Effects on Economic Development and International Standards

Workbook
Effects on Economic Development and International Standards

Workbook
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

The initial work for this training program was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 3a was further written and developed by Manuel Vasquez, International Monetary Fund. The draft was reviewed by John McDowell, the World Bank and Thomas Grahn, Financial Supervisory Authority of Sweden. Pedagogical guidance was provided by Sheila Jagannathan, and peer review was conducted by Emiko Todoroki, the World Bank. In 2007 and 2008, updates and review were provided by Klaudijo Stroligo, Cedric Mousset, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations” (2003) and “Special Recommendations on Terrorist Financing” (2005); and Paul Allan Schott, Reference Guide to Anti–Money Laundering and Combating the Financing of Terrorism, Second Edition, the World Bank, 2004.

Capacity Enhancement Program on Anti–Money Laundering and Combating the Financing of Terrorism

Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing. In this module the following key issues will be addressed:

1. Understanding money laundering and terrorist financing
   1.1 What is money laundering? 4
   1.2 How does money laundering occur? 5
   1.3 What is terrorist financing and how does it compare and contrast with money laundering? 7
   1.4 Where do laundering and terrorist financing operations take place? 11

2. The implications of money laundering and terrorist financing for development
   2.1 How do money laundering and terrorist financing affect the macroeconomy? 19
   2.2 How do money laundering and terrorist financing affect the rule of law? 20
   2.3 How do money laundering and terrorist financing affect the financial system? 20
   2.4 What are the effects of money laundering and terrorist financing on economic liberalization? 21
   2.5 What are the effects of money laundering on governance? 22

3. International standards and standard setters
   3.1 Why is there a need for an international framework to combat money laundering and terrorist financing? 23
   3.2 What are the international standards to fight money laundering and terrorist financing? What organization sets those standards? 23
   3.3 What is the FATF, what does it do, and who are its members? 24
3.4 What do the FATF Recommendations include? 26
3.5 Are there any other international bodies involved in fighting money laundering and terrorist financing? 28

4. Assessing compliance with international standards 40
4.1 Why assess compliance? 40
4.2 Who assesses compliance with the international standards? 40
4.3 Is there a standard method for assessing compliance? 40

At the end of Module 1, you will be able to
• understand what money laundering is and how it is similar to and different from terrorist financing;
• understand the basic terminology and give examples of how money is being laundered;
• achieve a general understanding of the international standards in this area;
• recognize the international participants in the fight against money laundering; and
• describe how compliance assessments take place and the methodology used for assessment.
How much do you know?

True or false?

1) Only drug dealers launder funds.
   a) True    b) False

2) The proceeds of any illegal activity could be subject to money laundering.
   a) True    b) False

3) Proof of a predicate offense is a prerequisite for a conviction of terrorist financing.
   a) True    b) False

4) Money laundering takes place only in developing countries.
   a) True    b) False

5) Although money laundering may occur through the banking sector, the securities industry is completely immune to money laundering.
   a) True    b) False

6) Financial Action Task Force (FATF)-Style Regional Bodies (FSRBs) are specialized organs of the United Nations dealing with terrorist financing.
   a) True    b) False

7) The FATF is the international standard setter for anti-money laundering and terrorist financing measures.
   a) True    b) False

8) Money laundering is an engine for economic and social development.
   a) True    b) False
9) Only the International Monetary Fund (IMF) and the World Bank may assess countries’ compliance with anti-money laundering international standards.
   a) True       b) False

10) Hawala systems are informal fund transfer systems.
    a) True       b) False

You will be asked the same questions at the end of this module. Let’s see how much you learned!

1.1. What is money laundering?
Mr. A is a drug trafficker who has a drug-trading business with a daily turnover of $100,000 in cash. One day Mr. A took $120,000 to a casino to buy chips/tokens. He stayed several days gambling with small amounts. Upon leaving the casino, he converted his chips/tokens in checks payable to third parties, which were then deposited in a securities firm. The money was later withdrawn and invested in a number of legitimate grocery shops owned by the trafficker and his cohorts.

**QUESTION 1.** Analyze the story above by asking yourself the following questions. Check the answers once you have responded.

1) What is the source of the funds?

2) How many transactions took place in the example above?

3) Did Mr. A always keep his money in cash?
4) Where did he finally invest his money?

QUESTION 2. The operation described above is a money laundering operation. Provide below a definition of money laundering.

1.2. How does money laundering occur?

Money is laundered in a number of ways. Broadly speaking, a complete money laundering operation is often analyzed using three essential stages, although the three stages is not a requirement to be considered as money laundering:

Placement: This is the first stage in which illicit funds are separated from their illegal source. Placement involves the initial injection of the illegal funds into the financial system or carrying of proceeds of crime, such as cash, across borders, among others. How?

The launderer could deposit the cash into a regulated financial institution, such as a bank or securities company. He or she could also buy expensive assets, such as cars, antiques, or jewelry with cash. Crossing the national borders with dirty cash without declaring it to the customs authorities could also be considered as the first stage of money laundering although there is no injection into the financial system yet.

Layering: After injecting the illicit funds into the financial system, laundering the funds usually involves creating multiple layers of transactions that further separate the funds from their illegal source. The purpose of this stage is to make it more difficult to trace these funds to the illegal source. How?

The launderer may buy or sell securities, precious metals, or other expensive assets. He or she may also wire the funds across the world through various accounts held in different banks, possibly by several shell companies operating under his control.

Integration: The final stage in a money laundering operation involves injecting the illegal funds into the legitimate economy. The funds now appear as clean and legitimate assets. The purpose of the integration of the funds is to allow the
criminal to use the funds without raising suspicion that might trigger investigation and prosecution. **How?**

The launderer may purchase an expensive house with a mortgage loan in which repayment is paid using the laundered money in a bank account. The launderer may also set up a business, such as a restaurant or a video rental shop, where the illegal funds could be injected into the business and reappear as fictitious profits or loan repayment. The launderer may also set up a web of front companies with fictitious import/export businesses and use false invoicing and fictitious transactions to integrate the funds as normal earnings from trade.

**QUESTION 3.** Looking at the scenario in section 1.1, can you identify the three stages of the described laundering operation? What methods did the launderer use at each stage?

Here is the Bank of Credit and Commerce International (BCCI) case, which is a good example of money laundering.

**Case study**  
The Bank of Credit and Commerce International

The story of the BCCI is one of complex criminality whereby bankers used their own bank to launder money. BCCI was founded in the early 1970s as the first multinational bank for the Third World. Its corporate structure was designed from the beginning to avoid effective banking regulation and supervision. The bank was first registered in Luxembourg and then in Grand Cayman, both jurisdictions with strong bank secrecy traditions. Further, the BCCI established the headquarters of its operation in England. The fragmentation of the corporate structure contributed to the difficulty in supervision. Similar patterns of compartmentalization could also be found in its auditing practices and in the strict practice of watertight Chinese walls separating the various operations of the BCCI.

This deliberately evasive structure of the BCCI allowed it to engage in dubious operations ranging from covering the bank’s losses, embezzlement, and personal enrichment of the staff, moving money secretly, fraud, and money laundering. To achieve its purposes, the BCCI relied on various methods, including mirror-image trading, front men, and off-balance-sheet accounting techniques. In 1988 the bank was indicted for drug money laundering, and several BCCI bankers were convicted in 1990 on counts of laundering drug proceeds. This was the beginning of the demise of the BCCI.

The role of the BCCI in the laundering of the corruption proceeds of Manuel Noriega, the former president of Panama, provides an example of its laundering activities. Appropriating the funds of the Panama National Guard for his personal use, Noriega deposited $23 million in BCCI accounts in Luxembourg and London between 1982 and 1986. In 1986, Noriega, with the help of the BCCI, started a laundering operation aimed at obscuring the paper trail linking Noriega to the embezzled funds. To achieve that, the money was transferred from the various accounts held by
1.3. What is terrorist financing and how does it compare and contrast with money laundering?

QUESTION 4. What is terrorist financing? Please select the answer you think is most appropriate.

a) It is a finance activity by terrorists. Therefore, all terrorists’ financial activities are considered terrorist financing. It has only to do with financial activities by terrorists.

b) It is financial support given to terrorists through laundering money. This is the only source of terrorist financing.

c) It is financial support given to terrorists. The source of money may be from both illicit and legitimate sources.

d) It is financial support given to terrorists by a governmental body and not from public sources.

After you attempt an answer, consider the following analysis:

Terrorist financing is the act of providing financial support to terrorists or terrorist organizations to enable them to carry out terrorist acts.

This definition is based on the internationally accepted definition of terrorist financing as provided by the United Nations (UN) International Convention for the Suppression of Financing of Terrorism (1999) and on Recommendation II of the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing and its Interpretative Note.
Article 2 of the International Convention for the Suppression of the Financing of Terrorism provides:

1. Any person commits an offense within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:

(a) An act, which constitutes an offense within the scope of and as, defined in one of the treaties listed in the annex;* or

(b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

2. [...]

3. For an act to constitute an offense set forth in paragraph 1, it shall not be necessary that the funds were actually used to carry out an offense referred to in paragraph 1, subparagraphs (a) or (b).

* The annex includes a list of all the international conventions that criminalize specific terrorist acts, such as the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1970) and the International Convention for the Suppression of Terrorist Bombings (1997).

For the purposes of FATF Special Recommendation II and this Interpretative Note the following definitions apply.

- **terrorist financing** includes the financing of terrorist acts, and of terrorists, and terrorist organizations

- **terrorist** refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist.

Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and (ii) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

**terrorist organization** refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Unlike criminal organizations, the primary aim of terrorist groups is non-financial. Yet, as with all organizations, terrorist groups require funds to carry out their activities. This simple fact—the need for funds—is key in fighting terrorism. Follow the money. Follow the financial trail. This is the core objective of all measures that aim to identify, trace, and curb terrorist financing. Take a look at the role of finance in determining the capacity and gravity of terrorist attacks.

The case of the 1993 attack on the World Trade Center provides evidence of both the importance of financing for terrorist groups and the importance of following the financial trail in investigating incidents of terrorism. According to the testimony of the then-FBI Director Louis Freeh before Congress in 1999, the terrorists were unable to achieve the destruction they originally intended because of shortage of funds. This limited their capacity to purchase explosive material sufficient to build a bomb of the size they intended. It also forced them to implement the operation ahead of the original schedule. These facts were revealed by Ramzi Yousef, who was captured and convicted as the mastermind behind the 1993 bombing. The investigative value of following the money trail is evident in the fact that the main evidential lead in the case stemmed from the attempt of the perpetrators to reclaim the deposit they paid to rent the truck that they used to transport the bomb to the site of the attack. This transaction set the police on the right track that eventually led to the identification of the perpetrators.

*(Testimony of Louis J. Freeh, director, FBI, before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, February 4, 1999.)*
But how do terrorists finance their activities? What is the source of their funds?

There is a recent trend in the methods used to finance terrorism. Terrorist financing has now become privatized. Previously, terrorism relied on the financial support of states, but state-sponsored terrorism has declined in recent years, and terrorists now rely increasingly on private sources to finance their operations.

Some of the major sources of terrorist financing include:
- Drug trafficking
- Extortion and kidnapping
- Robbery
- Fraud
- Gambling
- Smuggling and trafficking in counterfeit goods
- Contributions and donations
- Sale of publications (legal and illegal)
- Funds derived from legitimate business activities

**QUESTION 5.** What is the difference between the sources of terrorist funds and the sources of laundered funds?

**QUESTION 6.** What are some similarities between the processes used for money laundering and financing of terrorism?

**QUESTION 7.** Read the following hypothetical case and identify the sources that the terrorists used to generate their funds. How many layers did they create before delivering the funds to the terrorist organizations? Can you name three of the methods they used to hide the money trail?

