 provides that:

- Simplified CDD measures are not acceptable in any event when there is a suspicion of ML or TF or when specific higher risk scenarios apply; and
- The extent of risk sensitive CDD measures taken by insurers and intermediaries should also be consistent with national legislation and guidelines issued by the competent authorities.

10 Ongoing due diligence and monitoring

88. According to FATF Recommendation 10, the insurer or intermediary should perform ongoing due diligence on the business relationship. Ongoing due diligence should include scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile category and, where necessary, the source of funds. There should also be systems to detect prohibited (eg with entities designated by the relevant UNSCRs), unusual or suspicious transactions, and investigate them as required. The insurer or intermediary should pay attention to all requested changes to the policy and/or exercise of rights under the terms of the contract. It should assess whether the change/transaction fits the risk profile category of the customer and/or beneficial owner or is for some other reason unusual or suspicious.

89. Examples of transactions or trigger events after establishment of the contract that require CDD review are:

- A change in beneficiaries (for instance, to include non-family members or a request for payments to be made to persons other than beneficiaries);
- A change/increase of insured capital and/or of the premium payment (for instance, which appear unusual in light of the policyholder's income or where there are several overpayments of policy premiums after which the policyholder requests that reimbursement is paid to a third party);
- Use of cash and/or payment of large single premiums;
- Payment/surrender by wire transfer from/to foreign parties;
- Payment by banking instruments which allow anonymity of the transaction;
- Change of address and/or place of residence of the policyholder, in particular, tax residence;

approach. Through this approach, customers are allowed to access the basic first level set of services upon minimum identification, and to access the subsequent account levels and additional services only if/when the customer provides the required additional identification/verification.

- Lump sum top-ups to an existing life insurance contract;
- Lump sum contributions to personal pension contracts;
- Requests for prepayment of benefits;
- Use of the policy as collateral/security (for instance, unusual use of the policy as collateral unless it is clear that it is required for financing of a mortgage by a reputable financial institution);
- Change in the type of benefit (for instance, change in type of payment from an annuity to a lump sum payment);
- Early surrender of the policy or change in duration (where this causes penalties or loss of tax relief); and
- Request for payment of benefits at the maturity date if suspicious circumstances are present.

90. The above list is not exhaustive – insurers and intermediaries should consider other types of transactions or trigger events which are appropriate to their type of business. It should also be noted that some of the above events can be expected over the life of a contract and are not necessarily suspicious.

91. Occurrence of these transactions and events does not imply that (full) CDD needs to be applied. If identification and verification have already been performed, the insurer or intermediary is entitled to rely on this unless doubts arise about the veracity of the information collected. As an example, doubts might arise if benefits from one policy of insurance are used to fund the premium payments of another policy of insurance or where there is a suspicion of ML or TF in relation to that customer.

92. The CDD programme should be established in such a way that the insurer or intermediary is able to adequately gather and analyse information. According to FATF Recommendation 10, insurers and intermediaries should ensure that documents, data or information gathered under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers or business relationships.

93. Insurers and intermediaries could consider using automated tools to monitor transactions and to help them improve their ability to mitigate ML/TF risks. In order to achieve that monitoring they could, for example, define adequate thresholds or scenarios to filter out unusual transactions regarding the risk profile of a given customer. These thresholds, or scenarios, may change over time based on various factors such as specific experience with a customer or new typologies.

94. Insurers and intermediaries should also ensure that existing customers are regularly screened on a risk-sensitive basis against TFS lists in order to detect any persons or entities that are in existing business relationships and whose listing status has changed since the last screening, and to take appropriate actions in such cases.

11 Politically exposed persons

95. FATF Recommendation 12 requires enhanced CDD measures to be taken in relation to foreign PEPs. For this purpose, insurers and intermediaries should:

(a) Have in place appropriate risk management systems to determine whether a potential customer, a customer or the beneficial owner of a customer is a foreign PEP;

(b) Obtain senior management approval for establishing (or continuing for existing customers) such business relationships;

(c) Take reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as PEPs; and

(d) Conduct enhanced ongoing monitoring of the business relationship.

96. According to FATF Recommendation 12, insurers and intermediaries should also take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. In cases of a higher risk business relationship with a domestic PEP, insurers and intermediaries should apply the measures referred to in (b), (c) and (d) in paragraph 95.

97. In addition, according to FATF Recommendation 12, insurers and intermediaries should take reasonable measures to determine whether the beneficiary of a life insurance policy (and/or where required, the beneficial owner of the beneficiary) is a PEP. This should occur at the latest at the time of the payout. In addition to performing normal CDD measures, where higher risks are identified, insurers and intermediaries should:

- Inform senior management before the payout of the policy proceeds; and
- Conduct enhanced scrutiny on the whole business relationship with the policyholder and consider making a STR.

98. The requirements for all types of PEP also apply to family members or close associates of such PEPs.

99. Insurers and intermediaries may use a number of ways to assist with the identification of PEPs. These could include using internet and media searches, commercial databases, PEP lists from government authorities (if available), in-house databases, asset disclosure systems, customer self-declarations, etc. Regardless of the means used to identify PEPs, insurers and intermediaries should adopt commensurate measures, and be satisfied that they have taken adequate steps to comply with the relevant CDD requirements.

