ICP 28: Anti-Money Laundering and Combating the Financing of Terrorism

Basic-level Module
This module was prepared by Steve Butterworth, who was appointed the first Guernsey insurance supervisor in 1986. He retired in 2003 and has acted as an advisor and a director of insurance companies since that time. He is a chartered accountant, a chartered tax advisor, a certified fraud examiner, a member of the Institute of Risk Management, the Chartered Insurance Institute, and the Association of Insurance and Risk Managers. Before 2003, he was a founding member and significant contributor to the International Association of Insurance Supervisors (IAIS), serving on the Executive Committee and as chair of the Education Committee and the Insurance Fraud Subcommittee. He is executive director of the Offshore Group of Insurance Supervisors (OGIS) and was the founding chair of that organization.

This module was reviewed by Alma Gomez and Peter van den Broeke. Alma Gomez has been the acting supervisor of insurance, Office of the Supervisor of Insurance, Belize, since 2002. Prior to that, she was assistant supervisor of insurance in the Ministry of Finance for eight years. Until 2003, she was president of the Caribbean Association of Insurance Regulators. Peter van den Broeke has 20 years experience in legal, policy and prudential positions with supervisory authorities in the Netherlands. He holds degrees in law and forensic auditing and studied economics. He is the chair of the IAIS Insurance Fraud Subcommittee and responsible for the IAIS Standard on fit and proper requirements and assessment for insurers and the Guidance paper on anti-money laundering and combating the financing of terrorism. He has given presentations on issues of economic crime for several organisations like the Council of Europe, the Geneva Association, the Cambridge Symposium on economic crime and the International Association of Insurance Fraud Agencies.
Contents

About the Core Curriculum .............................................. v

Note to learner ............................................................... vii

A. Description of money laundering and terrorism financing ......................... 1

B. Vulnerabilities of the markets ............................................. 8

C. Addressing the vulnerabilities ............................................. 16

D. References ................................................................. 24

Appendix I. ICP 28 ............................................................ 26

Appendix II. Summary of selected FATF Recommendations ......................... 28

Appendix III. Answer key .................................................... 31

Case studies

Case study 1. Life insurance: “Operation Capston,” Colombia ......................... 9
Figures

Figure 1. Money laundering stages .................................................. 4
Figure 2. Money laundering using reinsurance ................................. 11
Figure 3. Money laundering using different parties .......................... 13
A financially sound insurance sector contributes to economic growth and well-being by supporting the management of risk, allocation of resources, and mobilization of long-term savings. The insurance core principles (ICPs), developed by the International Association of Insurance Supervisors (IAIS), are key international standards relevant for sound financial systems.

Effective implementation of the ICPs requires skilled and knowledgeable insurance supervisors. Recognizing this need, the World Bank and the IAIS partnered in 2002 to develop a “core curriculum” for insurance supervisors. The Core Curriculum Project, funded and supported by various sources, accelerates the learning process of both new and experienced supervisors. The ICPs provide the structure for the core curriculum, which consists of a set of modules that summarize the most relevant aspects of each topic, focus on the practical application of supervisory concepts, and cross-reference existing literature.

The core curriculum is designed to help those studying it to:

- Recognize the risks that arise from insurance operations
- Know the techniques and tools used by private and public sector professionals
- Identify, measure, and manage these risks
- Operate effectively within a supervisory organization
- Understand the ICPs and other IAIS principles, standards, and guidance
- Recommend techniques and tools to help a particular jurisdiction observe the ICPs and other IAIS principles, standards, and guidance
- Identify the constraints and identify and prioritize supervisory techniques and tools to best manage the existing risks in light of these constraints.
Welcome to ICP Module 28: Anti-money laundering and combating the financing of terrorism! This is a basic-level module on AML/CFT that does not require specific prior knowledge of this topic. The module should be useful to either new insurance supervisors or experienced supervisors who have not dealt extensively with the topic or are simply seeking to refresh and update their knowledge.

Start by reviewing the objectives, which will give you an idea of what a person will learn as a result of studying the module. Then proceed to study the module either on an independent, self-study basis or in the context of a seminar or workshop. The amount of time required to study the module on a self-study basis will vary, but it is best addressed over a short period of time, broken into sessions on sections if desired.

To help you engage and involve yourself in the topic, we have concluded the module with an exercise for you to complete. If you are working with others on this module, develop the answer through discussion and cooperative work methods. An answer key in appendix III sets out some of the points that you might consider when tackling the exercise.

As a result of studying the material in this module, you will be able to do the following:

1. Explain the vulnerabilities of the insurance market to money laundering
2. Describe the possible concealment of criminal interests within legitimate insurance business structures
3. Describe possible misuses of legitimate insurance products for money laundering purposes
4. Illustrate the transfer of secret profits through insurance products
5. Explain how insurance of untraceable assets could be used for money laundering
6. Describe supervisory activities that could be undertaken for anti-money laundering and combating the financing of terrorism (AML/CFT) purposes
7. Show how know-your-customer requirements can discourage money laundering
8. Show how money launderers could exploit jurisdictional issues
9. Illustrate how a supervisory authority could cooperate with other authorities for AML/CFT purposes
10. Summarize the requirements of ICP 28.
ICP 28:  
Anti-Money Laundering and  
Combating the Financing of Terrorism

Basic-level Module

A. Description of money laundering and terrorism financing

History

“Money laundering” (ML) is a fairly recent expression. It was first seen in a newspaper reporting on the 1973 “Watergate” break-in and was first used judicially in a 1982 United States case.

Some say that the origin of the term goes back to the 1920s–30s when gangsters wanted to conceal the origins of their huge illegal cash funds gained from bootleg (prohibited) liquor, extortion, gambling, and prostitution. The gangsters favored buying laundromats (coin-operated public laundries), which took cash-only sales, to which receipts were added regular contributions of criminal monies, all of which were then banked as legitimate laundromat sales.

Others say that this is a myth and that “money laundering” is so called because the name accurately conveys its meaning: the attempt to conceal the illegal origin of monies through one or more financial transactions. Colloquially, illegal monies are called “dirty monies” and legal monies called “clean monies,” hence, the analogy to laundering.

Whatever the term’s origin, it is certain that what we know as money laundering was occurring in the early twentieth century. Meyer Lansky, “the Mob’s Accountant,” used secret-numbered bank accounts in which to deposit illegal funds. These were then returned to him, disguised as loans. The loans appeared to come from a legitimate source—a well-respected, unrelated overseas bank.

1. Most of the specialist terms are explained within the text of this module. Insurance-related terms can be found in the IAIS Glossary (see IAIS 2005).
Unfortunately for them, the mobsters claimed tax deductions. For example, infamous gangster Al Capone was convicted and jailed on charges of tax evasion, the charge that the Federal Bureau of Investigation found most effective to pursue.

Money laundering as a crime next came to the fore in the 1970s–80s as a result of the big increase in drug trafficking. This increase was brought about by large drug abuse problems within affluent societies throughout the world.