---

QUESTION 8. Return to the question posed at the beginning of this section: What is terrorist financing? Reconsider your answer on the basis of the discussion.

a) It is a finance activity undertaken by terrorists. Therefore, only the terrorists’ financial activities are considered terrorist financing.

b) It is financial support given to terrorists through money laundering. This is the only source of terrorist financing.

c) It is financial support given to terrorists. The source of money may be from both illicit and legitimate sources.

d) It is financial support given to terrorists by a governmental body and not from the public.

You will learn more about terrorist financing and how to combat it in Module 6.

1.4. Where do laundering and terrorist financing operations take place?

QUESTION 9. Reexamine the BCCI case in section 1.2. How many jurisdictions were involved in the laundering of Panama strongman Manuel Noriega’s funds? Can you identify any particular characteristics of these jurisdictions?
Money laundering and terrorist financing are global crimes. Money launderers and financiers of terrorism internationalize their operations to achieve various objectives:

a) To avoid jurisdictions with strong regulatory and law enforcement frameworks
b) To take advantage of the constraints of communication and cooperation between regulators and law enforcement officers across national borders
c) To exploit regulatory and law enforcement weaknesses that characterize certain jurisdictions
d) To add layers to the transactions to make it difficult to follow the trail of the transactions

Money laundering and terrorist financing can exploit any jurisdiction, so no country is immune. You will find that these activities take place in both developed and developing countries.

Analysis shows that criminals, like legitimate business operators, consider the legal framework of a location when choosing a base for their operations. It is now well established that strong legal frameworks in the world’s major financial centers have pushed criminals to find other havens for their funds.

Jurisdictions with financial secrecy laws figure prominently in money laundering operations, especially at the layering stage. These jurisdictions are also sometimes referred to as financial havens or offshore financial centers. The BCCI case discussed in section 1.2 clearly shows the use of financial-secrecy havens for criminal purposes. It is important to note that offshore financial centers and financial-secrecy rules have legitimate uses within certain limits. Protection of business information is important for businesses and markets, but the regulatory and other relevant authorities must ensure that secrecy regulations are not abused.

**QUESTION 10.** Can you think of some reasons why legitimate business entities use offshore financial centers? List three below.

1. 
2. 
3. 

**QUESTION 11.** What are the main characteristics of a perfect financial haven?
The list of businesses that are vulnerable to money laundering and terrorist financing is growing. Examples of these businesses are:

- Cash-intensive businesses, such as bars and restaurants, are suitable for the placement of drug proceeds and the proceeds of other cash-based criminal activities.
- Trade in high-value items, such as expensive cars, antiques, and real estate provides another suitable vehicle for the laundering of funds.
- Banks and other nonbank financial institutions are particularly vulnerable because of the high volume of money and financial transactions and because they have access to the international financial system.
- Foreign exchange bureaus and remittance offices are also vulnerable because they are cash intensive and have access to the international financial system.
- Accountants, lawyers, notaries, and company formation agents have technical skills that are indispensable to highly sophisticated money laundering operations.

Although terrorist financiers use techniques that resemble those used by money launderers—and they may exploit the same channels of finance—certain businesses and activities are considered to be particularly vulnerable to exploitation by the former. These include nonprofit organizations and informal money transfer systems.

Module discussion

In your own country, where do you think money laundering takes place? In your opinion, is there any particular sector that is more vulnerable than others? Why?

In the BCCI case, you have seen how banks could be used for money laundering; let’s see how other sectors are used to launder illegitimate funds and to secretly pass money to terrorists.

Money laundering through securities firms

Mafia-related Organization O generated substantial amounts of money from various frauds. To launder the proceeds, Organization O executed a plan to feed large sums of money into a stock market. The first step was to deposit the money in a private bank in Country R, controlled by Organization O itself. Subsequently, these funds were used to purchase two publicly listed companies established in Country V; one of the companies was a stock brokerage and the other a small bank. Numerous small investors from abroad using false names purchased the shares of these two firms. None of the investors bought shares above a certain percentage of ownership that would trigger reporting under Country V’s laws.
Through a fictitious general shareholders’ meeting in which lawyers were involved, a new Board of Directors was appointed with people acting as front men for Organization O. Later on, the two companies applied for share increase and raised approximately US$42 million. In reality, the proceeds of the market manipulation along with the original funds were laundered by transferring the money from Country V to banks in Europe, from where it was transferred to Company N in Country Y, an offshore financial center. Company N owned marble mines in South Africa. The same money made the same circuit again, passing through banks in Europe and North America and reinvested in the brokerage company and the bank in Country V, thus stimulating foreign investment in the share capital of the two companies. This process of share buying and selling artificially raised the face value of the shares sixfold. The overpriced shares were then delivered to the members of Organization O. None of the operations above could have been possible without securities brokers who were complicit in knowledge and traded these shares.2

**Money laundering through the insurance sector**

Mr. L purchased marine property and casualty insurance for a phantom ocean-going vessel from a reputable insurance company through an intermediary. He paid large premiums on the policy and bribed the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. The money launderer requested that the claims be wire-transferred to bank accounts held by a third party. Some of the accounts were held in offshore financial havens. The well-reputed insurance company processed the claims promptly and wire-transferred the funds out of its bank accounts.3

**Money laundering online**

Mr. X is a rogue financier who accumulated substantial wealth by manipulating the securities markets. He placed his ill-gotten gains in an offshore financial center. His problem is that he cannot flaunt his wealth without raising suspicion. To display his wealth, he needs to have a good story to tell. He establishes an online company offering services payable through the Internet. Mr. X then purchases his own services and pays for them using credit and debit cards tied to accounts under his control, which are in the offshore center and contain his criminal proceeds. Mr. X then invoices the credit card company, which in turn forwards the payment for the service rendered. Mr. X can now have the lifestyle he has earned through his cost-efficient and thriving online business.4

---

Terrorist financing through charitable institutions

Organization P is a nonprofit organization. It had branch offices in different countries where it had cooperative development projects. Organization P had its headquarters in country X and a branch office in Country Y. Mr. T was in charge of Organization P’s branch office in Country Y. He was not on the payroll of Organization P’s headquarters. In his capacity as branch manager, he received donations from different people and international bodies to support development projects in remote parts of Country Y. The donors did not know the total amount of money collected. They were also not very effective in monitoring the implementation of the projects partly because of the location of the projects. Mr. T diverted the funds to a terrorist organization for carrying out terrorist activities.5

Terrorist financing through the informal fund transfer system

Mr. H runs a small business with annual total transactions of approximately $200,000. His private accounts showed total transactions of $3 million annually. It turned out that Mr. H’s business was “headquartered” in Country N for an international “underground bank” with “branches” in several Asian and European countries. Relying on family, ethnic, and business ties, he managed to transfer funds all over South Asia. While his informal money transfer system was used to transfer the remittances of workers in Europe to support family and relatives in Asia, it was also used to transfer funds between terrorist organizations and their operatives in Asia and Europe.6

**QUESTION 12.** Considering the case of “Money laundering through securities firms,” can you identify the characteristics of the securities market that make it vulnerable to money laundering?

**QUESTION 13.** In reviewing the case on “Money Laundering through the insurance sector,” it is evident that Mr. L has lost money on these transactions voluntarily. What did he achieve?

---

6 Hypothetical case stylized from different reported cases relating to the use of the informal money transfer system for money laundering and terrorist financing purposes.
QUESTION 14. Why is the insurance sector attractive to money launderers? If you are familiar with the insurance business, provide your personal analysis.

__________________________________________________________________________

__________________________________________________________________________

QUESTION 15. Name three characteristics of the Internet that make it a good medium for money laundering operations.

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

QUESTION 16. Concerning the case “Terrorist financing through charitable institutions,” what was the source of the funds Mr. T used to finance terrorism? How is that different from the source of the funds in the BCCI-Noriega money laundering case discussed in section 1.2?

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________

QUESTION 17. What does an informal money transfer system mean?

__________________________________________________________________________

__________________________________________________________________________

__________________________________________________________________________
What have you learned?

We have learned a number of facts about money laundering and terrorist financing that can help us understand their impact on development:

- Money launderers and terrorist financiers take advantage of the financial system, including differences between or among countries’ supervision, regulation, disclosure, and AML/CFT requirements. Although we did not go into the details, money launderers and terrorist financiers can also take advantage of designated non-financial businesses and professions (DNFBPs), such as casinos, real estate agents, dealers in precious metals and stones, lawyers, accountants, and trust and company service providers.
- Various methods are used to launder money and finance terrorism.
- Money laundering and terrorist financing allow criminals to defeat the efforts of law enforcement and escape the penal consequences of their acts.
- Money laundering allows criminals to retain the gains of their illegal activities and use it to achieve power and influence.
- Money laundering and terrorist financing enable criminals to finance their enterprises.
- Criminals and terrorists need the assistance and cooperation of otherwise legitimate players, such as bankers and lawyers, to process their funds.
In this section, we look at how money laundering and terrorist financing can affect a country’s macro economy, rule of law, financial system, economic liberalization, and good governance.

The managing director of the IMF described macroeconomic impact of money laundering in a speech:

“[.. ] While we cannot guarantee the accuracy of our figures—and you have certainly a better evaluation than us—the estimates of the present scale of money laundering transactions are almost beyond imagination—2 to 5 percent of global GDP would probably be a consensus range. This scale poses two sorts of risks: one prudential, the other macroeconomic. Markets and even smaller economies can be corrupted and destabilized. We have seen evidence of this in countries and regions which have harbored large-scale criminal organizations. In the beginning, good and bad monies intermingle, and the country or region appears to prosper, but in the end, Gresham’s law operates, and there is a tremendous risk that only the corrupt financiers remain. Lasting damage can clearly be done when the infrastructure that has been built up to guarantee the integrity of the markets is lost. Even in countries that have not reached this point, the available evidence suggests that the impact of money laundering is large enough that it must be taken into account by macroeconomic policy makers. Money subject to laundering behaves in accordance with particular management principles. There is evidence that it is less productive, and therefore that it contributes minimally, to say the least, to optimization of economic growth. Potential macroeconomic consequences of money laundering include, but are not limited to: inexplicable changes in money demand, greater prudential risks to bank soundness, contamination effects on legal financial transactions, and greater volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers.

Moreover, I should add that while, from the viewpoint of the Fund as a financial institution, I emphasize the economic costs, we must also remember the social and political dimensions of crime and related money laundering—the suffering

---

of the victims and the overall weakening of the social fabric and collective ethical standards. All of this lends urgency to anti-laundering efforts, which attack criminal activity at the most vulnerable point—where its proceeds enter the financial system.

But, does this mean that we should abandon the liberalization of the financial markets? This high-minded argument is often raised by those of our critics who believe that the IMF should halt its efforts to move its members away from control-based, toward market-based, financial systems because such systems open up possibilities for money launderers. Some have argued that keeping in place centralized credit allocation and foreign exchange control systems is necessary to identify money launderers—even if we now know that such systems are inimical to economic growth. However, I am reassured that Recommendation 22 of the FATF’s 40 Recommendations is very clear on this point: “Countries should...monitor the physical cross-border transportation of cash and bearer instruments—without impeding in any way the freedom of capital movements.” Information, rather than control of the transactions, is the key to the basic “know your customer” approach of the FATF. More generally, the value of adequate information to guide the supervision of financial markets has been made very clear by recent events in Southeast Asia. It is not just free financial markets that the IMF advocates, but also modern financial markets—in which there is a good measure of transparency and prudential regulation to ensure the fairness, soundness, and legality of the systems [. . . .]

2.1. How do money laundering and terrorist financing affect the macro economy?

We have seen how money launderers need to invest in legitimate businesses or assets to launder their funds. They often transfer money across jurisdictions to create layers of financial transactions to obscure the audit trail. Both practices have serious macroeconomic implications.

Money launderers choose their investments, not to obtain the highest rate of return but to avoid detection. The result is that they often put these large amounts of money in less-productive activities, as long as such activities provide opportunities of avoiding detection. This has implications for the efficiency and productivity of both domestic and world economies.