12 New or developing technologies and products[16]

100. According to FATF Recommendation 15, insurers and intermediaries should identify and assess the ML/TF risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. Insurers and intermediaries should undertake this assessment prior to the launch of the product, practice or technology, and should take appropriate measures to manage and mitigate the risks identified.

101. New or developing technologies can be used to market insurance products or facilitate the CDD process. E-commerce or using digital ID to support sales over the internet are examples of this. Insurers and intermediaries that use new and developing technologies should include these in the inherent risk assessment process to ensure that appropriate

[16] The identification and the assessment of product risk should be done periodically and when significant changes are made to product offerings (including the development of new products/services).

AML/CFT controls are implemented and maintained around them. Paragraph 54 provides general guidance for the adoption of independent digital ID systems, including examples of considerations that insurers and intermediaries could take into account when assessing the adoption of such systems. Insurers that accept premiums or pay claims in virtual assets should carefully assess and mitigate any potential ML/TF risks associated with those and consider the latest guidance from the FATF and relevant local laws.

13 Reliance on third parties[17]

102. Depending on the legislation of the jurisdiction in which the insurer operates, it may be allowed to rely on third parties to perform elements (a) to (c) of the CDD measures set out in paragraph 48.

103. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the insurer relying on the third party.

104. Where such reliance, or reliance for the purpose of introducing business, is permitted, FATF Recommendation 17 requires that the following criteria be met:

(a) Insurers relying on a third party immediately obtain from the third party the necessary information concerning elements (a) to (c) of the CDD measures set out in paragraph 48;

(b) Insurers take adequate steps to satisfy themselves 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; and

(c) Insurers satisfy themselves that the third party is regulated, supervised or monitored for and has measures in place for compliance with CDD and record-keeping requirements in line with FATF Recommendations 10 (customer due diligence) and 11 (record keeping).

105. FATF Recommendation 17 requires that reliance on a third party take into consideration the information available (eg whether the FATF has called for enhanced CDD measures or countermeasures to be applied) on the level of country or geographical risk of the jurisdiction in which the third party is based. Insurers and intermediaries should likewise consider information about these risks and, where appropriate, restrict the use of such third parties.

106. The FATF has also crafted similar provisions regarding financial groups. According to FATF Recommendation 17, where an insurer relies on a third party that is part of the same financial group, and where the following conditions are met, then the criteria of paragraph 104 (a) to (c) above could be considered met through its group programme:

- The group applies CDD and record-keeping requirements, in line with Recommendations 10 (customer due diligence), 11 (record keeping) and 12 (politically exposed persons), and programmes against ML/TF, in accordance with Recommendation 18 (internal controls and foreign branches and subsidiaries);

[17] The following paragraphs 102-109 do not apply to outsourcing or agency relationships other than relationships with insurance agents and brokers, ie they do not apply where the agent is acting under a contractual arrangement with the insurer to carry out its CDD functions.

- The implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority; and
- Any higher country risk is adequately mitigated by the group's AML/CFT policies.

107. The checks by the insurer do not have to consist of a check of every individual transaction by the intermediary or other third party; however, the insurer should be satisfied that AML/CFT measures are implemented, are operating adequately, are at least equivalent to their own legal and regulatory requirements, and comply with the CDD and record keeping requirements of FATF Recommendations 10 and 11.

108. Insurers should satisfy the above provisions by way of contractual agreement or other documentation with third parties, and by enforcement of the terms. Specific clauses should include commitments by third parties regarding performance of the necessary CDD measures, complete and up-to-date record keeping, granting access to customer files and sending (copies of) files to the insurer upon request within required timeframes and without delay. The agreement could also include other commitments, such as reporting to the FIU and the insurer in the case of a suspicious transaction or attempted suspicious transaction. It is recommended that insurers use application forms to be filled out by customers and third parties that include information on the identification of the customer and the beneficial owner(s), and on third party and PEP determination, as applicable, as well as the method(s) used to verify identity. Insurers should periodically review, in a systematic manner, the quality of customer information gathered and documented, to ensure their requirements continue to be met.

109. If the insurer has any doubts about the ability of the intermediary or other third party to undertake appropriate due diligence, or about the performance of due diligence responsibilities, it should undertake and complete its own CDD, including verification of identities and other collected information. Insurers should consider terminating relationships with intermediaries and other third parties that do not comply with agreed upon responsibilities or do not provide the requisite information to the insurer in a timely fashion.

110. The extent of the insurer's exposure to the third party should be addressed expressly in the insurer's inherent risk assessment.

111. Consideration should be given to the measures to be taken when insurers outsource part of their AML/CFT function to a third party that is neither regulated nor supervised for AML/CFT. In such case, insurers should include these third parties in their own internal AML/CFT control processes, and monitor their AML/CFT programmes. The insurer remains ultimately responsible for AML/CFT controls in such an outsourcing agreement and should monitor the effective implementation of its various procedures surrounding the application of CDD measures, as well as compliance of the outsourced entity with these procedures.