**Definition of money laundering**

“Money laundering’ is used to describe a number of techniques, procedures, or processes in which funds obtained through illegal or criminal activities are converted into other assets so as to conceal their true origin, ownership, or any other factors that may tend to reveal an irregularity. The main objective of money laundering is to legitimize income originating from these sources.”

This definition is one of many definitions that cover the subject. The Financial Action Task Force on Money Laundering (FATF)\(^3\) has a simpler definition: “the processing of criminal proceeds to disguise their illegal origin.” This definition is the basis for the IAIS definition used in ICP 28. However, anti-money laundering legislation is being passed in more and more jurisdictions with a proliferation of experience resulting from the many cases that have been heard. Consequently, the meaning of money laundering has broadened to sometimes include transfers of funds prior to the commission of the offense and to link the initial offense, such as fraud, with the offense of money laundering.

Law enforcement authorities tend to use whichever law will give them the surest means of achieving a prosecution. If, for instance, the prosecutor decides that there would be more certainty of conviction by prosecuting under anti-money laundering legislation than under general fraud legislation—for example, with an individual who fraudulently strips assets from an insurance company—then the prosecutor may choose this route. Whether this route could be achieved will depend partly upon whether the fraud comes within the money laundering definition. Laws usually are drafted in an attempt to be all-encompassing. The result of this policy is that the original definitions have been expanded as experience grows. Thus, the meaning of money laundering in some jurisdictions can include other types of fraud (see also ICP 27 Fraud\(^4\)).

---

3. www1.oecd.org/fatf/.
4. ICP 27 covers the areas that prevent, detect, and remedy insurance fraud. Thus, ICP 27 and ICP 28 are closely linked. It is recommended that the modules are studied either at the same time or the one right after the other.
**Placement, layering, and integration**

All insurers and insurance intermediaries are potentially at risk of being misused for money laundering and the financing of terrorism (FT). Criminals look for ways to conceal illegitimate origins of funds. Persons involved in organizing terrorist acts look for ways to finance these acts. The products and transactions of insurers can provide the opportunity to launder money or to finance terrorism. Insurers and intermediaries, in particular those insurers and intermediaries offering life insurance or other investment-related insurance products, could be involved, knowingly or unknowingly, in money laundering and financing of terrorism.

In the original sense of the meaning, money laundering consists of three stages, which may be effected in one or more transactions. Generally, these stages occur in sequence but often overlap:

1. **Placement** is the physical disposal of criminal proceeds. In the case of many serious crimes (not only drug trafficking), the proceeds take the form of cash that the criminal wishes to insert into the financial system. Placement may be achieved by a wide variety of means, according to the opportunities afforded to, and the ingenuity of, the criminals and their advisers and network.

2. **Layering** is the separation of criminal proceeds from their sources by the creation of layers of transactions designed to disguise the audit trail and provide the appearance of legitimacy. Layering, too, may be achieved by a wide variety of means, according to the opportunities afforded to, and the ingenuity of, the criminals and their advisers and network.

3. **Integration** is the stage in which criminal proceeds are treated as legitimate. If layering has succeeded, integration places the criminal proceeds back into the economy in such a way that they appear to be legitimate funds or assets.

Insurance entities could be involved, knowingly or unknowingly, in money laundering and financing terrorism. If an insurance entity is used for money laundering, there could be resulting prosecutions, and financial and reputational damage to the operation. Therefore, insurance entities should take adequate measures to prevent themselves from being misused by money launderers and terrorists and should address possible cases when they occur. To some extent, the 40 Recommendations and the 8 Special Recommendations on Terrorist Financing of the Financial Action Task Force (see D and References) on Money Laundering (FATF), jointly referred to as the FATF Special Recommendations, apply specifically to insurers and insurance intermediaries.

---

5. Insurance entities include insurance and reinsurance companies and insurance intermediaries.
Money transfer methods

For money laundering to be successful, the criminals must eliminate the “paper trail” (audit trail), or at least make it complex, to separate each of the steps and thereby confuse any investigator. They may be able to do so by infiltrating the financial system or by physically smuggling the currency out of the country concerned. Within the insurance system, money launderers may structure transactions, coerce employees to cooperate and not file proper reports, or establish apparently legitimate “front” insurance entities to launder money.

Money laundering networks continue to provide avenues to siphon money to individuals, groups, and nations across national borders and across the world for illegitimate purposes. Several methods of underground banking (sometimes termed “parallel” banking) are used in various parts of the world. There is a certain lack of understanding by authorities of these efficient but wholly unauthorized methods of money transfer, largely due to a lack of understanding of the cultures in which the systems operate.

The systems, sometimes referred to as “Black-Market Peso,” “Hawalla,” “Hundi,” and “Chop,” do not require the actual movement of money and avoid the use of conventional paper records. Monies are paid to an underground banker in one jurisdiction and can be drawn from a connected underground banker in the recipient’s jurisdiction. The receipt can be a symbol recognized by both “bankers.” For example, a picture of an elephant represented a collection receipt for U.S.$3 million at a certain gold shop.

The presence of underground banking does not necessarily mean money laundering is also present. However, historically, underground banking has proven itself to be one of the safest methods for money launderers to transfer large sums of money without a trace.
The internet has become a focus for concern in the field of money laundering and underground banking. “Cyberspace banking” and “cyberspace money laundering” have crept into the financial lexicon of the first cyber banks, which first opened for business in late 1994 and early 1995.

Online gambling, which relies on cyber banking, followed soon after in May and June 1995, and more online gambling has appeared since then. Stanley Morris, Director of the U.S. Treasury’s FinCEN, targeted cyber banking as one of his agency’s highest priorities. Given its home outside the present regulatory reach of the U.S. and most other countries, his concerns are not misplaced.

Cyberspace banking can provide payments for purchases and services over the internet, a process that is growing rapidly. Cyberspace banks can act as intermediaries in any transaction, including the sales of goods and services. Cyber banking is particularly vulnerable to money laundering because of the lack of face-to-face contact with customers, difficulties involved in supervising it, and jurisdictional challenges that can arise.

Smuggling currency out of the country, especially into jurisdictions with rigid secrecy standards, and then wire transferring the funds to financial institutions in the country of origin was a common method used by money launderers. In recent years, many secrecy laws have been repealed through pressure by FATF and related organizations. There were secrecy laws in many jurisdictions, including Europe, North America, and “offshore” jurisdictions.

In some jurisdictions that have a strict currency exchange control regime, there are sometimes exemptions for reinsurers due to national capacity limitations. If the criminals controlled, or were able to influence, an insurer, a payment of a reinsurance premium would be an easy method of exporting currencies without going through the normal reporting procedures.

The various regional and international organizations that are fighting money laundering have established a web-based International Money Laundering Information Network (IMOLIN). It is well worth looking at its website, which links to member sites such as Interpol and to regional groups, such as the Caribbean Financial Action Task Force.

The Offshore Group of Insurance Supervisors (OGIS) has brought out a useful paper, “Avoiding Money Laundering in the Insurance Sector.” This paper also is well worth reading because it explains some of the risks encountered with cross-border insurance business. These risks apply also to insurers that write overseas risks and are based in mainstream jurisdictions.