In addition, money launderers move their money in and out of jurisdictions, sometimes rapidly, to obscure the audit trail. The rapid movement of large amounts of money in and out of a country can destabilize small developing economies.

---

8 The reference to this Recommendation 22 is based on previous FATF 40 Recommendations of 1996 and differs from the current Recommendation 22 of the FATF 40 Recommendations (revised in 2003). The similar requirements are now addressed in the Special Recommendation IX.
QUESTION 18. Country A is an oil-producing country suffering from endemic corruption. Large amounts of government revenues are systematically appropriated and transferred out of the country. Country B is a neighboring country with good financial and communication infrastructure. As an aspiring offshore financial center, it has lax laws on the formation of companies and trusts. It also has a strong commitment to bank secrecy. The corrupt officials of Country A have developed a habit of transporting their funds to Country B and depositing their money in its financial sectors, as well as purchasing real estate. What do you think the impact of this massive injection of funds is on (1) asset prices and (2) exchange rates?

2.2. How do money laundering and terrorist financing affect the rule of law?

Establishing a legal system based on the rule of law is considered a precondition for economic development. That is because markets need reliable institutions to be able to function. Rule of law presumes that there is a transparent system of clear and certain rules that is applied consistently to all subjects. Money laundering and terrorist financing mechanisms allow criminals to defeat law enforcement and to escape the consequences of their acts. Pervasive money laundering and terrorist financing undermine the rule of law in the society.

2.3. How do money laundering and terrorist financing affect the financial system?

A well-functioning financial system is an important contributor to economic development. The use of the financial system to advance criminal purposes, such as money laundering and terrorist financing, undermines the function and integrity of the financial system. As the BCCI case in section 1.2 illustrated, controlling a bank is an effective way for international organizations to achieve their purposes. The BCCI case also illustrates the costs of allowing criminality to infiltrate financial institutions. Losses to depositors, destabilization of the financial system, and costs to the taxpayers are but the obvious and calculable costs of such activities. The other consequences of money laundering and terrorist financing on financial systems also cannot be ignored. For example, if a bank or another financial institution is closed down by authorities because of a high volume of seized or confiscated deposits of dirty money, or because sanctions are applied against the financial institution due to the commitment of money laundering or terrorist financing criminal offense, this can certainly have an enormous impact on the financial system in a certain country.
Criminals seeking to launder their funds and to finance terrorist activities engage in deliberate acts of corrupting bank officers and other financial market professionals, such as insurance and securities brokers. This corruption undermines the confidence in the financial market and spills over into other forms of criminality, such as fraud and extortion.

**Exercise**

Reread the two cases of money laundering in the securities and insurance sectors in section 1.4 and analyze the role played by the securities and insurance officers in the scheme. Were they knowing or unknowing participants?

Can you give examples from your country of collusion between financial market professionals and criminals?

---

**2.4. What are the effects of money laundering and terrorist financing on economic liberalization?**

It is now a widely held view that liberalization of a country’s economy and its integration into the global economy are important for economic development. Money laundering and terrorist financing undermine liberalization in the following ways:

First, countries that are suffering the outflow of funds or are concerned about the outflow of funds because of pervasive economic crime often try to impose capital controls to fence in funds and prevent them from leaving the jurisdiction. Second, countries concerned about the use of the financial system for money laundering and terrorist financing purposes may take measures to control financial dealings with jurisdictions that do not have adequate money laundering control policies. Third, countries that are viewed as weak in their control of money laundering and terrorist financing would suffer attracting investments whether direct or indirect investments. Fourth, use of trade to launder money (trade-based money laundering) impacts legitimate trades by necessitating authorities to be more vigilant in clearing goods at the customs.
These incidents restrict the liberal flow of funds and pose a regulatory burden on legitimate cross-border economic activity. Although the success of capital controls is debatable, the burden of prudential restrictions could be reduced through the harmonization of anti-money laundering and terrorist financing measures across the world.

2.5. **What are the effects of money laundering on governance?**

Corruption is a pervasive problem in many developing countries. It is now well established that good governance is a prerequisite for economic development. Government revenues badly needed in these countries for economic development often end up in bank accounts in major financial centers around the world. This could not be achieved without reliance on money laundering techniques and without complacent officers of financial institutions. A well-functioning anti-money laundering system makes it difficult for corrupt officials to expatriate their ill-gotten funds. It also allows such funds to be repatriated in cases where they have been deposited abroad. This is because anti-money laundering measures create channels of information that help to trace the fleeing funds. They also enable cooperation among law enforcement officers in different countries.

**QUESTION 19.** Corruption can take many forms. List the sources of illegal funds that a person who holds a prominent public position may try to launder.

---

---
3. Why is there a need for an international framework to combat money laundering and terrorist financing?

The cases we have discussed so far reveal that money laundering and terrorist financing are often cross-border activities. We also learned that criminals choose the place of their operations after assessing the risk of detection. The lower this risk, the better it is for criminals. This logic applies when laws and regulations or enforcement of those laws and regulations vary among jurisdictions. Achieving a degree of harmony among different jurisdictions has the potential to defeat money launderers and terrorist financiers by making all jurisdictions equally unfriendly to their operations. Adopting international standards is one way to coordinate and harmonize the laws against money laundering and terrorist financing.

QUESTION 20. Are you familiar with any other situations where countries must set standards and harmonize their laws and regulations to prevent abusers from taking advantage of countries’ differing rules and regulations?

3.2. What are the international standards to fight money laundering and terrorist financing? What organization sets those standards?

In 1989, the G7 summit established the Financial Action Task Force (FATF) to prevent money laundering. Its mandate was “to assess the results of cooperation already undertaken, in order to prevent the utilization of the banking system and financial institutions for the purpose of money laundering, and to consider additional preventive efforts in this field, including the adaptation of the legal and regulatory systems so as to enhance the multilateral judicial assistance.” The FATF began its work in Paris in 1990 and since then has produced the most comprehensive set of anti-money laundering standards; these are known as the FATF Forty Recommendations. As more countries accepted the FATF Recommendations, they became the global minimum standard for an effective anti-money laundering system. In 2001, the FATF introduced an additional set
of Eight Special Recommendations, addressing the special problems of terrorist financing. In 2004, the FATF added the ninth Special Recommendation, on cash couriers. This is why we now refer to the full set of FATF anti-money laundering and terrorist financing recommendations as the FATF 40 + 9 Recommendations.

The detailed analysis of this set of international standards will be set out in the more advanced modules. In this introductory module, you need to become familiar only with the basics of the standards. But before we do that, let’s learn a little bit more about the FATF.

3.3. What is the FATF, what does it do, and who are its members?

The FATF is an international task force that functions as an inter-governmental policy-making body with a specific purpose to establish international standards, and develop and promote policies, both at the national and international levels, to combat money laundering and terrorist financing. The FATF reviews its operations on a regular basis. On May 14, 2004, a Ministerial Meeting of FATF members made the decision to extend the FATF’s life for another eight years. The last review took place during 2007–08 as a mid-term review of the mandate of the FATF for 2004–12, and the revised mandate was published after the ministerial meeting of FATF members in April 2008 reaffirmed the revised mandate. The FATF has a small secretariat hosted by the Organisation for Economic Co-operation and Development (OECD) in Paris. See Appendix B for the FATF’s new mandate.

As of June 2008, the FATF had 34 members, including 32 countries and territories and 2 organizations. The original membership of the FATF was 16 members. In addition, the FATF has two observer countries and five associate members, consisting of five FATF-Style Regional Bodies (FSRBs) that fulfill certain conditions. See Appendix C for more about the FATF’s membership.

FSRBs are task forces with regional jurisdiction that are modeled on the FATF in their mandate, functions, and methods of operation. Currently there are eight functioning FSRBs for the Caribbean, Europe, Asia/Pacific, Eastern and Southern Africa, South America, Eurasia, the Middle East and North Africa, and Western Africa.

The FATF has four core functions:

1) Setting standards
2) Ensuring their implementation in its member countries
3) Studying the techniques and typologies of money laundering and terrorist financing
4) Conducting outreach activities that aim to spread the standards globally

Standard setting

The first product of the FATF was the first edition of the Forty Recommendations in 1990, which provided the first comprehensive international anti-money laundering framework. Throughout its history, the standard-setting function
continued to be very important. The Forty Recommendations were revised twice, first in 1996 and then most comprehensively in 2003. In addition, in 2001 the FATF mandate was expanded to cover terrorist financing and the FATF issued the Eight Special Recommendations dealing with the subject. In 2004, the FATF added the ninth Special Recommendation on cash couriers.

FATF standard-setting activities are not confined just to setting the general standard in the form of broad recommendations. In addition, the group continually issues Interpretative Notes and guidance on best practices, which, in fact, takes the process of harmonization to a deeper level.

The standard-setting role of the FATF received special reenforcement when the Boards of the World Bank and the IMF agreed to recognize the FATF Forty Recommendations as the appropriate standard for combating money laundering and to mandate that the institutions take steps to use the recommendations in the World Bank’s and IMF’s activities. This gave more impetus to the global reach of the FATF standards.

Ensuring Compliance

The FATF not only sets standards to combat money laundering and terrorist financing, but also implements rigorous internal review mechanisms that aim to ensure the compliance of countries with the standards. The FATF uses two types of review mechanism:

1) A self-assessment exercise based on a standard questionnaire that was designed by the FATF and used by its members to report on their anti-money laundering systems on an annual basis. The secretariat then uses the answers to compile reports on the level of compliance with the recommendations and on the specific successes and failures in each reporting country’s system.

2) A mutual evaluation process in which each country is evaluated by a team of experts drawn from other member countries. The team uses a standard questionnaire and is guided by a preset list of issues in assessing the level of the examined country’s compliance with FATF standards. The report is then discussed by the plenary and finalized. On the basis of the report, the assessed countries are to take certain measures to rectify shortcomings in their systems.

The FATF has conducted two full rounds of mutual evaluation. The first started in 1992 and was completed in 1995, and the second started in 1996 and was completed in 1999. The first round of evaluation focused on assessing the quality of the legal and regulatory framework by reference to the FATF Recommendations. The second round focused instead on the more difficult question of the effective implementation of anti-money laundering laws and regulations within the country concerned.

Since 1999, the FATF has carried out similar processes of mutual evaluation of new members. With this process completed, in 2004 the FATF launched a new full round of mutual evaluation of its members. In 1999, the FATF launched an
Module 1

initiative aimed at taking action against certain nonmember countries that had been assessed by the FATF to have deficiencies in their anti-money laundering systems. The initiative resulted in the publishing of a blacklist of countries designated as Non-Cooperative Countries and Territories (NCCTs). Between June 2000 and September 2001, 23 countries were designated as NCCTs and asked to modify their legal systems in accordance with the FATF Recommendations. Following amendments to their legal regimes, all 23 countries were removed from the list by October 2006.

**Studying techniques and typologies**

The third main role of the FATF is to provide a forum for sharing information on money laundering techniques and typologies and the best policies and measures to counter them. Through the group of multidisciplinary experts that meet in plenary sessions and in its various working groups, the FATF pools information on the state of the art in money laundering and terrorist financing and counter-measures. As part of this function, the FATF publishes an annual report on money laundering and terrorist financing typologies that draws on the experience of its member countries and member countries of some FSRBs.

**Outreach**

Communication and publicity should be sustained and further developed, in particular by reaching out not just to the public and governments, but also to parties affected by the FATF’s standards: financial institutions and certain designated non-financial businesses and professions (DNFBPs). For example, the president/secretariat could attend key meetings and forums of the private sector organizations to highlight the FATF’s work and receive feedback. Alternatively, there could be more focus on liaison mechanisms with associations or bodies representing such entities, subject to reasonable resource implications.

**3.4. What do the FATF Recommendations include?**

The FATF Recommendations include the minimum measures that countries should have in place within their criminal justice and regulatory systems, the preventive measures that financial institutions and some non-financial businesses and professions should adopt, and the measures for international cooperation.