14 Suspicious transaction reporting

112. According to FATF Recommendation 20, if an insurer or intermediary suspects, or has reasonable grounds to suspect, that funds are the proceeds of a criminal activity, or are related to TF, it should report its suspicions promptly to the FIU by means of a STR. All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction. Insurers and intermediaries should also take note of other reporting obligations in their jurisdiction, including those relating to assets frozen or actions taken in compliance with the prohibition requirements of the relevant UNSCRs.

113. When relying on the identification and verification work completed by insurance intermediaries, insurers should ensure that they will receive a copy of the relevant CDD record(s) without delay upon request, in order to facilitate the filing of STRs.

114. An important pre-condition of recognition of a suspicious transaction is for the insurer or intermediary to know enough about the customer and business relationship to recognise that a transaction, or a series of transactions, is unusual. This is facilitated through ongoing CDD and monitoring processes.

115. Suspicious transactions might fall into one or more of the following non-exhaustive examples of categories:

- Any unusual financial activity of the customer in the context of their usual activities;
- Any unusual transaction in the course of some usual financial activity;
- Any unusually linked transactions;
- Any unusual or apparently disadvantageous early redemption of an insurance policy;
- Any unusual employment of an intermediary in the course of some usual transaction or financial activity (eg payment of claims or high commission to an unusual intermediary);
- Any unusual method of payment; and
- Any involvement of any person subject to international sanctions.

116. Verification at the commencement of a business relationship, once begun, should be pursued either to a conclusion or to the point of refusal. If a prospective policyholder does not pursue an application, this may be considered suspicious.

117. FATF Recommendation 21 provides that insurers and intermediaries, their directors, officers and employees (permanent and temporary) should not disclose the fact that a STR is being made or related information is being reported, or has been reported, to the FIU. A risk exists that customers could be unintentionally tipped off when the insurer or intermediary is seeking to perform its CDD obligations in these circumstances. The customer's awareness of a possible STR or investigation could compromise future efforts to investigate the suspect ML/TF operation.

118. Therefore, if insurers and intermediaries form a suspicion that transactions relate to ML or TF, they should take into account the risk of tipping-off when performing the CDD process. If the insurer or intermediary reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file a STR. Insurers and intermediaries should ensure that their employees are aware of, and sensitive to, these issues when conducting the CDD process.

15 Internal controls and foreign branches and subsidiaries

119. According to FATF Recommendation 18, insurers and intermediaries should have in place and implement programmes and systems to prevent ML/TF.

120. FATF Recommendation 18 requires these programmes to include internal policies, procedures and controls linked to the risk of ML/TF and the size of the business, and which cover:

- Appropriate compliance management arrangements, including the appointment of an AML/CFT compliance officer[18] at the management level;
- Adequate screening procedures to ensure high standards when hiring employees;
- An ongoing employee training programme, highlighting employees' responsibilities with respect to AMLT/CFT; and
- An (external or internal) independent audit function to test the AML/CFT system.

121. The training programme could include information on new developments; information on current ML/TF techniques, methods and trends, and a clear explanation of all aspects of AML/CFT laws and obligations and, in particular, requirements concerning CDD and suspicious transaction reporting. Internal audit could include sample testing.

122. Internal policies, procedures and controls could usefully cover all aspects of AML/CFT programmes of insurers and intermediaries, such as:

- CDD;
- Detection of unusual or suspicious transactions and reporting obligations;
- Record keeping and record retention arrangements; and
- Communication of policies, procedures and controls to employees.

123. Each programme and system should:

- Be sufficiently robust to handle the volume of information processed by that insurer or intermediary effectively and efficiently;
- Constitute an operational, practical and precise approach for dealing with ML/TF risks; and
- Be adapted to the group, its organisational (eg joint back office) and responsibility structures, and to products and market conditions.

The development of policies, procedures and controls enables the insurer or intermediary to comply with their AML/CFT obligations and to determine the standard of CDD that is suitable for their own organisation.

124. It is important that the Board and senior management of the insurer or intermediary should not only establish and support the development of internal policies, procedures and controls but should also ensure that they are properly implemented and adhered to. Implementation of internal AML/CFT measures should constitute a relevant priority for insurers and intermediaries. In addition, the Board and senior management of an insurer or intermediary should be kept regularly informed of all significant matters relating to AML/CFT measures and whether the insurer or intermediary is suspected of being used to launder

[18] The term "compliance officer" may in some jurisdictions be referred to as the money laundering reporting officer or chief anti-money laundering officer, or similar. The compliance officer would have responsibility for ongoing monitoring of the fulfilment of AML/CFT duties by the insurer or intermediary, and act as the contact point regarding AML/CFT issues, both internal and external, including reporting suspicious transactions. To carry out these responsibilities effectively the compliance officer should have sufficient resources. The compliance officer would also need to be sufficiently independent from other business functions to ensure that AML/CFT concerns are raised with and addressed objectively by the insurer's or intermediary's Board.

money or to finance terrorism. This information should be used to evaluate the effectiveness of the programmes and to take appropriate action.