---

6. FinCEN is the U.S. government agency that has the primary responsibility for detecting and combating money laundering. www.fincen.gov/
7. www.imolin.org
8. www.ogis.net
**Definition of terrorist financing**

Terrorist financing can be defined as the willful provision or collection—by any means, directly or indirectly—of funds with the intention that the funds should be used, or in the knowledge that they are to be used, to carry out terrorist acts. Terrorism can be funded from legitimate income. It often will not be clear at what stage legitimate earnings become terrorist assets.

The process of terrorist financing can also be divided into three stages.

In the first stage, *sources are found and funds are gathered*. The FATF has indicated that terrorist financing comes from two primary sources:

- **Financial support provided by States or organizations** with large enough infrastructures to collect and then make funds available to the terrorist organization, that is, “State-sponsored” terrorism, or, in more recent times, by wealthy individuals.

- **Income from “revenue-generating” activities**. These activities could be either legal or illegal. Terrorist groups might fund their activities by kidnapping, extortion, drug trafficking, smuggling, or various types of fraud. The funding also may involve income from legitimate sources. Legal means of “fundraising” could consist of donations, regular enterprises, and borrowing money. Some charities are followed closely because of their potential or perceived involvement in terrorism. Enterprises such as bars or restaurants can generate revenues for the terrorists that control these businesses.

In the second stage, *the funds are transferred to their destinations*, or temporarily deposited before being used for their intended purpose. Some ways of moving funds from source to destination have been witnessed in practice, and these and other methods are discussed later.

In this stage, terrorists could try to process funds through financial institutions. Although insurance companies are less likely to be misused, even insurance could be a source or used to deposit money, at least in theory. Funds could become available through an early surrender of a life policy. The destination of the benefits from the policy could be altered by changing the beneficiary to the insurance contract. It is not unusual that people use their last wills or life insurance policies to leave money to others or to charities.

In the third and final stage, *the funds reach their intended destination*. Again, two types of purposes can be distinguished: (a) illegal or (b) legal (or in general considered as legal). Sometimes funds are used for more legal purposes and have political or social objectives. Some terrorism movements have a political wing that needs to fund propaganda. In addition, some groups have made arrangements to support the families of incarcerated or killed terrorists.
The financial institution may be the source of funds (loan, insurance), or it may serve as an intermediary to transfer or deposit the funds. A financial institution may be involved in legal money being processed for legal purposes or illegal purposes and with illegal funds being processed through its organization with legal or illegal objectives.

Terrorist financing sometimes has the features of money laundering, but, in the case of legal funds being used for illegal purposes, this phenomenon can be seen as reverse money laundering, or “blacking.” In this case, it is the intention of the terrorist to interrupt the paper trail to avoid a legitimate source from being linked to its illegal use.

As discussed later, FATF has brought out eight Special Recommendations covering CFT (Combating the Financing of Terrorism).

The United Nations Security Committee has established a Counter-Terrorism Committee, which has created a global network of organizations, including the IAIS, working to counter terrorism.

---

B. Vulnerabilities of the markets

Size of the problem

Former U.S. Secretary of State George Schultz said, “Today’s criminals make the Capone crowd and the old Mafia look like small-time crooks.”

The problem is vast, although estimates of its magnitude vary. For instance, the “John Walker model,” published in 1998, put the value of money laundering, even then, in the region of $2.85 trillion per year, heavily concentrated in Europe and North America.\(^\text{10}\) The International Monetary Fund has stated that the aggregate of money laundering in the world could be two percent–five percent of the world’s gross domestic product.

Billy Steel says that “money laundering is the crime of the ‘90s…the world’s third largest business,” and that in the UK alone, “A recent survey by the insurance industry reckons that crime costs the country £85 billion per year and that 85% of that is drug related.”\(^\text{11}\)

Now that most jurisdictions have implemented anti-money laundering legislation, the resources involved in preventing and detecting money laundering and prosecuting offenders also are vast.

There is even an association, the Association of Certified Anti-Money Laundering Specialists (ACAMS), whose mission is ‘To advance the professional knowledge, skills and experience of those dedicated to the detection and prevention of international money laundering, and to promote the development of sound anti-money laundering policies and procedures.”\(^\text{12}\)

Nature of the vulnerabilities

Financial institutions, including insurance entities, have become major targets of money-laundering operations because of the variety of services and investment vehicles offered that can be used to conceal the source of money.

Money laundering poses significant reputational and financial risks to insurance entities, as well as the risk of criminal prosecution if they become involved in laundering the proceeds of crime. Involvement in money laundering can lead to the loss of the company’s license, or the large surrenders may cause a liquidity problem for the insurer.

The perfect scenario within which criminals could launder monies would be a financial services sector. This sector is global, consists of large and well-respected companies, keeps customer confidentiality, is adaptable in its operations, and uses the latest technology for speedy and accurate transfers of monies on a 24-hour basis.

\(^{10}\) http://members.ozemail.com.au
\(^{11}\) www.laundryman.u-net.au
\(^{12}\) www.acams.org
The insurance sector drops neatly into most of the above descriptions.

Primarily, an insurance entity needs to use the services of a bank to transfer monies to and from the client. The involvement of an intermediary financial institution makes insurance less vulnerable to money laundering than banking.

Nevertheless, an insurance transaction can be a very significant part of the layering process.

---

**Case study 1. Life insurance: “Operation Capstone,” Colombia**

The authorities in the United States, the Isle of Man, Colombia, and other jurisdictions worked together to expose a very sophisticated scheme that laundered some $80 million worth of Colombian drug proceeds over several years. International insurance brokers—some affiliated with and some independent of the cartel with little relevant knowledge—were manipulated to place monies with international life insurers. Their focus on commission income obscured any thoughts about money laundering, such as “know your customer,” wealth of the policyholder, or unusual methods of payment of the premiums. In some cases, the funds came to the U.S. through a kind of underground banking system.

The brokers had much autonomy and control over policies. Some had pre-signed payment instructions for early withdrawals and used existing policies owned by sometimes unsuspecting policyholders who had no knowledge of the transaction by way of “top-ups.” A top-up is the process of adding lump sums to an existing investment-type insurance policy.

The cartels routinely surrendered the life insurance policies after relatively short periods, receiving “clean” surrender benefits from the insurance companies.

The insurers involved had inadequate procedures and controls, and little reliable information about the brokers or the policyholders. They did not recognize indicators such as payments from third parties, through currency exchanges, or via consecutively numbered checks and money orders.

---

**Case study 2. Non-life insurance: “The Red Dawn,” Eastern Europe**

An Eastern European oil and gas company paid premiums to a European insurer on the basis that the insurer would repay them if there were few or no claims. The risk covered was goods-in-transit, a non-life insurance business. No claims were forthcoming, and part of the premiums were repaid, but to a company later found to be owned by certain directors of the unsuspecting utility company. These directors had fraudulently extracted monies from their employer by using a class of business that had few claims and exaggerated the premium rates.