The Forty Recommendations require countries to implement a basic set of measures:

- **Criminalization**: to criminalize money laundering and terrorist financing. While initially the focus was on drug proceeds, the definition of money laundering offenses has now expanded to include at least all serious offenses.
- **Provisional measures and confiscation**: to put in place measures to identify, trace, freeze, or seize, and, finally, to confiscate the illegal proceeds and funds of terrorists and of those who finance terrorism and terrorist organizations.
Customer due diligence: to impose duties on financial institutions and some non-financial businesses and professions to know their customers and to abolish the use of anonymous accounts. Obligations of additional care when dealing with persons holding a public function and in relation to cross-border correspondent banking also need to be put in place.

Record keeping: to impose obligations on financial institutions and some non-financial businesses and professions to keep records on all the transactions that they conduct.

Suspicious transactions reporting: to impose an obligation on financial institutions and some non-financial businesses and professions to report if they suspect that funds are the proceeds of criminal activity, or are related to terrorist financing, without alerting the clients.

Internal controls: to ensure that financial institutions and some non-financial businesses and professions adopt internal mechanisms that allow them to comply with the regulatory requirements.

Implementation: to create regulatory and supervisory agencies that are capable of implementing the international standard set by the Recommendations and to give them sufficient powers.

International cooperation: to put in place a system that allows it to cooperate with other countries on all issues related to money laundering and financing of terrorism, including formal and informal exchange of financial and law enforcement information, preservation and confiscation of assets, and extradition.

The Nine Special Recommendations require countries to implement a basic set of measures, which—when combined with the FATF Forty Recommendations on money laundering—set out the basic framework for detecting, preventing, and suppressing the financing of terrorism and terrorist acts. They include:

I. Ratification and implementation of UN instruments related to financing of terrorism
II. Criminalizing the financing of terrorism and associated money laundering
III. Freezing and confiscating terrorist assets
IV. Reporting suspicious transactions related to terrorism
V. International cooperation relating to the financing of terrorism, terrorist acts, and terrorist organizations
VI. Requirements for alternative remittance transfers
VII. Requirements for wire transfers
VIII. Requirements for nonprofit organizations
IX. Requirements for cash couriers
QUESTION 21. The FATF Recommendations are:

a) A set of best practices in the area of money laundering and terrorist financing control that countries should aspire to follow.

b) A set of minimum standards that countries need to achieve to have a sufficiently functioning anti-money laundering and counter-terrorism financing system.

c) A maximum set of obligations for countries to achieve to have a functioning anti-money laundering and counter-terrorism financing system.

QUESTION 22. The FATF Recommendations are developed for all countries, so all countries are expected to implement them.

a) Yes, all countries need to follow the FATF Recommendations.

b) No, countries that are not members of the FATF do not need to follow the Recommendations.

3.5. Are there any other international bodies involved in fighting money laundering and terrorist financing?

Four other types of organizations combat money laundering and terrorist financing by setting standards, developing technical understanding, facilitating international cooperation, and implementing the international standard:

- International organizations and bodies with wider mandates that have adopted initiatives in fighting money laundering and terrorist financing. These include the UN, the World Bank, the IMF, and the Basel Committee on Banking Supervision.

- FSRBs, which are task forces with regional jurisdiction that are modeled on the FATF in mandate, functions, and methods of operation.

- Regional organizations with wider mandates that have adopted initiatives against money laundering and terrorist financing. For example, the Organization of American States, the Council of Europe, and the Asian Development Bank (ADB).

- Groups of special players in the fight against money laundering and terrorist financing. For example, the Egmont Group, which is a network of financial intelligence units (FIUs).

Let's now learn a little more about each of the major participants in this global effort.

International organizations

The United Nations

The UN Office on Drugs and Crime (UNODC) coordinates the main efforts of the UN with regard to money laundering control and prevention. The UNODC implements the Global Program against Money Laundering (GPML), which is a
research and technical cooperation initiative that aims to increase the effectiveness of international efforts against money laundering. In addition to providing technical assistance to governments in the field, the GPML coordinates the International Money Laundering Information Network (IMoLIN) Web site and the Anti-Money Laundering Information Database (AMLID).

The IMoLIN was the product of a 1996 agreement among the leading international organizations involved in the fight against money laundering. It is a common Web site where information can be shared between national and international anti-money laundering agencies. It serves the global anti-money laundering community by providing information about national money laundering laws and regulations and country contacts for assistance. The information on IMoLIN is freely available to all Internet users, whereas AMLID is a secure database.

Since the events of September 11, 2001, the UN Security Council has assumed an active role in combating terrorism and gives special attention to the issue of combating terrorist financing (CTF). The Security Council issued Resolution 1373 (2001), which requires all UN member countries to take comprehensive measures to suppress terrorism. The resolution placed special emphasis on the area of financing of terrorism and all other forms of direct and indirect assistance. The resolution established the Counter-Terrorism Committee (CTC), which monitors the implementation of the resolution and assesses countries’ compliance through a procedure of self-assessment and reporting mechanisms. Resolution 1373 imposes binding obligations on all UN member countries with the aim of combating terrorism in all its forms and manifestations. The resolution requires the member countries to:

- deny all forms of financial support for terrorist groups (operational paragraph [o.p.] 1a, b, c, d);
- suppress the provision of safe haven, sustenance, or support for terrorists; (o.p. 2a, c, d, g, 3f, g);
- share information with other governments on any groups practicing or planning terrorist acts (o.p. 2b, 3a, b, c);
- cooperate with other governments in the investigation, detection, arrest, and prosecution of those involved in such acts (o.p. 2b, f, 3a, b, c);
- criminalize active and passive assistance for terrorism in domestic laws and bring violators of these laws to justice (o.p. 2e); and
- become party as soon as possible to the relevant international conventions and protocols relating to terrorism (o.p. 3d).

Several international instruments that are central to the fight against money laundering and terrorist financing were created under the auspices of the UN. These include:

- The UN Convention against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988). One of the most important contributions of this instrument is that it has provided what has become a globally
accepted definition of the offense of money laundering. The convention also contained detailed provisions on international cooperation.

- **The UN Convention against Transnational Organized Crime (2000)** is commonly referred to as the Palermo Convention. It is the first binding international instrument that deals with organized crime in a comprehensive manner. The convention has contributed significantly to the codification of anti-money laundering standards of prevention and control.

- **The United Nations Convention against Corruption (2003).** This convention is an important step in the fight against corruption. As the first comprehensive instrument in this regard, it places particular emphasis on taking profit out of crimes of corruption, a fundamental strategy for control and prevention. For this purpose, the convention deals comprehensively with the question of money laundering and codifies a comprehensive regime of prevention and control through regulation and criminalization. The convention also elaborates on measures to seize, confiscate, and recover the proceeds of corruption.

- **The International Convention for the Suppression of the Financing of Terrorism (1999).** This was the first international instrument to address the financing of terrorism. The definitions established by the convention provide the basis for the current international standard in this area. According to the Security Council Resolution 1373 and the FATF Special Recommendations, countries are now required to ratify this convention and ensure its effective implementation.

**The World Bank and the International Monetary Fund**

In July 2002, the Boards of the World Bank and the IMF made a decision to add the FATF Recommendations to the list of standards and codes that are relevant to the operational work of the Bank and the IMF, and from which Reports on the Observance of Standards and Codes could be prepared. This decision acknowledged the FATF Recommendations as an international standard for money laundering control and prevention and included an assessment of compliance with this standard in financial sector assessment programs that the Bank and the IMF carry out. Since then, the Bank and the IMF have expanded their involvement in anti-money laundering and terrorist financing efforts.

In April 2004 the Boards of the Bank and the IMF made a decision to endorse the continued involvement of the Bank and the IMF in fighting money laundering and terrorist financing, and adopted a more integrated and comprehensive approach to their work in this area. While the Bank and the IMF would continue to assess countries’ compliance with the standards, they would commit more resources to supplying technical assistance to help countries bring their systems into compliance with international standards. As part of their technical assistance efforts, the Bank and the IMF organized a Global Policy Dialogue Series that promoted awareness of money laundering and terrorist financing.
control and prevention. The Bank and the IMF also provided technical assistance to jurisdictions on a bilateral basis or through regional initiatives.

The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision was established in 1974 by the central bank governors of the Group of Ten countries. It meets in plenary form four times a year and has a number of technical working groups and task forces that meet regularly.

The committee’s members come from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States. Countries are represented by their central bank or by the authority with formal responsibility for the prudential supervision of the banking business where this is not the central bank.

The committee does not produce legally binding norms. Instead, it formulates broad supervisory standards and guidelines and recommends statements of best practice, in the expectation that individual authorities will take steps to implement them through detailed arrangements—statutory or otherwise—which are best suited to their own national systems. The purpose of the committee is to encourage convergence and approximation among countries’ supervisory approaches. It does not aim at achieving deep and detailed harmonization of rules.

The Basel Committee produced the first set of international principles for combating money laundering. This occurred in 1988, when the Committee issued its "Statement on the Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering." The statement sets out the basic principles of customer identification, which precludes assistance to criminals and encourages cooperation with law enforcement officers.

In October 2001, the Basel Committee published a detailed guidance paper on customer due diligence, looking at the best practices in this area from a wider prudential perspective as well as from an anti-money laundering perspective.9 Subsequently in February 2003, General Guide to Account Opening and Customer Identification10 was added to Customer Due Diligence for Banks.

The International Association of Insurance Supervisors

Established in 1994, the International Association of Insurance Supervisors (IAIS) promotes worldwide cooperation among insurance supervisors in setting standards for insurance sector supervision and enhancing coordination between insurance sector supervisors and other financial market supervisors. The IAIS has 180 members.

---

9 Basel Committee on Banking Supervision, Customer Due Diligence for Banks, October 2001.
In October 2003, the IAIS approved and issued the *Insurance Core Principles and Methodology*, which revised the core principles for the supervision of insurers. The Insurance Core Principle 28 requires insurance supervisory authorities to take effective measures to deter, detect, and report money laundering and financing of terrorism consistent with the FATF Recommendations.

In 2004, the IAIS issued *Guidance Paper on Anti–Money Laundering and Combating the Financing of Terrorism for Insurance Supervisors and Insurance Entities*. This document elaborated on the possibilities for, and methods of, money laundering in the insurance sector and the duties of both the supervisors and the supervised entities in fighting money laundering.

**The International Organization of Securities Commissions (IOSCO)**

IOSCO is recognized as the international standard setter for securities markets and its wide membership regulates more than 90 percent of the world’s securities markets. IOSCO promotes cross-border enforcement and exchange of information among the international community of securities regulators.

IOSCO’s objectives and principles of securities regulation include actions that supervisory authorities should take to minimize risk of money laundering in the sector. In 2002, IOSCO established a Task Force on Client Identification and Beneficial Ownership and issued a report in May 2004 entitled “Principles on Client Identification and Beneficial Ownership for the Securities Industry.” Subsequently in October 2005, *Anti-Money Laundering Guidance For Collective Investment Schemes* was issued to clarify application of global standards to the operation of collective investment schemes.

**FATF-Style Regional Bodies**

**The Asia/Pacific Group on Money Laundering**

The Asia/Pacific Group on Money Laundering (APG) was established in 1997. Its regional scope covers South Asia, Southeast Asia, and East Asia and the South Pacific with 38 member jurisdictions as of July 2008. The purpose of the APG is to facilitate the adoption, implementation, and enforcement of internationally accepted standards against money laundering and the financing of terrorism.

The functions of the APG include improving the understanding of money laundering and terrorist financing typologies in the region through systematic analyses of typologies, monitoring the implementation of international standards through processes of self-assessment and mutual evaluation, and providing technical assistance to member jurisdictions.