125. The compliance officer should be well versed in the different types of products and transactions which the institution handles and which may give rise to opportunities for ML/TF. On receipt of a report from a member of staff concerning a suspicious customer or transaction, the compliance officer should determine whether the information contained in such a report supports the suspicion. The compliance officer should have sufficient independence and resources to investigate and verify the details in order to determine whether the insurer or intermediary should submit a report to the FIU. The compliance officer should keep adequate records of all such reports and investigations, including a register of all reports to the FIU and a separate register of all reports submitted by staff (see also paragraphs 112-118 for suspicious transaction reporting).[19]

126. Where the compliance officer delegates part of the role to other staff for the purpose of efficient execution, the ultimate responsibility for ongoing monitoring of the fulfilment of AML/CFT duties should still lie with the compliance officer. In this respect, the compliance officer should establish that the delegated staff are appropriately supervised and required to report to the compliance officer in an appropriate and timely manner.

127. Insurers and intermediaries should ensure that:

- There is a clear procedure for staff to report suspicions of ML/TF without delay to the compliance officer or to a person specifically designated for this purpose;
- There is a clear procedure for investigating and reporting suspicions of ML/TF without delay to the FIU; and
- All staff knows to whom their suspicions should be reported.

Some jurisdictions require that a specified compliance officer (for example a Money Laundering Reporting Officer) be responsible for reporting all suspicions reported to him/her via internal procedures.

128. According to FATF Recommendation 18, insurers and intermediaries should implement group-wide programmes against ML/TF, which should be applicable, and appropriate, to all branches and majority-owned subsidiaries of the financial group. These should include the measures set out in criterion 18.1 of the FATF Methodology (see paragraph 120), and also:

- Policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;
- The provision, at group-level compliance, audit and/or AML/CFT functions of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes; and
- Adequate safeguards on the confidentiality and use of information exchanged.

129. Depending on the circumstances and local legal requirements, the parent company should perform a consolidated risk assessment for the entire group, taking into account the geographic situations of each relevant life insurance entity and, if any, the legal obstacles preventing foreign entities from applying AML/CFT group-wide procedure including exchange

[19] Including agency and temporary staff.

of information within the group. This will help to ensure that there is adequate oversight and consistent mitigating measures among all relevant entities of the group.

130. According to FATF Recommendation 18, in the case of foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those of the home country, insurers and intermediaries should ensure that their branches and majority owned subsidiaries implement the AML/CFT requirements of the home country to the extent that local (ie host country) laws and regulations permit. Insurers and intermediaries should pay particular attention that this principle is observed with respect to their branches and subsidiaries in jurisdictions identified as higher risk countries by the FATF. Where local applicable laws and regulations prohibit this implementation, or where the host country otherwise does not permit the proper implementation of AML/CFT measures consistent with home country requirements, insurers and intermediaries should apply appropriate additional measures to manage the ML/TF risks and inform the supervisor in the jurisdiction of the parent institution that they cannot apply the group-level AML/CFT programmes and FATF Recommendations for this reason.

131. It is recommended that insurers, intermediaries and other financial institutions exchange information both on trends and risks in general and on concrete cases, subject to their obligations concerning privacy and data protection. The IAIS encourages trade associations to promote and/or facilitate this exchange of information.

132. Internal controls should include an (external or internal) independent audit function to periodically examine all aspects of the AML/CFT system. It is also important that, if applicable, the auditor has direct access and reports directly to management and the Board.

16 Screening and training of staff

133. In order to meet FATF Recommendation 18, staff should have the level of competence necessary for performing their duties. Insurers and intermediaries should ascertain whether they have the appropriate ability and integrity to conduct insurance activities, taking into account potential conflicts of interests and other relevant factors.

134. Insurers and intermediaries should identify the key staff within their organisation with respect to managing AML/CFT risks and define fit and proper requirements which these key staff should possess. Paragraphs 139 to 143 provide a description of relevant positions.

135. The responsibility for initial and ongoing assessment of the fitness and propriety of staff lies with the insurer or intermediary. Procedures concerning the assessment of whether staff meet the fit and proper requirements should include the following:

- Verification of the identity of the person involved; and
- Verification of whether the information and references provided by the employee are correct and complete.

136. Decisions regarding the employment of key staff should be based on a well-founded judgement as to whether they meet the fit and proper requirements.

137. Insurers and intermediaries should keep records on the identification data obtained on key staff. The records should demonstrate the due diligence performed in relation to the fit and proper requirements.

138. Consistent with FATF Recommendation 18, the staff of insurers and intermediaries should receive initial and ongoing training on relevant AML/CFT legislation, regulations and guidance and the insurers' own AML/CFT policies and procedures. Such training and the

criteria for determining who should be trained should be appropriate given the risk of ML/TF and the size of the business. Although each insurer and intermediary should decide for itself how to meet the need to train members of staff in accordance with its particular legal, regulatory and commercial requirements, the programme would be expected to include at minimum:

- A description of the nature and processes of ML/TF, including new developments and current ML/TF techniques, methods and trends;
- A general explanation of the underlying legal obligations contained in the relevant laws, regulations and guidance; and
- A general explanation of the insurer's AML/CFT policy and systems, with particular emphasis on verification, the recognition of suspicious customers/transactions and the need to report suspicions to the compliance officer.