As discussed above, in most jurisdictions, this form of fraud comes under the legal definitions of money laundering.
The IAIS is very much aware that the insurance industry is at risk of being misused by criminals for fraudulent activities and in 2002 agreed that work in this area should be among the association's priorities. The financial resources of insurance companies and their methods of doing business attract fraudsters. However, as mentioned above, the nature of the insurance business means that other financial institutions are more vulnerable to money laundering. Because of their ability to move funds quickly and the inherent confidential relationship between bank and customer, banks are particularly vulnerable to money laundering.

**Insurance product types**

The terms “insurance” and “insurance business” cover a variety of products and services under which risks are underwritten and processed within the insurers. It is necessary to have a comprehensive understanding of the risks involved and a need for a risk-based approach when supervising all aspects of insurance, including AML/CFT.

Life insurance and non-life insurance can be used in different ways by money launderers and terrorist financiers. The vulnerability depends on such factors as the complexity and terms of the contract, distribution, payment system, and contract law. In practice, life insurance is perceived to be the predominant class being used by money launderers.

**Non-life insurance**

Non-life insurance (sometimes called property and casualty insurance) money laundering can be seen through false claims. False claims occur when money launderers purchase legitimate businesses, then through arson or other means, cause a bogus claim to recover part of their investment.

This happened in Florida, where the Cali drug cartel purchased a gold refining plant which was destroyed in an act of arson. However a characteristic of insurance that differentiates it from banking is that insurance gets a second chance to “know your customer” and stop the payment of the claim until the loss adjuster13 is completely satisfied that it is bone fide. In the above case, Lloyd’s of London refused to pay the claim, and some individuals were indicted.

**Reinsurance**

Another form of money laundering using non-life insurance involves reinsurance. The relevant reinsurers normally would have connections, either through influence or through affiliation, to the money launderer.

---

13. A person who investigates, quantifies, and certifies losses.
Examples of money laundering and the financing of terrorism using reinsurance are:

- Establishment of bogus reinsurers to launder the proceeds of crime
- Establishment of bogus insurers to place the proceeds of crime with legitimate reinsurers
- Deliberate placement by the insurer of the proceeds of crime with reinsurers to disguise the source of funds.

Figure 2 shows one way in which money laundering might be done using reinsurance. In this case, the criminals have used some of the proceeds of crime to purchase both a legitimate non-financial business and a reinsurer. The non-financial business purchases insurance against various esoteric risks from a legitimate insurance company. The insurance company, which is uninterested in retaining any of these risks, nevertheless has agreed to write the insurance policies and fully reinsure them under a fronting arrangement with the reinsurer. The insurance company’s reward for participating in the process is a guaranteed fronting fee of 7.5 percent of premiums, which is attractive to its management in light of the fact that it has retained no insurance risk.

Since there is little or no insurance risk under the policy, the reinsurer earns large profits on the transaction, which it could return directly to its owners, the criminals. In the example, the trail of funds is further disguised by layering, using a second reinsurer, also tied to the criminals, to which the first reinsurer retrocedes business.
LIFE INSURANCE

It should be noted that there are several types of life insurance. The products can vary both in the form of the payment of the premium—single, or regular ongoing—and the extent to which they provide coverage or are oriented towards investment.

Because of their investment nature, unit-linked policies and the sale of second-hand endowment policies are the contracts that are more subject to abuse and are the reason for many of the following guidelines. These guidelines may not necessarily be applicable to other types of life insurance, such as term life, group life, and credit life (see IAIS Glossary). If there is no built-up surrender value, and payments are made only after death, the last three have a remote chance of misuse.

Examples of the types of contracts that are particularly attractive as vehicles for laundering money are single premium investment policies:

- Unit-linked single premium contacts
- Purchase of annuities
- Lump sum top-ups to an existing life insurance contract
- Lump sum contributions to personal pension contracts.

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 to others—possibly against payment—before maturity or surrender to benefit from any insurer payments to the beneficiary. A policy might be used as collateral to purchase other financial instruments. These investments may be merely one component of a sophisticated web of complex transactions and often will have their origins elsewhere in the financial services system.

If, for instance, the criminal uses the most common form of money laundering—a single premium life insurance policy—the money launderer will look to take back the monies by early surrender or by way of a fraudulent claim.

Whether from the life sector or the non-life sector, suspicious transactions always should be reported. However, some of the guidance notes mentioned above (see also “IAIS Guidelines” below) may not be appropriate when an insurer is contracting for most types of non-life insurance business. The insurance supervisor must realize that these notes are for guidance only, and judgment should be used to assess which are applicable in each circumstance.

Insurance intermediaries

Throughout this module, “insurance entity” is used to include insurance agents, sub-agents, and insurance brokers. Part of the vulnerability of the insurance sector is due

---

14. Second-hand endowment policies are investment-type endowment policies in which the beneficiary has sold the right to the proceeds to a third party prior to maturity. The purchaser must take over the liability for premium payments.
to the extensive use of such intermediaries. Insurance intermediaries—independent or otherwise—are important for distribution, underwriting, and claims settlement. They often are the direct link to the policyholder. Therefore, intermediaries should play an important part in anti-money laundering and preventing the financing of terrorism.

When introducing clients to insurance companies, the insurance entity should decide how much reliance should be placed on the work of intermediaries, bearing in mind that the ultimate responsibility is with the insurer or reinsurer. Past experience clearly shows that some insurance intermediaries have not always taken their anti-money laundering responsibilities seriously enough. Some intermediaries have been known to have been created specifically to assist with the criminal activities and launder money. The same principles that apply to insurers generally should apply to insurance intermediaries.

**Concealment of criminal interests within legitimate business**

Section A described how the 1920s mobsters in the United States used laundromats as legitimate businesses to assist in the laundering of their dirty monies. Nearly any type of business that has a turnover based on cash receipts or deals in valuable, liquid products can assist the owner to launder dirty monies. Recent examples have involved restaurants, diamond agents, fine art dealers, philately dealers, and even insurance brokers and agents.

The establishment or purchase of a legitimate trading or financial services company is central to many methods of laundering.

Bertolt Brecht wrote, “If you want to steal, then buy a bank.” He should have continued by saying, “If you want to be really clever, then buy an insurance company, too.”

An organized crime group could, for example, be based and own a bank in South America, and own a series of restaurants and a life insurer in Europe. The laundering process could be effected through one or all of the above entities. The proceeds of crime

---

**Figure 3. Money laundering using different parties**

![Diagram of money laundering using different parties](Image link)

- **Organized crime group**
  - **South American licensed bank**
    - Controls and adds criminal funds to takings
  - **European life insurer (may or may not be affiliated)**
    - Takes out policies
  - **European restaurants**
    - Controls and deposits with

- **Integration**
could be directly invested in the European restaurants or used to purchase insurance policies with a European life insurer. They might also be layered, by first channeling them through the group’s South American bank. Eventually, clean funds are returned to the group, for example, in the form of surrender benefits from the life insurer and dividends from the bank and the restaurants.