---

THE CARIBBEAN FINANCIAL ACTION TASK FORCE

The Caribbean Financial Action Task Force (CFATF) is the oldest FSRB. It was established in 1992 by a group of 30 countries of the Caribbean basin to ensure the proper implementation and enforcement of the international AML/CFT standards. Like other FSRBs, one of the core functions of the CFATF is to monitor the implementation of international standards by its member jurisdictions through processes of self-assessment and mutual evaluation. The CFATF also conducts technical analysis of money laundering and terrorist financing typologies in the region and publishes reports. In addition to implementing the FATF Recommendations, the CFATF also implements its own set of 19 recommendations, which are geared to address the peculiarities of the money laundering and terrorist financing phenomenon in the region.

THE COUNCIL OF EUROPE SELECT COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI–MONEY LAUNDERING MEASURES

The Council of Europe Select Committee of Experts on the Evaluation of Anti–Money Laundering Measures (MONEYVAL) was established as the PC-R-EV in 1997 by the Committee of Ministers of the Council of Europe, as a subcommittee of the European Committee on Crime Problems of the Council of Europe (CDPC). Its main purpose is to monitor the implementation of anti-money laundering and countering financing of terrorism standards in Council of Europe member countries that are not members of the FATF. In 2002, the PC-R-EV formally changed its name to MONEYVAL. Currently it has 30 members (28 permanent members and 2 temporary members). As do other FSRBs, MONEYVAL conducts mutual evaluations of its members and reviews members’ self-assessment exercises. MONEYVAL has concluded two rounds of mutual evaluations and is currently conducting a third round of mutual evaluations.

THE EASTERN AND SOUTHERN AFRICA ANTI–MONEY LAUNDERING GROUP

The Eastern and Southern Africa Anti–Money Laundering Group (ESAAMLG) was established in 1999 as an FSRB for eastern and southern Africa. It comprises 14 countries. It monitors the implementation of AML/CFT international standards in its member countries through self-assessment exercises and mutual evaluation. The ESAAMLG also conducts technical analysis and publishes reports of money laundering and terrorist financing typologies in the region, and provides and facilitates technical assistance to the member countries.

THE SOUTH AMERICAN FINANCIAL ACTION TASK FORCE

The South American Financial Action Task Force (GAFISUD) was established in December 2000 to monitor the implementation of anti–money laundering standards in its member countries. The GAFISUD currently has 10 members. Similarly to other FSRBs, the GAFISUD monitors the implementation of inter-
national standards through processes of self-assessment and mutual evaluation, undertakes typologies studies, facilitates international cooperation, and provides technical assistance to member jurisdictions.

Eurasian Group on Combating Money Laundering and Financing of Terrorism

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) was established in Moscow in October 2004. It currently has seven members and started its first round of mutual evaluations in 2007. The main goals of the EAG are to facilitate implementation of international standards; carry out joint programs within the FIU sphere of competency; conduct evaluations of the effectiveness of existing AML/CFT mechanisms; coordinate technical assistance cooperation; and analyze trends (typologies) in the AML/CFT sphere and exchange experience in combating these crimes.

Middle East and North Africa Financial Action Task Force

The Middle East and North Africa Financial Action Task Force (MENAFATF) was established at an inaugural ministerial meeting held in Manama, Bahrain, in November 2004. Its headquarters is in the Kingdom of Bahrain and it currently has 17 members. MENAFATF monitors implementation of international standards through self-assessment and mutual evaluation, undertakes typologies studies, facilitates international cooperation, and provides technical assistance to member jurisdictions.

Intergovernmental Action Group against Money Laundering in Africa

The Authority of Heads of State and Government of the Economic Community of Western African States (ECOWAS) decided to establish the Intergovernmental Action Group against Money Laundering in Africa (GIABA) in December 1999. GIABA’s mandate was revised in January 2006 to fully incorporate and properly reflect the imperative to fight the financing of terrorism.

The objectives of GIABA are to protect the national economies and the financial and banking systems of signatory states against the proceeds of crime and to combat the financing of terrorism; to improve measures and intensify efforts to combat the proceeds from crime; and to strengthen cooperation among its members. GIABA consists of all ECOWAS members and currently has 15 members.

Regional organizations

The Asian Development Bank

The Asian Development Bank (ADB) has long been involved in money laundering control and prevention both directly and indirectly. In April 2003, the ADB adopted a policy to refine its role in this area according to three principles: (1) to streamline the ADB’s efforts so they fall within the wider context of its goals and objectives; (2) to avoid duplicating the work of other agencies, including
the FATF and the APG; and (3) to consider carefully the needs of the ADB’s
developing member countries.

The policy has three key elements:

1) Assisting developing member countries in the establishment and implementa-
tion of effective legal and institutional systems for AML/CFT
2) Increasing collaboration with other international organizations and aid agencies
3) Strengthening internal controls to safeguard the ADB’s funds

The ADB finances technical assistance projects to combat money laundering and
terrorist financing. This sometimes takes the form of a standalone project and is
introduced as an element in wider financial sector and legal reform projects.

THE INTER-AMERICAN DEVELOPMENT BANK

The Inter-American Development Bank (IADB) Group is the main source of
multilateral financing for economic, social, and institutional development in
Latin America and the Caribbean. It also plays a leading role in regional integra-
tion. The IADB pays special attention to questions of money laundering and
terrorist financing in its client countries. In this regard, it has partnered with the
Inter-American Drug Abuse Control Commission (CICAD) to provide technical
assistance on money laundering control and prevention. One of the IADB’s
initiatives involved training bank regulators and bank officers in the detection
of money laundering transactions. The IADB also considers money laundering
issues when it provides loans to client countries for financial sector reform.

THE INTER-AMERICAN DRUG ABUSE CONTROL COMMISSION

CICAD is an agency of the Organization of American States (OAS) that

- fosters multilateral cooperation on drug issues in the Americas;
- executes action programs to strengthen the capacity of CICAD member
  states to prevent and treat drug abuse, combat production and trafficking of
  illicit drugs, and deny the traffickers their ill-gotten gains; and
- promotes drug-related research, information exchange, specialized training,
  and technical assistance.

In 1996, through the Summit of the Americas, CICAD was asked to conduct a
follow-up to the implementation of the Plan of Action of Buenos Aires, on the
control of money laundering. The CICAD Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses
was amended repeatedly to reflect developments in the international standards.
Since 1996, because of the mandates received by CICAD, the Group of Experts
on money laundering that developed the model regulations in 1996 began to
meet on an annual basis, and in some cases biannually. Also in 1999, a series
of technical cooperation programs were executed as a product of joint efforts
between the IADB and the OAS/CICAD.
The CICAD created an Anti–Money Laundering Unit in 2001 to meet the increased demand for training and technical assistance by the member states of OAS. In 2001, given the clear relationship between the mechanisms to prevent money laundering and that of the financing of terrorism, CICAD expanded its sphere of action to include this area by working closely with the Inter-American Committee against Terrorism (CICTE). The principal functions of the unit consist of organizing meetings for the Group of Experts and executing programs and training seminars, as well as organizing technical assistance and studies and analyses on the different technical aspects of money laundering and the financing of terrorism.

**The Inter-American Committee against Terrorism**

In 1998, CICTE was established as part of the OAS, comprising competent national authorities of the member states. The committee renewed its focus after the events of September 11, 2001. On September 21, 2001, the 23rd Meeting of Consultation of Ministers of Foreign Affairs adopted a Resolution Strengthening Cooperation to Prevent, Combat, and Eliminate Terrorism (RC.23/RES.1/01).

In 2002, CICTE established an Executive Secretariat within the OAS General Secretariat. A key milestone in 2002 was the drafting and signing of the OAS Convention against Terrorism. This landmark document was signed by 30 of the Organization’s Member States at the OAS General Assembly in Bridgeton, Barbados, on June 3; it was put into effect in July 2003.

**The European Bank for Reconstruction and Development**

The European Bank for Reconstruction and Development (EBRD) has elaborate internal procedures and practices that focus primarily, but not exclusively, on reducing the prospects of financial institutions and intermediaries that the EBRD finances or channels funds through of being used as vehicles for money laundering. These procedures and practices relate, for example, to due diligence, representations, covenants, and compliance with local laws, as well as best practices and EBRD nomination of directors to local banks.

Also, where EBRD funds are being channeled through offshore jurisdictions, particular care is taken to ensure that there are both sound business reasons for doing so and that the place of incorporation is an acceptable one for the FATF Recommendations. It is a categorical commitment of the EBRD, according to its “Anti-terrorist Statement,” that it will not provide financing to entities or individuals that, according to UN Security Council Committees, may be supporting terrorist activities. Moreover, the EBRD will not finance any contracts for the supply of goods, works, or services awarded to such entities and individuals on their projects. The statement also confirms that the EBRD closely follows the work of the FATF.
THE COUNCIL OF EUROPE

The Council of Europe is a standard setter widely known for its two money laundering– and terrorist financing–related conventions (the Strasbourg Convention and the Warsaw Convention). It also adopted two conventions related to terrorism. In addition, it provides AML/CFT technical assistance to all its members (currently 47 countries).

THE EUROPEAN UNION

The European Union (EU) adopted three money laundering– and terrorist financing–related directives and several other legally binding documents related to money laundering, corruption, and organized crime.

THE COMMONWEALTH SECRETARIAT

The heads of government of the Commonwealth established in 1965 the Commonwealth Secretariat as its principal organization. Its purpose is to implement the decisions of the 53 member governments. The Commonwealth Secretariat crafts legal cooperation among its member countries in constitutional law, transnational crime, human rights, trade law, and other emerging areas of law.

In 2000, the Commonwealth Secretariat published *The Model of Best Practice for Combating Money Laundering in the Financial Sector*, which reviewed the existing international legal framework for fighting money laundering. It also addressed issues of particular relevance to some of its members, such as laundering the proceeds of corruption.

In the aftermath of the events of September 11, 2001, the Commonwealth issued a Statement on Terrorism (October 25, 2001) committing members to implementing UN Security Council Resolution 1373, in keeping with the fundamental values of the association, including support for democracy, human rights, the rule of law, freedom of belief, freedom of political opinion, justice, and equality. Within this context, heads of government agreed that any member state that aided, supported, instigated, financed, or harbored terrorists, or permitted such activities within its jurisdiction, violated the fundamental values of the Commonwealth and should have no place in it.

The Commonwealth has set up the Commonwealth Committee on Terrorism, which is charged with developing a Commonwealth plan of action for fighting terrorism. The plan of action concentrates on helping member countries execute the UN Security Council Resolutions, the UN Conventions on Terrorism, and the international standards. The committee also sought to sharpen international cooperation in penal matters between member countries and, in this regard, extend the existing framework of the Commonwealth.
**Europol**

Europol is a European law enforcement organization that seeks to improve the effectiveness and cooperation of its member states in the fight against terrorism, unlawful drug trafficking, and other serious forms of international organized crime. In the area of money laundering, Europol offers member states’ law enforcement authorities significant operational and analytical support by way of its Europol Liaison Officers (ELOs) and analysts. Europol also has a specialized financial group within its serious crime department that supplies member states with adequate support in fighting money laundering at the EU level.

In 2001, Europol opened an Analytic Work File for suspicious transactions. Its main objective is to compile suspicious transactions handled by police or justice authorities of the member states. The next step is to identify potential links among suspicious transactions and to provide specialized law enforcement agencies of the member states with long-term analytical support.

In the fight against terrorism, Europol and the member states have developed an operational strategy, based on previous and different experiences of the member states, for directional guidelines. To date, within the framework of the Europol Terrorism Task Force, Europol and seconded experts from the member states have achieved significant expertise and have exchanged operational information on the financing of terrorism.

**Other specialized organizations**

**The Egmont Group**

The Egmont Group was established in 1995 by a group of financial intelligence units (FIUs), which are governmental agencies set up for the purpose of collecting financial information, analyzing it, and disseminating it to appropriate governmental or law enforcement agencies. The group takes its name from the Egmont Arenberg Palace, where the FIUs first met with the goal of improving international cooperation. Their work is central to the fight against money laundering and terrorist financing. Although every FIU operates differently, most FIUs can exchange information under certain provisions with foreign counterpart FIUs. In addition, many FIUs can assist by providing government administrative data and public record information to their counterparts; this can be very useful to the investigators.