139. Employees who, due to their assigned work, need more specific training can be divided into two categories.

140. The first category of employees is those staff who deal with:

- New business and the acceptance – either directly or via intermediaries – of new policyholders, such as salespersons;
- The settlement of claims; and
- The collection of premiums or payments of claims.

141. Employees need to be made aware of their legal responsibilities, the AML/CFT and all other relevant policies and procedures of the insurer or intermediary. They need to be aware, in particular, of customer acceptance policies, the requirements of verification and records, as well as the need to recognise and report suspicious customers/transactions and any suspicion of TF. They also need to be aware that suspicions should be reported to the compliance officer or their designate in accordance with AML/CFT policies and procedures.

142. A higher level of instruction covering all aspects of AML/CFT policy and procedure should be provided to the second category of staff, including directors and senior management, responsible for supervising or managing staff and for auditing the system. This training should include:

- Responsibility regarding AML/CFT policies and procedures;
- Relevant laws, regulations and guidance including the offences and penalties arising from breaches of requirements;
- Procedures relating to the service of production and restraint orders (to stop writing business);
- Internal reporting procedures; and
- Requirements for CDD verification and record keeping.

143. In addition to the training mentioned in previous paragraphs, the compliance officer should receive in-depth training concerning all aspects of relevant legislation and guidance on AML/CFT policies and procedures. The compliance officer should have adequate skills and resources and will require extensive initial and continuing instruction on the validation and reporting of suspicious customers/transactions and freezing assets in accordance with relevant legislation.

17 Record keeping and retention

144. Consistent with FATF Recommendation 11, insurers and intermediaries should maintain records of identification data and other records obtained through CDD measures, and retain them for at least five years following the end of a business relationship (or longer if requested by a competent authority in specific cases and upon proper authority). Records include customer, policy or other account files, business correspondence and the results of any analysis undertaken (eg inquiries to establish the background and purpose of complex, unusual or large transactions). This would include information on the risk profile of each customer and/or beneficial owner and the data obtained through the CDD process, such as the customer's (and beneficiary's) name, address (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, the type and identifying number of any account involved in the transaction, and official identification documents (such as passports, identity cards or similar documents). For insurers and intermediaries, this implies that the prescribed period for keeping relevant records is at least five years after the expiration of policies.

145. Insurers and intermediaries should also maintain all necessary records on transactions, both domestic and international, for at least five years after completion of the transaction (or longer if requested by a competent authority in specific cases and upon proper authority). This requirement applies regardless of whether the business relationship is ongoing or has ended. Transaction records must be sufficient to permit reconstruction of individual transactions (including the amount and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

146. Insurers and intermediaries should ensure that they have adequate procedures:

- To access initial proposal documentation including, where these are completed, the customer financial assessment, customer needs analysis, copies of regulatory documentation, details of the payment method, illustration of benefits, and copies of documentation in support of verification by the insurer;
- To access all post-sale records associated with the maintenance of the contract, up to and including maturity of the contract; and
- To access details of the maturity processing and/or claims settlement including completed "discharge documentation".

147. All customer identification data, other CDD information, transaction records and other relevant information should be available in a timely fashion to the AML/CFT compliance officer and other appropriate staff. Such data and information should also be readily available to appropriately entitled domestic competent authorities.

Annex 1: Money Laundering Case Studies

While the case studies in Annex 1, contributed from the IAIS Membership, are illustrative and may assist in understanding how ML can occur in the insurance sector, they are not necessarily exhaustive nor are they intended to imply that such cases are common. To the extent some case studies involve non-life business, they are offered for illustrations that may be helpful in the context of life insurance, to which this application paper applies.

Case study 1. Early cancellation, insider collusion.

Mrs T (teacher) from country A, entered into a life insurance policy with a small initial premium being paid. The transaction was arranged by Mr B who was the agent of insurance company C and a cousin of Mrs T. Two days later, company C made a payment of an additional premium, in excess of €540,000, on behalf of Mrs T. After one month, Mrs T cancelled her policy and transferred the refund of contributions to three different accounts:

a) Mr MD (Managing Director of Company C) – €240,000;

b) Mrs N (niece of Mr MD) – €150,000; and

c) Mr U – €150,000.

All of them subsequently transferred the money onwards to other accounts in different banks. Following an investigation it appeared that the money being laundered was linked to fuel smuggling. The FIU ordered the accounts to be blocked and the case was forwarded to the public prosecutor.

Case study 2. High premium, early cancellation.

A single premium on a life policy, totalling more than €500,000 was paid on behalf of Mr A by Mr A's employer, who was a related person. Half of the amount was withdrawn by Mr A within a month of paying the premium. A request for withdrawing the balance of the amount was filed at the same time.

Following a report to the FIU subsequent checks revealed that Mr A had a criminal record and was involved in pending legal proceedings. It also appeared that Mr A was allegedly involved in drug dealing and assassinations. Following further investigation and collection of information, including tax records, and movements of funds on Mr A's accounts the relevant information was forwarded to law enforcement agencies.

Case study 3. High premium, false pretences for structured withdrawals.