The life insurer in this example may or may not be affiliated with the organized crime group. This is one of the important reasons that great emphasis is placed on due diligence, or “fit and proper tests” on individuals concerned with the ownership and management of insurers. These tests are important both at the application stage and when any subsequent changes are made. See also ICP 7:

**ICP 7—Suitability of persons:** The significant owners, board members, senior management, auditors, and actuaries of an insurer are fit and proper to fulfill their roles. This requires that they possess the appropriate integrity, competency, experience, and qualifications.

In the case of significant owners and key functionaries such as board members, senior management, auditors, and actuaries, fit and proper requirements relate to the persons and their financial soundness. A significant owner is defined as a person (legal or natural) who, directly or indirectly, alone or with an associate, exercises control over the insurer. The main responsibility for assessing the fitness and propriety of key functionaries lies with the insurers themselves.

The supervisory authority should be satisfied that significant owners and key functionaries have the requisite levels of competence for their roles. It also should ascertain whether they have the appropriate ability and integrity to conduct insurance business, taking account of potential conflicts of interests.

A wide range of businesses can be and are used in money laundering. For example, in late 2003, the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC) added 39 businesses acting as front companies for the Cali drug cartel, based in Colombia—and 95 individuals associated with the cartel and its activities—to its list of Specially Designated Narcotics Traffickers (SDNTs). The U.S. Treasury stated:

“Through a network of pharmaceutical businesses, the cartel has laundered money and has penetrated the Colombian economy. These front companies form a vital part of the Cali cartel’s international money laundering network. This action froze their assets and prohibited financial and commercial transactions with U.S. nationals. Included among the 39 businesses designated were Interfarma/Jomaga de Costa Rica in Costa Rica, Latinfarmacos and Espibena in Ecuador, Colfarma

15. From the IAIS Glossary, “Fit and proper requirements are those personal requirements concerning the honesty, solvency and appropriateness of an individual to hold shares or office in an insurer.” See also the IAIS paper, “Fit and Proper Principles and Their Application,” www.iaisweb.org/02fit.pdf. At the time of writing this module, the “fit and proper” paper is due to be revised and to be presented at the IAIS annual general meeting in the last quarter of 2006.
Peru in Peru, Premier Sales in Panama, and C.A. V.J. Corporation in Venezuela, all affiliated with the international drug distribution of Cali cartel pharmaceutical laboratories Pentacoop and Farmacoop on the SDNT list.”

Also named were numerous financial fronts in Colombia, such as Coopdisan, Drofarco, and Incommerce, which were created by the Cali cartel using trusted corporate officers to provide bank account services to its business fronts. Inversiones Carfeni and two internet companies in Spain as well as Ash Trading, Inc. in the United States also were named.

The international network of the 39 Cali cartel fronts named joined 340 other Colombian drug cartel businesses on the SDNT list. The list includes Cali cartel businesses Copservir, and its Drogas La Rebaja drugstore chain and Credirebaja charge card, the Obursatiles stock brokerage and Internacional de Divisas money exchange house, the Cosmepop cosmetics company, the America de Cali professional soccer team, as well as consulting, investment, financial, construction, real estate, agricultural, and distribution firms. These companies demonstrate the diversity of trades used to launder money.
C. Addressing the vulnerabilities

The FATF is the primary international body responsible for AML/CFT, but the IAIS also plays an important role in describing measures that insurers, intermediaries, and their supervisors can take to address these vulnerabilities.

The IAIS has given high priority to anti-money laundering (AML) and combating the financing of terrorism (CFT). IAIS considers the FATF Recommendations to be the standards in the field of AML and CFT for insurance entities and insurance supervisors. So long as it is built on these recommendations, the IAIS feels there is room for specific guidance for insurance entities and insurance supervisors, hence the issuance of the “guidance notes” already mentioned.

FATF 40 Recommendations and 9 Special Recommendations regarding terrorist financing

The Financial Action Task Force (FATF) was established by the G-7 Summit in Paris in July 1989 to examine measures to combat money laundering. In 1990 FATF issued Forty Recommendations to address this problem. The Recommendations were revised for the first time in 1996 and then again in June 2003 to respond to changes in money laundering methods, techniques, and trends. In October 2001, FATF expanded its mandate and issued Eight Special Recommendations to deal with the issue of terrorist financing, and in 2004 added a ninth Special Recommendation.

The IAIS has acknowledged the various FATF Recommendations as the standards so far as these are applicable to life insurance business and supervision. However, these recommendations do not yet address non-life issues. The recommendations most relevant to the insurance sector are summarized in appendix II of this module.

It should be noted especially that FATF always refers to “financial institutions” and indicates that, from an insurance perspective, these are insurers and insurance intermediaries underwriting or placing life insurance and other investment-related insurance. Thus, the Task Force does not yet address other types of life insurance or any type of non-life insurance business.

16. According to FATF Recommendation 25, the “competent authorities should establish guidelines, and provide feedback which will assist financial institutions and designated non-financial businesses and professions in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions.”

17. At the time of this writing, FATF comprised 31 governments and 2 regional organizations that represent major financial centers in all parts of the globe. The Task Force members’ delegations are drawn from a wide range of disciplines, including experts from the Ministries of Finance, Justice, Interior, and External Affairs; financial regulatory authorities; and law enforcement agencies. The IAIS is an observer to FATF. There are FATF-style and FATF-supported regional bodies in Eastern and Southern Africa, Asia/Pacific, Caribbean, Europe, and South America. www.fatf-gafi.org.


ICP 28

The ICPs were revised in October 2003, and ICP 28 (along with ICP 27: Fraud) was one of several new ICPs. The full text of ICP 28 with the explanatory notes and essential criteria appears in appendix I.

ICP 28—Anti-money laundering, combating the financing of terrorism (AML/CFT): The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment-related insurance, to take effective measures to deter, detect and report money laundering and the financing of terrorism consistent with the Recommendations of the Financial Action Task Force on Money Laundering (FATF).

Note that ICP 28 makes an explicit link to the FATF Recommendations. Essential criterion a further states, “The measures required under the AML/CFT legislation and the activities of the supervisors should meet the criteria under those FATF Recommendations applicable to the insurance sector.” ICP 28 and its criteria provide three main areas in which action is required:

- Legal framework
- Measures to be taken by insurers and intermediaries
- Measures to be taken by the insurance supervisor and other authorities.

AML and CFT legislation

In most jurisdictions that have the relevant legislation, these laws require individuals to report not only knowledge of the crime but also suspicions of any money laundering offense. All persons, even those tangentially involved, usually are covered by the legislation, from the banker and lawyer to the waitress who inadvertently might have overheard a conversation. Of course, this requirement includes all insurance company and insurance broking company staff, not just the senior management.

Governments are making the AML and CFT legislation tougher than many other pieces of legislation, having in some cases sentences with no remissions. In other words, an individual sentenced to 15 years’ imprisonment must serve all of the time.