The FIU members of the Egmont Group meet regularly to find new ways to cooperate, especially in the areas of information exchange and in training and the sharing of expertise. There are currently 106 countries with recognized operational FIU units and others in various stages of development. Countries must go through a formal procedure established by the Egmont Group to meet the Egmont definition of an FIU. The Egmont Group as a whole meets once a year, conducting its business through working groups and committees. One of the main goals of the Egmont Group is to create a global network by promoting
international cooperation among FIUs. It also develops principles and standards of best practice for international cooperation and information sharing.

**The Wolfsberg Group**

The Wolfsberg Group currently comprises 11 global banks. Together, they develop financial services industry standards and related products that support know-your-customer (KYC) and AML/CFT policies. The group was organized in 2000 at Chateau Wolfsberg in northeastern Switzerland to work on draft private banking guidelines for combating money laundering. Since then, the Wolfsberg Group issued Wolfsberg Standards that consist of various sets of AML principles and guidelines. This includes those relating to correspondent banking and private banking. In 2004, the Wolfsberg Group focused on the development of a due diligence model for financial institutions, in cooperation with Banker’s Almanac, thereby fulfilling one of the recommendations made in the Correspondent Banking Principles.

**INTERPOL**

Interpol is the largest international police organization in the world. Organized in 1923 to facilitate cross-border police cooperation, Interpol today has 186 member countries spread over five continents. It supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime.

The Interpol General Assembly has passed a number of resolutions in recent years that have called on member countries to concentrate their investigative resources on identifying, tracing, and seizing the assets of criminal enterprises. These resolutions have also called on member countries to increase the exchange of information in this field and encouraged governments to adopt laws and regulations that would allow police access to the financial records of criminal organizations and the confiscation of proceeds gained by criminal activity. Interpol has been involved in the fight against terrorism since 1985; a special subdirectorate is dedicated to terrorism. Interpol also advocates the disruption of terrorist financing as essential to controlling and preventing terrorist activities.

**QUESTION 23.** An FSRB is:

a) A member organization of the FATF  
b) A regional organization that deals with money laundering issues and that has been designed to function and operate on the model of the FATF

**QUESTION 24.** The FATF is the only international body that works in the area of money laundering and terrorist financing control.

a) True  
b) False
Assessing compliance with international standards

4.1. Why assess compliance?
Assessing compliance with an international standard is a way to achieve harmonization. A peer-review mechanism ensures that all countries make sufficient efforts to meet the minimum international standard. This is part of the global process of implementing international standards. In this sense, anti-money laundering standards are no different.

4.2. Who assesses compliance with international standards?
As you learned in section 3.3 of this module, one main function of the FATF is to ensure compliance with the Recommendations. You have seen that the FATF conducts mutual evaluation of its members.

Each FSRB engages in similar evaluations of its members’ compliance with international standards on money laundering and terrorist financing. These evaluations are considered central to the function of each group.

The Boards of the World Bank and the IMF endorsed the use of the FATF Recommendations by adding them to the list of standards and codes relevant to the operational work of the Bank and the IMF, and for which Reports on the Observance of Standards and Codes (ROSCs) could be prepared. This decision was significant in acknowledging the FATF Recommendations as the international standard on money laundering and terrorist financing; it also included a way to assess compliance with this standard in financial sector evaluations carried out by the Bank and the IMF.

4.3. Is there a standard method for assessing compliance?
Working together with the FATF and FSRBs, the World Bank and the IMF developed a comprehensive assessment methodology. This methodology is used for all the assessments of compliance with international standards in this area. As mentioned above, these include the FATF, FSRBs, the World Bank, and the IMF. The purpose of developing a comprehensive methodology is to ensure a consistent assessment process. This, in turn, creates greater harmony of rules and practices across national jurisdictions. As we know, this is one of the ultimate objectives of standard setting and is the only guarantee of reducing the advantages criminals find in the varying regulations across international jurisdictions.
The comprehensive methodology addresses in detail all the necessary elements of the AML/CFT standard established in the FATF Recommendations. We are not going into the details of the methodology in this module because the understanding of the AML/CFT systems, which are covered by subsequent modules, is a prerequisite for understanding the assessment methodology. However, if you are interested in the assessment methodology, please visit the FATF website.12

Check your understanding

Now, consider again the pretest that you attempted at the beginning of the module.

True or False?

1) Only drug dealers launder funds.
   a) True   b) False

2) The proceeds of any illegal activity could be subject to laundering.
   a) True   b) False

3) Proof of a predicate offense is a prerequisite for a charge of terrorist financing.
   a) True   b) False

4) Money laundering takes place only in developing countries.
   a) True   b) False

5) Although money laundering may occur through the banking sector, the securities industry is completely immune to money laundering.
   a) True   b) False

6) FATF-Style Regional Bodies (FSRBs) are specialized organs of the United Nations dealing with terrorist financing.
   a) True   b) False

7) The FATF is the international standard setter for anti-money laundering and terrorist financing measures.
   a) True   b) False

8) Money laundering is an engine for economic and social development.
   a) True   b) False

12 http://www.fatf-gafi.org/
9) Only the IMF and the World Bank may assess countries’ compliance with anti-money laundering international standards.
   a) True       b) False

10) *Hawala* systems are informal fund transfer systems.
    a) True       b) False
Appendix A: References

FATF Recommendations

  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- *Special Recommendations on Terrorist Financing* (FATF, October 2004)

Useful Web sites

- African Development Bank Group
  http://www.afdb.org/
- Asian Development Bank (ADB)
  http://www.adb.org/
- Asia/Pacific Group on Money Laundering (APG)
  http://www.apgml.org/
- Basel Committee on Banking Supervision (BCBS)
  http://www.bis.org/bcbs/
- Caribbean Financial Action Task Force (CFATF)
  http://www.cfatf.org/eng/
- Commonwealth Secretariat
  http://www.thecommonwealth.org/
- Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) [European regional AML body for Eastern Europe and offshore jurisdictions that are not members of the FATF]
  http://www.coe.int/moneyval/
- Eastern and Southern Africa Anti–Money Laundering Group (ESAAMLG)
  http://www.esaamlg.org/
- Egmont Group
  http://www.egmontgroup.org/
- European Bank for Reconstruction and Development (EBRD)
  http://www.ebrd.org/
- Financial Action Task Force on Money Laundering (FATF)
  http://www.fatf-gafi.org/pages/0,2966,en_32250379_32235720_1_1_1_1,00.html
• Financial Action Task Force on Money Laundering in South America (GAFISUD)  
  http://www.gafisud.org/home.htm
• Inter-American Development Bank (IDB)  
  http://www.iadb.org/
• Inter-American Drug Abuse Control Commission (CICAD)  
  http://www.cicad.oas.org/EN/Default.asp
• International Association of Insurance Supervisors (IAIS)  
  http://www.iaisweb.org/
• International Monetary Fund (IMF)  
  http://www.imf.org
• International Organization of Securities Commissions (IOSCO)  
  http://www.iosco.org
• United Nations (UN)  
  http://www.un.org/
• Wolfsberg Group  
  http://www.wolfsberg-principles.com/index.html
• World Bank  

**Reference Documents**

• *Core Principles for Effective Banking Supervision* (Basel Core Principles)  
  (BCBS, September 1997)  
  http://www.bis.org/publ/bcbsc102.pdf
• *Customer Due Diligence for Banks* (BCBS, October 2001)  
  http://www.bis.org/publ/bcbs85.pdf
  http://www.bis.org/publ/bcbs85annex.htm
• *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering* (BCBS, December 1988)  
  http://www.bis.org/publ/bcbsc137.pdf
• *Guidance Paper on Anti–Money Laundering and Combating the Financing of Terrorism* (IAIS, October 2004)  
• *Insurance Core Principles and Methodology* (IAIS, October 2003)  
  http://www.iaisweb.org/__temp/Insurance_core_principles_and_methodology.pdf
• *A Resolution on Money Laundering* (IOSCO, October 1992)
• *Principles on Client Identification and Beneficial Ownership for the Securities Industry* (IOSCO, May 2004)
• *Anti–Money Laundering Guidance For Collective Investment Schemes* (IOSCO, October 2005)
• *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: Vienna Convention* (UN, 1988)
• *United Nations Convention for the Suppression of the Financing of Terrorism* (UN, 1999)
• *United Nations Security Council Resolution 1373* (UN, September 2001)
• *Financial Havens, Banking Secrecy, and Money Laundering* [UN, May 1998]
  [offers a very good analysis of banking secrecy and offshore financial centers]
• *The BCCI Affair: A Report to the Committee on Foreign Relations United States Senate by Senator John Kerry and Senator Hank Brown* (December 1992) [see Chapter 21, “Capcom: A Case Study of Money Laundering”]
• *Corruption in Empirical Research—A Review: Transparency International Working Paper* (Johann Graf Lambsdorff, November 1999) [offers a good review of the causes of corruption and the impact of corruption on various aspects of the economy and it is based on a review of the empirical research on these matters]
  http://www.transparency.org/

**Publications**

• *Legal Globalization: Money Laundering Law and Other Cases* (Heba Shams, British Inst of Intl & Comparative, April 2004) [For a thematic history of the evolution of AML standards, read chapter 2; to understand the relationship between money laundering control and globalization, read chapter 3.]
• *Money Laundering and the International Financial System* (Vito Tanzi, IMF Working Paper No. 55, May 1996) [It is one of the earliest attempts at economic analysis of the impact of money laundering.]
Appendix B: The Mandate for the Future of the FATF (FATF Revised Mandate 2008–2012)

I. Introduction and Background

1. Since its creation in 1989, the Financial Action Task Force (FATF) has worked to ensure that its 40+9 Recommendations are recognized globally as the international standards for anti-money laundering and combating the financing of terrorism (AML/CFT). The work of the FATF, covering more than 170 jurisdictions, has had a significant impact on the global detection and prevention of money laundering and terrorist financing, and is critical to the implementation of more robust AML/CFT regimes around the world.

2. The FATF, since its establishment, has focused its work on three main activities: standard setting, ensuring effective compliance with the standards, and identifying money laundering and terrorist financing threats. These activities will remain at the core of the FATF’s work for the remainder of this mandate. Going forward, the FATF will build on this work and respond to new and emerging threats, such as proliferation financing and vulnerabilities in new technologies that could destabilize the international financial system.

3. A mid-term review was conducted in 2007 to ensure that the FATF is equipped to respond flexibly to new challenges. The FATF mandate, revised through this mid-term review process, will expire in December 2012.

II. FATF Standards

4. The core work of the FATF since its creation has been to combat money laundering (40 Recommendations), and since 2001, terrorist financing (9 Recommendations). The FATF has taken concerted action to combat these threats. The FATF continues to revise and clarify these standards, and will continue to do so when necessary. This approach has so far provided the right balance between giving the required stability to the FATF standards, while allowing for the necessary flexibility to respond to the changing nature of the threats faced. Maintaining this balance between stability and flexibility allows for more predictability, and consistent implementation globally.
III. Promoting Global Implementation of the Standards

5. Full and effective roll-out of the 40+9 Recommendations in all countries is one of the fundamental goals of the FATF. Members are assessed through the mutual evaluation process, which is an essential and long-standing core activity of the FATF. This peer review process has now been extended through the FATF-Style Regional Body (FSRB) network to more than 170 countries, and is the critical mechanism for promoting timely and effective implementation of FATF Recommendations and for contributing to the creation of a level playing field throughout the membership and beyond. Countries that are not FSRB members will be encouraged to join the relevant regional body. The FATF will complete the third round of mutual evaluations of its membership (using the common assessment methodology) to determine the degree to which all members have implemented the 40+9 Recommendations. Also, the FATF will continue to undertake appropriate follow-up action from mutual evaluations to ensure that members correct, as quickly as possible, any deficiencies that are identified through the mutual evaluation process.