A life insurance policy with a very high single premium included a clause for partial redemption, at the customer's request, at the end of each year. The customer claimed that the purpose of the clause was to repay the interest on a loan with a duration of 10 years, intended to facilitate the building of a warehouse. The insurer reported a suspicion to the local FIU because of the high premium and because the customer refused to name the bank where he had taken up the loan. After careful examination by the FIU, it turned out that the customer was known to the police as he had committed financial fraud. It appears that the customer had tried to launder money by means of a life insurance product.

Case study 4. Foreign policyholders, source of wealth.

An insurance company filed a report of suspicion concerning two foreign individuals each of whom bought a single premium life insurance contract. The premiums were very high. The investigation by the FIU showed that the premiums for these insurance policies were paid through the current accounts of the two customers, while payments to the accounts consisted of cash deposits the origin of which was unknown. Moreover, the accounts were only used for payment for the insurance policy and the account holders had already been the subject of a report on illegal drug trafficking. According to the police reports, the individuals were members of a network responsible for trafficking drugs from Latin America to Western Europe. The insurance company reported suspicion of potential ML on the basis of several factors, namely that the policyholders did not have an official address in the country where they wanted to buy the policy, they were not exercising any professional activity in that country, and they could not explain the origin of the money. This case is currently subject to legal proceedings.

Case study 5. Source of wealth.

Mr A, who claimed to be a 25 year old garage owner, bought a life insurance policy with a high single premium in relation to his age. The policy was issued for a duration of 10 years with Mr A being the beneficiary if alive and Mrs B being the beneficiary in the case of the death of Mr A during the 10 year duration of the policy (Mrs B being the grandmother of Mr A). The insurance company reported the case to the FIU. Research by the FIU showed that Mr A did not own a garage but had been involved in drug trafficking. The FIU forwarded its report to the department of justice, which dealt with cases of drug trafficking.

Case study 6. Early cancellation.

A couple in their twenties purchased several single premium life insurance contracts with the same insurance company. A little later they requested an early repayment of these policies in cash. This, combined with the young age of the insured, attracted the attention of the insurance company. The FIU found that both policyholders had convictions and were the subjects of a drug investigation. The file was referred to the criminal court.

Case study 7. Early cancellation, payout to third party.

A policyholder living abroad bought a life insurance policy and, soon afterwards, requested early surrender of the policy. This early surrender resulted in high costs for the policyholder. Afterwards, the policyholder made a request by fax to transfer the money to an account of another person living abroad. The insurer contacted the FIU, which, in light of the urgency of the situation, requested that the transaction should be postponed for 24 hours. This gave the FIU time to collect data, which indicated that the policyholder had been convicted for illegal public attraction of savings. The case has been transferred to the justice department for further investigation.

Case study 8. Source of wealth.

Two life insurance policies were bought for a large amount in the names of Mr X and Mr Y. The payments were made by cheque, originating from the account of a European investment company. Both polices were used as security for a mortgage loan with a company that specialised in leasing. As the beneficiaries were not the policyholders and in light of the unusual financing being provided by a leasing company, the insurer contacted the investment company in order to understand the origin of the money that had been deposited in the account. It appeared that the money was deposited with the company in cash by random customers. Following the disclosure of suspicion by the insurance company it became evident

that Mr X and Mr Y were known by the customs authorities for the illegal importation and exportation of cars.

Case study 9. Early cancellation, source of wealth.

A 34 year old car dealer received a loan through a broker of a life insurance company to purchase a house. He invested around 25% of the loan in a single-premium life insurance policy. He later surrendered the policy early to pay back the loan (capital and interest), making up the shortfall through other funds. The use of a substantial proportion of the loan to purchase a policy combined with the unexpectedly early repayment of the loan led to the FIU being contacted. The FIU's investigation revealed that the policyholder was known for stealing and receiving stolen cars. Moreover, he had used false documents to prove the sources of his income and wealth.

Case study 10. Adverse media for existing customer.

A life insurance company was contacted by a financial adviser calling on behalf of a customer who had taken out a policy. The customer had recently been convicted of fraud and wished to ascertain whether such a conviction would compromise the policy's terms and conditions. The conviction did not pose a problem for the continuation of the policy. However the disclosure of fraud prompted an internal review. Active investment policies were identified and a media article was found, which stated that the customer had been part of a gang involved in a €6 million tax fraud and subsequent ML offences. A suspicious activity report was submitted to the FIU. Following dissemination of the intelligence by the FIU, the tax authority advised the insurance company that its report provided useful information, allowing a case for confiscation of assets to be made.

Case study 11. Source of funds.

A life insurance company received a payment of €25,000 for an existing customer via an "over the counter" transaction. When the money was received, enquiries were made by the company as to where the money had come from. It transpired that the money had been deposited in cash at a bank in order to pay premiums to the insurance company. The receiving bank had not asked questions when the cash was received. However, the life insurance company considered the transaction to be suspicious in light of the amount, the fact that it had not received such a payment from the customer before and that it contradicted confirmations provided by the customer as to how payments would be made, and the absence of reasonable responses by the customer to questions by the insurance company. Consequently, a suspicious activity report was made to the FIU.

Case study 12. Foreign PEP.