The legal framework may impose both direct and indirect reporting duties. In the case of a direct duty, the law stipulates that suspected cases must be reported. The indirect system provides that a financial institution could be found guilty of money laundering unless it has filed a suspicious transaction report to the Financial Intelligence Unit. The FIU is a special unit, usually made up of police and customs officers, formed
to investigate financial crimes, including money laundering. FATF promotes the first method.

Legislation also must enable the supervisors and other authorities to take appropriate action. Essential criterion b requires:

“The supervisory authority has adequate powers of supervision, enforcement and sanction to monitor and ensure compliance with AML/CFT requirements. Furthermore, the supervisory authority has the authority to take the necessary supervisory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in an insurer or an intermediary.”

Essential criterion c goes on to state:

“The supervisory authority has appropriate authority to co-operate effectively with the domestic FIU and domestic enforcement authorities, as well as with other supervisors both domestic and foreign, for AML/CFT purposes.”

Responsibilities of insurers and intermediaries

The main principle in anti-money laundering legislation is that institutions must know their customers (often referred to as KYC, or “know your customer”). To do so, they must perform customer due diligence (CDD), the process of verifying the identity and ensuring the fitness and propriety of a prospective or existing policyholder. Adequate due diligence on new and existing customers is essential. It is exactly the main principle of good underwriting. For sound business practice and proper risk management, insurers already should have in place controls to assess risk and check business relationships.

Because customer due diligence is a business practice suitable not only to assess commercial risk but also to prevent money laundering and financing of terrorism, control measures should be linked to these pre-existing practices. Thus, in theory, the requirements of anti-money laundering are the same as those used to make optimal profits. A life insurer needs to know the age, sex, identity, state of health, lifestyle, geographic location, and life expectancy of an insurance applicant. Examples of the extra requirements to “know your customer” for anti-money laundering purposes are the proof of identity, the reasons for wanting to take out the policy, 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 third parties, and any bearer arrangements.
The need to perform CDD is addressed by essential criterion e, which further describes the responsibilities of insurers and intermediaries:

“The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to comply with AML/CFT requirements, which are consistent with the FATF Recommendations applicable to the insurance sector, including:

- Performing the necessary customer due diligence (CDD) on customers, beneficial owners, and beneficiaries
- Taking enhanced measures with respect to higher-risk customers
- Maintaining full business and transaction records, including CDD data, for at least 5 years
- Monitoring for complex, unusual large transactions, or unusual patterns of transactions that have no apparent or visible economic or lawful purpose
- Reporting suspicious transactions to the FIU
- Developing internal programs (including training), procedures, controls and audit functions to combat money laundering and terrorist financing
- Ensuring that their foreign branches and subsidiaries observe appropriate AML/CFT measures consistent with the home jurisdiction requirements.”

It should be understood that there are important financial considerations for insurance entities in complying with anti-money laundering principles. Typically, legislation requires insurers to:

- Initiate procedures for verifying client identities (CDD)
- Initiate record-keeping procedures for CDD and the transactions
- Set up internal reporting procedures for suspicions, including the appointment of a Compliance Officer/Money Laundering Reporting Officer
- Train employees in the relevant legal requirements and the required procedures.

The costs of instituting the above—revising computer programs, producing new manuals, and being subjected to targeted AML supervisory and internal on-site inspections and internal audits—can be significant. However, the CDD (initial and ongoing) is important from the underwriting and reputational aspects as well as the AML aspect. Thus, in the best-managed insurance entities, most of these cost requirements already exist, even if there were no additional AML-related expenses.

Insurance entities are expected to appoint Compliance Officers to lead their AML/CFT efforts. In-depth training concerning all aspects of the relevant legislation and guidance and AML/CFT policies and systems will be required for the Compliance Of-
In addition, the Compliance Officer will require extensive initial and continuing instruction on the validation and reporting of suspicious transactions and on the feedback arrangements. The person also should keep a register of all reports made to the law enforcement authority and all reports made to her or him by key staff.

Factors that may increase or help to mitigate risk are dealt with in the legislative frameworks of various jurisdictions. In some jurisdictions, short-term life insurance contracts of, for example, three years, might be allowed, while in others this is either not legally possible or non-existent because of fiscal prohibitions. The same applies for the early surrender of the policies.

Another factor is the possibility of changing the designated beneficiaries without knowledge or consent of the insurance companies. In some jurisdictions, this could be possible, while in others it is not common practice or not legally possible.

**Responsibilities of supervisory authorities**

To facilitate the prevention and detection of money laundering in insurance entities, it is important that insurance supervisory authorities have adequate powers, including the authority to:

- Conduct on-site compliance visits, including the ability to inspect all books and records of the insurance entity and should be able to impose adequate administrative sanctions for failure to comply with such requirements;
- Exchange information with national and international law enforcement authorities, international insurance supervisors, other financial services supervisors and other investigative and supervisory authorities;
- During the licensing process, take account of the extent to which an insurance entity proposes to have anti-money laundering measures in place. Such information should be confidential and not able to be disclosed to third parties. Persons reporting, in good faith, suspicions that a person is laundering money should receive immunity from suit for their comments; and
- File a suspicious transaction report when relevant information is found, for example, during an on-site visit, and to have protection from suit for filing the report in good faith.

However, it is not enough that the supervisory authorities have adequate powers. They also must have the resources and capabilities to implement these powers and then exercise their authority as appropriate. Essential criterion d states:

“The supervisory authority devotes adequate resources—financial, human and technical—to AML/CFT supervisory activities.”
Furthermore, as mentioned above, essential criterion e calls upon the supervisory authority to require compliance by insurers and intermediaries. Finally, the power to cooperate with other authorities is essential to the proper functioning of an AML/CFT regime.

**IAIS Guidelines**

In 2002 the IAIS issued “Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities.” This document has been redrafted by the IAIS Insurance-Fraud Sub-Committee. This document provides additional, more detailed, information on the issues discussed above, such as:

- The need to develop clear customer acceptance policies and procedures taking account of the various risk factors involved, including the types of products and customer profile
- Implications for the insurers
- Establishing a business relationship
- Timing needs of identification and verification
- Transactions and events in the course of a business relationship
- Methods of identification and verification of individuals, companies, partnerships, and other institutions. These may include high-risk customers and politically exposed persons
- Reliance on intermediaries and third parties.

All of the above are relevant to CDD. In addition, the guidance notes detail:

- Reporting suspicious transactions to the FIU, including various examples and the offense of “tipping-off” (knowingly or unknowingly alerting the criminal or associates that the insurance entity is suspicious and will file a report)
- The obligations of the insurance supervisory authority
- AML/CFT training needs
- Various examples/case studies.

At a minimum, the guidance notes apply to those insurers and intermediaries that offer life insurance products or other investment-related insurance. The IAIS is concerned to ensure that the potential risks to the non-life insurance sector also are considered by insurance supervisors and insurance entities and that AML/CFT guidance and policies cover these risks. The FATF Recommendations apply to insurers and intermediaries offering life insurance and other investment-related insurance. Any decision to requirements beyond the scope of the FATF Recommendations should be based on

18. www.iaisweb.org
a thorough analysis of the risks of money laundering or terrorism financing for these types of insurance.