6. All countries, including nonmembers, should implement the FATF Recommendations effectively, to ensure a more effective global system for combating AML/CFT risks. However, many countries, in particular low-capacity countries, face challenges in the implementation of FATF standards. To minimize both their own vulnerabilities and the associated risks for the international financial system, the FATF, in close collaboration with the FSRBs and other international partners, will develop strategies to facilitate the implementation of the FATF Recommendations by countries facing capacity constraints. As a first step the FATF and FSRBs will continue their work to support the effective implementation of the FATF standards in these countries.

IV. Identifying and Responding to New Threats

(a) High-risk jurisdictions

7. A key element of the FATF’s work will continue to be its action to identify and address risks posed by jurisdictions with significant deficiencies in their AML/CFT regimes to protect the international financial system from criminal threats. Action such as the Non-Cooperative Countries and Territories exercise led to significant improvements in the AML/CFT regimes of more than 20 countries.

8. In 2006, the FATF adopted a new surveillance process—the International Co-operation Review Group—to identify, examine, and engage with vulnerable jurisdictions that are failing to implement effective AML/CFT systems. The FATF will continue to use this process to reach out to those countries and, where appropriate, will take firm action when a country chooses not to engage with the appropriate FSRB or the FATF or to reform its systems.
(b) Systemic money laundering and terrorist financing threats

9. The FATF is uniquely placed to analyze and draw international attention to emerging money laundering and terrorist financing vulnerabilities, and has significantly enhanced its process for the identification of money laundering and terrorist financing threats (the typologies process). The generation and dissemination of in-depth typologies studies is central to the work of the FATF and provides a solid foundation for ongoing policy development at the national and international levels. The FATF will continue to produce such studies, which present detailed information about the methods, trends, and techniques of money laundering and terrorist financing, and provide practical input to policy makers and the standard-setting process. In pursuing this work, the FATF will continue its expanded co-operation with the FSRBs and other international bodies, and will also harness the experience and expertise which the private sector can bring to this process.

10. Looking forward, the FATF will intensify its surveillance of systemic criminal and terrorist financing risks to enhance its ability to identify, prioritize, and act on these threats. In this context, and drawing on contributions from the FATF membership, the private sector, and the FSRBs, it will support the development of national threat assessments through best practice guidance and establish stronger and more regular mechanisms for sharing information on risks and vulnerabilities. The results of the enhanced strategic surveillance function will be disseminated publicly via the publication of a regular global threat assessment.

11. The FATF will also examine the available data to measure the impact of AML/CFT regimes on underlying criminal and terrorist activity, encouraging research into the effectiveness of its regime. It will examine the feasibility of implementing cost-benefit analysis across the field of AML/CFT policy.

(c) Emerging threats

12. Globalization has created potential new risks as criminals and terrorists seek to penetrate the global financial system. The FATF will remain at the center of international efforts to protect the integrity of the financial system and will respond to the significant new threats emerging which are related to, but may fall outside, its core activities. The FATF will only consider limited expansions of its field of action where it has a particular additional contribution to make.

13. Proliferation financing is an example of an area where the FATF can add value to the wider efforts of the international community and, consistent with the needs identified by the UN Security Council Res-
olutions, the FATF will continue to work on this issue. In doing so, the FATF will ensure that it does not duplicate existing efforts elsewhere.

V. Relations with Stakeholders and Partners

(a) Outreach to the private sector and the public

14. The private sector is at the front line of the international battle against money laundering, terrorist financing, and other illicit financing threats. The FATF has significantly increased its engagement with the private sector, through events with industry groups and the production of joint analysis on issues of common concern, soliciting private sector input to the typologies process, and through the establishment of a new private sector consultative forum. Looking forward, it will deepen its engagement with the private sector, through holding regular dialogues between the FATF and the private sector in support of our common objective of a more effective implementation of FATF standards.

15. More generally, in accordance with better regulation practice, the FATF will maintain high levels of transparency in its work, through direct communication, outreach, and awareness-raising across all stakeholders, and making use of all available channels of communication.

(b) Relations with other international organizations

16. The FATF relies on and values its close partnerships with other international organizations, including the United Nations, the International Monetary Fund, the World Bank, and the Financial Stability Forum, in the delivery of its objectives. The FATF has conducted targeted outreach to improve the FATF’s knowledge of particular issues and to ensure that the FATF standards do not conflict with the work of other international organizations. In particular, the IMF and the World Bank have made an important contribution to global efforts to combat money laundering and terrorist financing in non-FATF member countries, and the FATF supports this valuable contribution to the global effort. The FATF will continue to work actively with all partners to further FATF objectives and to draw on their knowledge in developing FATF policy.

(c) Relations with Associate Members and FSRBs

17. The FSRBs, several of which are now associate members of the FATF, play an important leadership role in their respective regions and provide important regional expertise and input into the FATF policy-making function. The FATF and FSRBs will continue to strengthen their working relationships, as well as extending outreach at a regional level with key partners.
VI. Operational Issues

(a) FATF Structure and Organization

18. The FATF’s task force structure has enabled it to respond decisively and promptly to emerging threats and to accommodate efficiently several expansions in its membership. This structure remains broadly the right one for the organization and should be maintained.

19. Over the long term, it will be vital for the FATF to evolve if it is to maintain an effective response to the constantly changing threats facing the international financial system. It will therefore be essential that the structure, organization, and operational planning of the FATF remain flexible and able to adapt to meet new challenges as they arise.

(b) Membership

20. The FATF has gradually increased its membership, and since 2000 has admitted six new members and has accepted two observer countries that are expected to become members in due course. The FATF will continue to work actively toward the membership of the remaining two countries. The FATF will maintain its open approach and will consider the structure of the global AML/CFT architecture, including the enhanced role played by associate members and FSRBs, and FATF membership, once the current expansion is completed. In this regard, the strategic importance of a country, the geographic balance of FATF membership overall, and a country’s commitment to implementing the FATF standards will remain the guiding principles of future membership decisions.

21. The FATF currently has 22 observer organizations/bodies. To make the most effective and efficient use of these relationships the FATF will review its policy on observer status.

(c) Presidency

22. Each Presidency will continue to be designated by the Plenary for the duration of one year, and will be supported by a Vice-Presidency, which will be the Presidency-designate.
(d) The Steering Group

23. The seven-member Steering Group is an advisory body for the President. The composition of the Steering Group will continue to reflect the geography and size of the FATF as well as include the President, the immediate past Presidency, and the Presidency-designate.

(e) The Secretariat and Budget

24. The Secretariat will continue to support the work of the FATF, including through the working groups and ad hoc groups to ensure coordination and consistency.

25. The current arrangements for financing FATF activities will be retained. The cost of the Secretariat and other services will be met by the FATF budget, through the OECD, with member contributions in line with OECD scales, and with the option of additional contributions.

VII. Ministerial Accountability

26. The FATF is accountable to the Ministers of its membership. To strengthen this accountability, the FATF President will report annually to Ministers on key aspects of FATF work, including on global threats. Given the potentially destabilizing effects of criminal and terrorist action against the international financial architecture, occasional ministerial meetings will provide an ongoing accountability mechanism whereby Ministers can shape the strategic direction of FATF policy making.
To guard its decision-making capacity, the organization sets certain criteria for the recruitment of new members (Source: *FATF Annual Report 2003–04*, p. 12):

- To be fully committed at the political level to implement the FATF Recommendations and to undergo regular mutual evaluations
- To be a full and active member of the relevant FATF-Style Regional Body (where one exists), or be prepared to work with the FATF or even to take the lead to establish such a body (where none exists)
- To be a strategically important country
- To have already made the laundering of the proceeds of drug trafficking and other serious crimes a criminal offense
- To have already made it mandatory for financial institutions to identify their customers and to report unusual or suspicious transactions

The balance between inclusion of more countries and ensuring the efficiency of the group is a tricky one. This is particularly so considering that the FATF is challenged by the continuous geographic expansion of money laundering and terrorist financing activities. The tightening of controls in FATF member countries was in itself a trigger for this change in money laundering geography. This means that the FATF has long been aware of the need to expand its regime to more countries without expanding its membership.

To achieve that, the FATF resorted to various alternatives:

- Carefully and strategically selecting new members, as we saw previously
- Offering some agencies an observer status
- Paying special attention to achieving geographic balance when recruiting new members
- Conducting worldwide consultation that includes nonmembers on high-priority policy issues, such as the review of the international standard
- Maintaining an ambitious outreach program that promotes its message throughout the world, and as part of that encouraging the establishment of FSRBs
Answers
Module 1 Answers

Answer 1
1) The money involved was most likely derived from crime—namely, drug trafficking, given his drug trafficking business.

2) Mr. A conducted five transactions using the funds: first, he bought chips/tokens in a casino; second, he converted to check; third, the check was deposited in a securities firm; fourth, the money was withdrawn; and, finally, he invested it in a grocery business.

3) At the casino, Mr. A converted his cash into deposits and then withdrew it in checks drawn on the casino’s bank accounts.

4) Mr. A finally invested his money in a number of legitimate grocery shops.

Answer 2
Money laundering is the processing of criminal proceeds to disguise their illegal origin.

The internationally accepted definition of this offense is the one provided by the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 1988). According to Article 3 of the convention, money laundering means the following conduct when committed intentionally:

The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or for assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;

The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity. This is not an obligatory element of the definition since it is subject to country’s constitutional principles and basic concepts of its legal system.
The Vienna Convention did not in fact use the term *laundering*. The scope of the offense as defined by the convention was limited to funds derived from a drug-trafficking offense. This has now changed. The international standard expands the scope of money laundering at least to funds derived from any “serious crime.” You will learn a lot more about money laundering offenses and the offenses that generate the funds, so-called predicate offenses, in subsequent modules.

**Answer 3**

Placement: Depositing the money into the casino.

Layering: Withdrawing the money from the casino, depositing the money into the securities firm, and withdrawing it from the firm.

Integration: Investing the money in a chain of grocery shops.

**Answer 4**

Go to Question 8.

**Answer 5**

While the source of laundered funds is always criminal, terrorist financing is sometimes derived from legal sources. Terrorists also resort to crime to generate funds for their activities, and in these cases their financial activities are very similar to those of launderers. In fact, it is difficult to determine from the financial transactions alone whether they are linked to terrorism or to other types of criminality. Making this determination requires other types of intelligence and investigative work.

**Answer 6**

Even though terrorists are not in business for the money, and even though they sometimes derive their funds from legitimate sources, terrorists still need to hide the movement of these funds and deliver them to their destination as discreetly as possible. To achieve this objective, terrorists use the same methods as money launderers to handle their funds. Analysis of terrorist financing methods reveals that money launderers and terrorist financiers use front companies, shell companies, nominees and structuring, credit cards, electronic fund transfers, among others. In addition, there is evidence of abuse of informal money transfer systems and nonprofit organizations by terrorist financiers.

**Answer 7**

They used both legitimate and illegitimate sources of funding. The contraband trade in cigarettes, which exploited the tax differences between jurisdictions, was clearly criminal. The gas station, on the other hand, is a perfectly legitimate business.
They created four layers between the source and the destination of the money:

1. money was deposited into bank accounts held by nominees in country A;
2. money was transferred to numbered accounts in an offshore jurisdiction;
3. money was transferred to accounts held in the names of their nominees in country B; and
4. the money was delivered to a terrorist organization.

They used front companies, nominees, offshore jurisdictions with bank secrecy, wire transfers, and numbered accounts.

**Answer 8**
The correct answer is (c). It is financial support given to terrorists. The source of money may be from both illicit and legitimate sources.

**Answer 9**
The BCCI-Noriega laundering operation involved five jurisdictions: Panama, Luxembourg, Switzerland, Germany, and the United Kingdom.