A financial adviser approached a life insurance company in order to make a pre-application enquiry on behalf of a potential customer to PEP classifications and other issues. The potential applicant was married to a former president of a developing country who was in self-imposed exile due to outstanding criminal matters. The spouse was seeking a whole life product in order to protect her tax liabilities. However, the husband was implicated in a multi-million dollar theft of public state money. The business was rejected and a report made to the FIU.

Case study 13. Source of funds, complex scheme.

A company director from Company W, Mr H set up a ML scheme involving two companies, each one established under different legal systems. Both of the entities were to provide financial services and providing financial guarantees for which he would act as director. These

companies wired the sum of USD1.1 million to the accounts of Mr H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in Country U amounted to some USD1.2 million and represented the last step in the laundering operation.

Case study 14. Source of funds.

A husband and wife took out a life insurance policy each in their own name with annual premiums. In the event of the death of one of the spouses, the other spouse would become the beneficiary of the insurance. The holder of the account through which the premiums had been paid was found not to be the policyholders but a company abroad of which they were directors. However, this was a life insurance policy taken out privately by the couple and not by the company. Investigation revealed that the scenario set up had been intended to conceal the illicit origin of the funds which originated from serious and organised tax fraud for which the couple involved was known.

Case study 15. Inappropriate beneficiary.

A mayor concluded a unit-linked life insurance contract as the representative of the municipality. He was named as the insured person and the insurance fee was taken directly from the budget of the municipality. In case of expiry of the contract, the municipality would have been the beneficiary. However, a notification was submitted to the insurance company after the expiry of the contract, assigning the mayor as the new beneficiary of the insurance policy, and requested the payment to be fulfilled on his private bank account following the expiry of the contract. The insurance company submitted a STR to inform the FIU.

Case study 16. Employee / Agent fraud, source of funds.

Misled by an agent of an insurance company, customers deposited large cash payments to the bank account of an insurance company in favour of the insurance policy of the daughter of the agent. The source of these cash payments was a large amount of winning derived from foreign gambling. Certainly, the customers believed that they deposited the cash in favour of their own insurance policies. Then, after numerous claims of partial redeems sent to the insurance company, the agent finally repurchased the unit-linked insurance policy of her daughter.

Case study 17. Source of funds.

The deputy mayor of a medium-sized town was in charge of social care and of the elderly. He received, in three months, € 1 million transferred from the account of an advisor society and € 0.6 million from the account of a real estate society (of which he later became a shareholder) to build a retirement home. After having justified the inflows of funds by producing invoices, the elected representative used part of the funds to build a life insurance portfolio and invest in a private real estate purchase. The case was reported to the FIU.

Case study 18. Source of funds.

After an investigation, the chairman of a private elementary school was sued by the prosecutor and was judged guilty because he had misused the miscellaneous fees (for tutor classes,

comprehensive activities, bilingual classes, etc.) the school received from students. Such fees were not precisely recorded in the school's financial report or the income statement required by the authorities. Having realized that the fees paid by students were deposited in a bank account that belonged to school, the chairman instructed the school's accountant to withdraw the cash in order to hand over to him. A part of the illegal income was used to pay for the premium fee of 15 insurance policies held by him, his wife, and son. Another portion of the illegal income was spent on purchasing properties, stocks, vehicles, trust funds, and long-term deposits. The rest amount of the illegal income was hidden in a safe-deposit box.

Case study 19. Intermediary collusion.

A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raised no suspicion at the bank since the insurance broker was known to them as being connected to the insurance branch. The insurance broker delivered, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding raising suspicions with the insurance company.

Case study 20. Intermediary collusion, payout to third party.

Customers in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the customer by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the customer stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Case study 21. Employee / Agent collusion, multiple withdrawals.

A drug trafficker, whose wife was a part-time insurance agent, used the proceeds of his illegal activities to purchase insurance policies from his wife and invest in several businesses including a restaurant business. Substantial increase in monthly premium for one of the insurance policies, multiple withdrawals, where the proceeds were subsequently used to pay premiums of other existing insurance policies and advance premium of one year for most of the insurance policies are some of the risk indicators revealed by the investigation of which he, his mother and his wife were subjected.

Case study 22. Employee/agent collusion, source of wealth, early cancellation.

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the customer had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in his policy.

Case study 23. Unusually high premium.

An insurer in Country A sought reinsurance with a reputable reinsurance company in Country B for its directors and officers cover of an investment firm in Country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that – although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

Case study 24. Complex scheme.

A group of persons with interests in home construction effected a payment in favour of construction company A under contracts connected with their participation in investment construction (at cost price). Insurance company P accepted possible financial risks to these contracts under a contract of financial risks insurance and received an insurance premium. At the same time the insurance company P concluded with the construction company A a secret agreement providing that the difference between the market cost of housing and the cost price was transferred in favour of the insurance company as a premium under the contract of financial risks insurance. When the funds were received by the insurance company P they were transferred as insurance premium under the general reinsurance contract in favour of insurance company X. By way of fictitious service contracts and commission payments made under an agency contract, insurance company X channelled the funds to several off-shore shell firms. Beneficiaries of the actual profit, being withdrawn abroad, were owners and directors of the construction company A.