The IAIS indicates that there is a need for finding a balance between the fact that guidelines on the facilitating of prevention and detection of money laundering must be sufficient and clear, and the desire that the guidelines not be an unnecessary burden for the insurance entities to administer. The requirements in the internal guidelines, training programs, and specific internal structure must meet the needs of the insurance entity in question. The insurance supervisory authority’s requirements should take into account the size and nature of the particular insurance entity.

It must be noted that the guidelines are neither mandatory nor exhaustive. The IAIS recognizes that anti-money laundering matters are dynamic and that the guidelines will need regular updating.

**Meeting the challenges**

As risk escalates and the cost of compliance increases, insurance supervisors face enormous challenges. Increasingly, regulators are looking for evidence of risk-based underwriting, risk control, market conduct compliance, as well as fraud and AML/CFT controls.

From the viewpoint of an insurance entity, key to meeting all of the above challenges is the ability to “know your customer,” including his or her underlying business.

It has been suggested that the following will improve the AML/CFT objectives, which are the detection, investigation, and prosecution of perpetrators of ML/FT:

- Strengthen national and international cooperation and coordination among the many agencies involved
- Ensure that, in regulatory bodies, in other agencies, and within the insurance industries, there are sufficient human and financial resources available, with proper systems and procedures in place, using all relevant new technologies For instance, software is available that can analyze financial behavior and highlight unusual or suspicious activities
- Train industry and the public to be aware of the threats from ML/FT
- Ensure FATF 40 + 9 recommendations are developed further within the insurance area and are implemented consistently throughout the world
- Share the proceeds of seized assets with the national and international agencies involved in the investigations.
Exercise

On one or two pages, prepare a checklist for a forthcoming anti-money laundering onsite inspection of a life insurer that writes life insurance and pension contracts domestically and in foreign jurisdictions. The checklist should include actions that you want the insurance supervisory staff to perform and questions for the appropriate staff of the insurer.
D. References

Although the following sites were active at the time of writing, they may have expired by the time you read this module. If so, or if you come across more useful sites, please inform the World Bank, with a copy to IAIS (see their websites below for contact details).

Publications


Websites cited in the text


www.fatf-gafi.org

www.fincen.gov

www.iaisweb.org/02fit.pdf

www.imolin.org. International Money Laundering Network. An essential read, this site includes a database of AML legislation throughout the world, an electronic library, and a calendar of conferences and links to other relevant sites. IMoLIN was set up by the leading international organizations involved in the fight against money laundering.


www1.oecd.org/fatf/

www.ogis.net

www.un.org

Additional AML/CFT websites, in order of usefulness

www1.worldbank.org/finance/html/amlcft/referenceguide.htm. The Comprehensive Reference Guide to AML/CFT. This is a very well organized, essential-to-read site
split into three parts: (1) problem and international response; (2) elements of an AML/CFT framework; and (3) role of the World Bank.


www.ex.ac.uk/~RDavies/arian/scandald/launder.html. This site contains useful money laundering links to many relevant sites. It includes the following delightful quote from Nest of Vipers by Linda Davies: “The money screamed across the wires, its provenance fading in a maze of electronic transfers, which shifted it, hid it, broke it up into manageable wads which would be withdrawn and redeposited elsewhere, obliterating the trail.”


www.state.gov. U.S. Department of State, then search for “money laundering,” then use an advanced search. Contains information from a U.S. perspective.

www.fsround.org. The Financial Services Roundtable. A U.S. association representing 100 of the largest integrated financial services companies. This site contains interesting arguments against the proposed AML/CFT regime in the U.S. including comments on why certain insurance classes should be exempt.

www.freedomandprosperity.org/Papers/rahn01-30-01/rahn01-30.01.shtml. Why the war on money laundering is counterproductive. Read the other side of the story.
Appendix I. ICP 28

ICP 28  Anti-money laundering, combating the financing of terrorism (AML/CFT)
The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to take effective measures to deter, detect and report money laundering and the financing of terrorism consistent with the Recommendations of the Financial Action Task Force on Money Laundering (FATF).

Explanatory note

28.1. In most IAIS member jurisdictions, money laundering and financing of terrorism are criminal acts under the law. Money laundering is the processing of criminal proceeds to disguise their illegal origin. The financing of terrorism involves the direct or indirect provision of funds, whether lawfully or unlawfully obtained, for terrorist acts or to terrorist organizations.

28.2. Insurers and intermediaries, in particular those insurers and intermediaries offering life insurance or other investment related insurance could be involved, knowingly or unknowingly, in money laundering and financing of terrorism. This exposes them to legal, operational and reputational risks. Supervisory authorities, in conjunction with law enforcement authorities and in co-operation with other supervisors, must adequately supervise insurers and intermediaries for AML/CFT purposes to prevent and counter such activities.

Essential criteria

a. The measures required under the AML/CFT legislation and the activities of the supervisors should meet the criteria under those FATF Recommendations applicable to the insurance sector.\(^{19}\)

b. The supervisory authority has adequate powers of supervision, enforcement and sanction to monitor and ensure compliance with AML/CFT requirements. Furthermore, the supervisory authority has the authority to take the necessary supervisory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in an insurer or an intermediary.

c. The supervisory authority has appropriate authority to co-operate effectively with the domestic Financial Intelligence Unit (FIU) and domestic enforcement agencies.

\(^{19}\) See FATF Recommendations 4–6, 8–11, 13–15,17,21–23, 25, 29–32 and 40 as well as Special Recommendations IV, V, VII and the AML/CFT Methodology for a description of the complete set of AML/CFT measures that are required.
authorities, as well as with other supervisors both domestic and foreign, for AML/CFT purposes.
d. The supervisory authority devotes adequate resources—financial, human and technical—to AML/CFT supervisory activities.
e. The supervisory authority requires insurers and intermediaries, at a minimum those insurers and intermediaries offering life insurance products or other investment related insurance, to comply with AML/CFT requirements, which are consistent with the FATF Recommendations applicable to the insurance sector, including:

- Performing the necessary customer due diligence (CDD) on customers, beneficial owners and beneficiaries
- Taking enhanced measures with respect to higher risk customers
- Maintaining full business and transaction records, including CDD data, for at least 5 years
- Monitoring for complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose
- Reporting suspicious transactions to the FIU
- Developing internal programs (including training), procedures, controls and audit functions to combat money laundering and terrorist financing
- Ensuring that their foreign branches and subsidiaries observe appropriate AML/CFT measures consistent with the home jurisdiction requirements.
Appendix II. Summary of selected FATF Recommendations

Appendix II is a summary of some of the FATF 40 Recommendations and 9 Special Recommendations. For the entire text, click on www.fatf-gafi.org, and locate the document within the site.

Specifically, FATF Recommendations 4–6, 8–11, 13–15, 17, 21–23, 25, 29–32, and 40 as well as Special Recommendations IV, V, VII, and the AML/CFT Methodology are important for insurance.

These recommendations provide measures to address money laundering and terrorist financing by:

- Prescribing that secrecy laws do not inhibit implementation of the FATF Recommendations (Rec. 4), for example, by ensuring that there are gateways to provide information to other national and international supervisors, regulators, and appropriate law enforcement agencies;
- Requiring insurers and intermediaries involved in life insurance or other investment-related insurance to perform the necessary customer due diligence (CDD);\(^{20}\);
- Requiring these insurers and intermediaries to take enhanced measures with respect to higher risk customers such as politically exposed persons (Rec. 6), for example, by obtaining up to date public information about vulnerabilities, lifestyles, and by accessing confidential information from international agencies, where possible;
- Requiring financial institutions to pay special attention to any money laundering threats that may arise from new or developing technologies (Rec. 8), for example, new forms of electronic money transfer;
- Permitting financial institutions under specific conditions to rely on intermediaries or other third parties to perform certain elements of the CDD process or to introduce business (Rec. 9), for example where these intermediaries are in the same jurisdiction and are regulated;
- Requiring financial institutions to maintain full business and transaction records, including CDD data, for at least 5 years (Rec. 10);
- Requiring financial institutions to monitor for complex, unusual large transactions, or unusual patterns of transactions, that have no apparent or visible economic or lawful purpose (Rec. 11);
- Requiring financial institutions to report suspicious transactions to the FIU (glossary—the FIU is the Financial Intelligence Unit, in some jurisdictions it is termed the Financial Intelligence Service. They are usually made up of police and customs officers who have expertise in financial services);
- Prescribing that financial institutions, their directors, officers and employees a) be protected by legal provisions from criminal and civil liability for breach of

---

20. IAIS Glossary: Customer due diligence is the process of making relevant and appropriate checks on customers and potential customers, and is part of the “know your customer” process.
any restriction on disclosure of information, if they report their suspicions in
good faith to the FIU, and b) be prohibited by law from disclosing the fact that a
suspicious transaction report (STR) or related information is being reported to
the FIU (Rec. 14);

• Requiring financial institutions to develop internal programs (including train-
ing), procedures, controls and audit functions to combat money laundering and
terrorist financing (Rec. 15);

• Requiring countries to ensure that effective, proportionate and dissuasive sanc-
tions are available to deal with failures to comply with anti-money laundering or
terrorist financing requirements (Rec. 17);

• Requiring financial institutions to give special attention to business relation-
ships and transactions with persons from countries which do not or insuffi-
ciently apply the FATF Recommendations (Rec. 21);

• Requiring financial institutions to ensure that their foreign branches and sub-
sidiaries observe appropriate AML/CFT measures consistent with the home ju-
risdiction requirements (Rec. 22);

• Prescribing that countries should ensure that financial institutions are subject to
adequate regulation and supervision and are effectively implementing the FATF
Recommendations (Rec. 23);

• Prescribing that the competent authorities should establish guidelines, and pro-
vide feedback to assist financial institutions in applying national measures to
combat money laundering and terrorist financing, and in particular, in detect-
ing and reporting suspicious transactions (Rec. 25);

• Requiring that supervisors should have adequate powers to monitor and ensure
compliance by financial institutions with requirements to combat money laun-
dering and terrorist financing (Rec. 29);

• Prescribing that countries should provide their competent authorities involved
in combating money laundering and terrorist financing with adequate financial,
human and technical resources (Rec. 30);

• Recommending that countries should ensure that policy makers, the FIU, law
enforcement and supervisors have effective mechanisms in place to co-operate
concerning the development and implementation of policies and activities to
combat money laundering and terrorist financing (Rec. 31);

• Recommending that countries ensure that their competent authorities can re-
view the effectiveness of their systems to combat money laundering and terrorist
financing systems by maintaining comprehensive statistics on matters relevant
to the effectiveness and efficiency of such systems (Rec. 32), for example, on the
number of disclosures, per company and also per sector; and

• Recommending that countries ensure that their competent authorities provide
the widest possible range of international co-operation to their foreign coun-
terparts and that there be clear and effective gateways to facilitate the exchange
of information relating to both money laundering and the underlying predicate offences (Rec. 40).

Special Recommendation IV requires financial institutions to file a report with the competent authorities if they suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations.

Special Recommendation V calls for the greatest possible measure of assistance between countries in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.

Special Recommendation VII requires financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or related message through the payment chain. Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).
Appendix III. Answer key

Exercise

On one or two pages, prepare a checklist for a forthcoming anti-money laundering onsite inspection of a life insurer that writes life insurance and pension contracts domestically and in foreign jurisdictions. The checklist should include actions that you want the insurance supervisory staff to perform and questions for the appropriate staff of the insurer.

When possible, insurance supervisory staff should verify that the answers given to the questions below are borne out in practice by inspecting any relevant documentation.

Supervisory staff should inspect a sample of files and assess that the “know your customer” procedures are in place and are adequate. The files selected should include contracts written directly and through intermediaries, for clients in various jurisdictions. Both active and terminated contracts should be reviewed.

Supervisory staff should look particularly at the geographic spread of policyholders and at the lapses in each area.

Suggested questions include:

- How is the insurer structured? How many people are employed by the insurer? What types of policies are written, for example, single and periodic premium; regular and unit-linked; endowment, whole-life, and term policies? What is the mix of business by gross premiums paid in the last 12 months, for each geographic area?
- Who are the compliance and money laundering reporting officers? Will there be any conflicts of interest with, for instance, remunerated sales targets? What are their qualifications? Are they sufficiently senior, and have they been given an independent status so that they cannot be overruled by directors? Do all staff members know who these officers are? Who within the organization is responsible for developing and updating AML/CFT policies, procedures, and controls? Have you studied where in the organization money laundering is most likely to occur? Can we have a copy of the study? When was the last review?
- Could we have a copy of the part of your procedures manual that covers policy, procedures, and controls on preventing, detecting, and reporting on suspected ML/FT? Do you ever allow exceptions to established procedures, and, if so, what form do they take, and who authorizes them? Have all staff seen this document and been trained in its use, and know their legal and moral responsibilities with regard to AML/CFT? Are all staff trained to identify suspicious transactions?
- How do you test the effectiveness of the AML/CFT controls?
- What systems do the MLRO (money laundering reporting officer) use to provide required information to management and to identify suspicious transactions? Are these systems satisfactory? Is there software in use that highlights
unusual transactions, such as policy top-ups, lapse rates, early surrenders? How regularly does the MLRO report generally on the area of responsibility and in what form does this report take? Can sanctions be imposed in the event that policies and procedures are breached?

- Are there electronic transactions? Can these compromise the policy, procedures, and controls?

- How do you “know your customers” if they are direct clients and also if they come through a broker, agent, sub-agent, and/or introducer? How are the intermediaries checked for fitness and propriety? Are the procedures effective for overseas clients? When considered necessary, do you require details of the source of the funds and source of wealth?

There will be a whole range of additional, subsidiary questions relating to verification of clients, the nature of which is indicated by the above text. For example:

- Do you rely on intermediaries to perform customer due diligence, or do you have independent tests?