Case study 25. Compendium of STR characteristics.

To promote good practices in the insurance industry, an IAIS member has published a compendium that provides several categories of representative samples of a high-level description and characteristics of STRs. Examples include:

(1) Cases identified with a focus on the use of cash
- Transactions where a policyholder pays premium by a large amount of cash or a cheque, in particular in a case where the amount is high and not considered affordable in terms of income and assets of the policyholder.

(2) Cases identified with a focus on the possibility of concealing the true policyholder
- Transactions related to an insurance contract that is suspected to be concluded with a fictitious name or another person's name.

(3) Cases identified by developments after a conclusion of contracts
- Transactions that are unusual from the viewpoint of economic rationality. For example, cases where contracts are terminated at an unusually early stage.

(4) Cases identified with a focus on transactions with parties in foreign countries
- Transactions related to a beneficiary who requests to receive claim payment or a policyholder who requests to receive surrender value in a country or region that is non-cooperative with measures for anti-money laundering and combating the financing of terrorism ("AML/CFT measures") or a country or region that exports illicit drugs.

(5) Other cases
- Transactions related to organized crimes.

Annex 2: Terrorist Financing Case Studies

While the case studies in Annex 2, contributed from the IAIS Membership, are illustrative and may assist in understanding how TF can occur in the insurance sector, they are not necessarily exhaustive nor are they intended to imply that such cases are common. To the extent some case studies involve non-life business, they are offered for illustrations that may be helpful in the context of life insurance, to which this application paper applies.

Case study 1. Early cancellation, payment method.

In October a motor insurance policy was purchased by Mr X. The premium was based on 4 years no claims bonus and the premium was paid by way of debit/credit card via the internet. Mr X cancelled cover on the 5th of November and asked for the refund of premium to be paid by personal cheque as he had lost the relevant debit/credit card.

On 3rd December Mr X contacted the insurer's call centre and took out cover on a different vehicle, a Vauxhall Corsa. This time he attempted to pay via a debit/credit card and initially the transaction was declined. The premium was paid in full by debit card the following day. Mr X now claimed that he had not earned any claims bonus and bought every possible "added on" product. Once again Mr X requested that this policy be cancelled. He requested that the refund of premium should not be paid via the original debit card as that particular bank account had been closed. Consequently he asked for a personal cheque to be sent to him. This was refused with the insurer insisting that the refund should be paid via the original debit card. The insurer has subsequently established that the first refunded cheque was presented to cash converters.

Subsequent action

The series of transactions was reported to the FIU. Subsequent investigations indicated that the individual concerned appeared to be linked to a terrorist network.

Case study 2. Fraudulent claim.

A leader of a terrorist organisation instructed Mr X, who was trained in Afghanistan and fought U.S. forces in the country for several years, to set aside his initial intention to volunteer as a suicide bomber and sent him to Country A to support the organisation from there. In September 2004, Mr X attempted to acquire large sums of money from life insurance companies fraudulently, intending to direct a great part of this money to the terrorist organisation in order to fund its terrorist activities. To this end, Mr X recruited Mr Y and Mr Z, Mr Y's brother. Life insurance policies of 4 million euro were taken out for Mr Y with his brother, Mr Z, as the designated beneficiary. Mr Y was to fake a fatal traffic accident during his stay in Country B. By obtaining a death certificate, if necessary through bribery, the life insurance benefits were to be collected by Mr Z who would transfer the proceeds abroad via foreign bank accounts to fund terrorist activities. Mr X was primarily responsible for paying the insurance premiums for these life contracts. The plan was thwarted when Mr X and Mr Y were arrested in January 2005.

Subsequent action

Mr X and Mr Y were convicted of membership in a terrorist organisation and multiple counts of fraud. Mr X was sentenced to seven years in prison and Mr Y to six. Mr Z was also convicted

of the lesser charge of supporting a terrorist organisation and fraud. He was sentenced to three and a half years in prison.

Case study 3. Early cancellation.

Setting up the return of a foreign fighter from a conflict zone required several thousand euros. Accordingly, the close associates of the individual wishing to come back to France had to mobilize funds. Transactions were observed on the accounts of members of the family and a circle of sympathizers of individuals present in the combat zone. These operations took various forms. The most frequent were cash withdrawals arising from the proceeds of car or house sales, or from early surrender of a life insurance policy. The insurer submitted a STR to the FIU.

Case study 4. Suspicious claim.

An UK based insurer underwrote Jewellers block coverage for a Jewellery company based in Miami Florida, USA. A claim against the policy was made. However, the company owner, Mr X was unable to provide evidence of the loss and as a result an investigation took place. The investigation identified discrepancies in the financial records of the company and raised questions with regard to the movement of monies between bank accounts. Of significant interest was the transfer of funds to a bank account in Beirut. Under oath, Mr X stated that the account contained in excess of $200,000. No explanation for the movement of monies was provided and no bank statements were produced with regard to the bank account in the Middle East.

Subsequent action

This matter was reported to US law enforcement agencies by the insurer's attorneys. The law enforcement agencies were particularly interested in the movement of funds and indicated that these could have been used for the purposes of terrorist funding.