It can be observed that, apart from Panama, where the illegitimate activity that generated the funds originated, all the other jurisdictions, where the money laundering took place, are large financial centers of economically developed countries.

**Answer 10**
Some of the reasons are:

- Legitimate companies take advantage of tax concessions generally provided by these centers.
- A large number of financial service providers often operate in these centers, which allows business enterprises access to a variety of financial services at a competitive price.
- Companies use offshore financial centers to avoid onerous regulations; this allows them flexibility in their business operations.
- Firms may use offshore financial centers to protect their business information.
**Answer 11**

Major characteristics:

- Lax financial regulation and supervision
- Provisions for creating/registering corporations within a short time
- Corporate secrecy laws
- Excellent facilities for electronic communications
- Weak law enforcement culture/practice
- Strong bank secrecy laws
- Large tourist trade, which can help maintain major inflows of cash
- Use of major world currency, preferably the U.S. dollar, as the local currency
- A high degree of economic dependence on the financial services sector
- A geographic location that facilitates business travel and communications

Additional characteristics:

- A free-trade zone
- Availability of a flag-of-convenience shipping registry

*Source:* United Nations Office on Drugs and Crime

**Answer 12**

Securities markets are highly international. Many companies are traded on different domestic exchanges, and investment is open to investors from all over the world. This gives the launderers the advantage they seek by using multiple jurisdictions. Organization O exploited this characteristic by simulating foreign investment movements across several jurisdictions.

Brokers’ reliance on commissions may tempt them to relax their compliance with regulatory obligations to avoid losing clients to their competitors. The case also provides an obvious example of the risks.

Trading is easy. Customers can open accounts with an investment service provider in person or remotely via the phone or the Internet, thus making customer due diligence more demanding. Organization O used several front men as small foreign investors and bought and sold the shares repeatedly across jurisdictions, exploiting the ease of trading in this market.

**Answer 13**

Mr. L’s goal was not to defraud the insurance company but to give his illegal funds a legitimate appearance. By setting up a fictitious marine business and creating fictitious losses and liabilities, Mr. L managed to give his illegal funds a legitimate appearance as claims payments from a reputable insurance company. Mr. L can now move his funds freely in the financial system. Financial institutions are likely to accept payments originating from insurance companies without suspicion.
**Answer 14**

“The experts viewed the insurance sector as potentially vulnerable to money laundering because of the size of the industry, the easy availability and diversity of its products, and the structure of its business. In regard to this last point, it is important to note that insurance is, in some jurisdictions, often a cross-border business and more frequently than not involves the distribution of its products through brokers or other intermediaries who are not necessarily affiliated with, or under the control or supervision of, the company that issues the product. Moreover, because the beneficiary of an insurance product is often different from the policyholder, it is sometimes difficult to determine when and for whom it is necessary to perform consumer due diligence (for the policy holder only or also for the beneficiary?).”


**Answer 15**

The Internet is truly global, and there are still unresolved issues of jurisdiction in its regulation.

Internet communication offers the opportunity for near anonymity, which a money launderer can certainly appreciate.

Because of the lack of uniformity in maintaining online communication records, it is difficult for investigators to follow the path of communication. This is an ideal situation for the money launderer, whose objective is to confound the audit trail.

Online communications occur at a high speed and are unmatched by the investigators’ capacity to gather information. (See *Report on Money Laundering Typologies, 2000–2001*, FATF, pp. 12–14.)

**Answer 16**

Mr. T diverted funds originally derived from legitimate sources. The donors were public bodies with developmental objectives and individuals with an interest in development. In the BCCI case, the money was corruption money. This is one of the fundamental differences between money laundering and terrorist financing. The funds in terrorist financing are sometimes derived from legal sources.

**Answer 17**

“An informal money or value transfer system is one in which money is received for the purpose of making it of an equivalent value payable to a third party in another geographical location, which may or may not be in the same form. Such transfers generally take place outside of the conventional banking system through nonbank financial institutions, or other business entities whose primary business activity may not be the transmission of money.”

**Answer 18**

“Large inflows or outflows of capital could significantly influence variables, such as the exchange rates and the interest rates, or even the prices of particular assets toward which the money is invested, such as land and houses. In some countries identified with money laundering activities, there have been increases in asset prices (land and houses) that often could not be explained by the changes in the countries’ policies. When the exchange rate is free to fluctuate, the inflow of large amounts of laundered money into a country would lead to its appreciation and/or to an expansion of the country’s monetary base. The appreciation of the exchange rate would reduce the competitiveness of traditional exports and would encourage more imports. The expansion of the monetary base, in the absence of sterilization, would also put some upward pressure on domestic prices.”


**Answer 19**

The sources of the funds that a person who holds a prominent public position may try to launder include not only the proceeds of bribes, illegal kickbacks, and other obvious forms of corruption, but also embezzlement or outright theft of state assets or funds from political parties and unions, as well as tax fraud. In certain cases, a person holding a public position may be directly implicated in other types of illegal activities, such as organized crime or narcotics trafficking.


**Answer 20**

Countries, through the work of the Basel Committee on Banking Supervision, try to harmonize prudential regulations to prevent banks from avoiding important prudential regulations by setting their operations in countries with a lower regulatory threshold.

Concern for the environment is prompting sympathetic countries to push for harmonization of environmental standards. The purpose of these efforts is to prevent corporations from moving their production activities to jurisdictions with lax environmental requirements.

Labor rights constitute another area where regulatory variations between countries offer corporations opportunities for forum shopping and put pressure on countries to relax their standards. Harmonization of regulatory standards is one way to limit variations in the regulatory burden that give rise to forum shopping and regulatory competition.
Tax laws offer another contentious example. Corporations constantly exploit differences in tax treatment and set up their operations in the jurisdictions that offer them the least burdensome tax treatment.

**Answer 21**
The answer is (b). Because the legal systems of countries vary substantially, the Recommendations represent the minimum on which countries could agree. Therefore, they do not represent the ultimate set of best practices that countries should aspire to achieve. They also do not represent the exact standard that countries should not exceed. Countries can improve on the content of the Recommendations and adopt measures that go beyond their scope. They are a set of minimum standards that accept the existing variations among countries in their legal systems.

**Answer 22**
The answer is (a). The FATF Recommendations are recognized as the international standard, and therefore all countries, including nonmember countries, are expected to follow and implement them.

**Answer 23**
The answer is (b). FSRB is an FATF-Style Regional Body.

**Answer 24**
The answer is (b). Other organizations and groups play roles in developing and enforcing the international anti-money laundering and terrorist financing regime. There are FSRBs, which work regionally, and global standard setters, such as the Basel Committee and the IOSCO, which set standards on money laundering and terrorist financing relating to their scope of operations. International financial institutions play an active role enforcing and implementing standards. The United Nations has a program dedicated to capacity building in this area. Other groups and organizations are also involved in various capacities and ways. Countries also develop norms to fight money laundering and terrorist financing through a growing web of international treaties.

**Check your understanding**

**Answer 1. False.**

Initially, concern was focused on the proceeds from drugs. It has since expanded to include the proceeds from all serious offenses. In many countries around the world, predicate offenses for money laundering now include the proceeds from all serious criminal offenses or a list of designated categories of predicate
offenses. For the latter, the FATF Recommendations list 20 designated categories of offenses as a minimum that countries should include. See Module 2 for further detail.

**Answer 2. True.**

Defining the exact scope of money laundering as an offense is essentially a matter for national jurisdictions, and there also are national variations to be discussed in the subsequent modules.

**Answer 3. False.**

A predicate offense is the offense that generates the proceeds that are then laundered. Terrorist financing is distinct from money laundering in that it sometimes involves the use of legally derived funds for terrorism. There isn’t always an illegal activity generating funds in the case of terrorist financing.

**Answer 4. False.**

Money laundering takes place wherever it is possible to hide funds.

**Answer 5. False.**

There is evidence of money laundering through the securities sector and often in collusion with securities professionals.

**Answer 6. False.**

FSRBs are regional organizations that address money laundering and terrorist financing issues and have been designed in terms of functions, structures, and operations on the model of the FATF.

**Answer 7. True.**

The FATF is the standard setter for AML/CFT matters and is recognized as such by the Executive Boards of the IMF and the World Bank. Other groups and international organizations, such as Basel Committee and the UN, also engage in setting standards (conventions) or providing guidance.

**Answer 8. False.**

Although some economies seem to have gained some economic advantage by luring fugitive money, the rewards are short term. Worse, the systemic effects of money laundering and terrorist financing detract in the long run from the development objectives of any country.
The FATF and FSRBs also assess their members. All assessors use the same methodology to evaluate the level of compliance with the international standard. However, some FSRBs, for example, MONEYVAL, may also include in their evaluation process standards adopted by regional organizations, such as the EU AML/CFT Directives.

Answer 10. True.
Although they may be sometimes abused for money laundering and terrorist financing purposes, **hawala systems** are simple informal money transfer systems that perform a number of legitimate functions.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

**Module 1:** Effects on Economic Development and International Standards

**Module 2:** Legal Requirements to Meet International Standards

**Module 3a:** Regulatory and Institutional Requirements for AML/CFT

**Module 3b:** Compliance Requirements for Financial Institutions

**Module 4:** Building an Effective Financial Intelligence Unit

**Module 5:** Domestic (Inter-Agency) and International Cooperation

**Module 6:** Combating the Financing of Terrorism

**Module 7:** Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti–Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Legal Requirements to Meet International Standards

Workbook
Legal Requirements to Meet International Standards

Workbook
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

The initial work was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 2 was further written and developed by Paul Allan Schott, the World Bank. The draft was reviewed by Jean-Francois Gil Thony, IMF, and Elizabeth Joyce, UNODC. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by John McDowell and Emiko Todoroki, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Heba Mahmoud Mokhtar Shamseldin, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations,” 2003, and “Special Recommendations on Terrorist Financing,” 2005; and Paul Allan Schott, Reference Guide to Anti–Money Laundering and Combating the Financing of Terrorism, Second Edition, the World Bank, 2004.

Capacity Enhancement Program on Anti–Money Laundering and Combating the Financing of Terrorism

Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Legal Requirements to Meet International Standards

Satisfying the international standards for anti-money laundering and combating the financing of terrorism (AML/CFT) has implications for a country’s legal framework and usually requires legislative action. In exploring those implications and possible legislative needs, this module answers the following questions:

1. **What are the international conventions and treaties that deal with AML/CFT?**
   - 1.1 United Nations Conventions and Resolutions 5
   - 1.2 Regional legal instruments 6

2. **What legal and institutional arrangements satisfy international standards?**
   - 2.1 Criminalization of money laundering 8
   - 2.2 Criminalization of terrorist financing and associated money laundering 9
   - 2.3 Predicate offenses for money laundering and methods for describing them 10
   - 2.4 Scope of criminal liability 13
   - 2.5 Freezing, seizing, and confiscating proceeds of crimes 16
   - 2.6 Persons and entities subject to AML/CFT requirements 20
   - 2.7 Integrity standards 23
   - 2.8 Laws consistent with implementation of international standards 24
   - 2.9 Interagency cooperation 25

3. **What are the legal issues related to international cooperation?**
   - 3.1 Mutual legal assistance 26
   - 3.2 International aspects of confiscation 27
   - 3.3 Extradition 28
   - 3.4 Other forms of international cooperation 28

4. **Where can one find model laws?** 31
This module covers the following Recommendations of the Financial Action Task Force (FATF) on money laundering:

- Forty Recommendations on Money Laundering
  - Legal systems: Recommendations 1–4, 20, 23, 24
  - Institutional and other measures: Recommendations 31, 33, 34
  - International cooperation: Recommendations 35–40
- Nine Special Recommendations on Terrorist Financing
  - Ratification and implementation of UN instruments: Special Recommendation I
  - Criminalizing the financing of terrorism and associated money laundering: Special Recommendation II
  - Freezing and confiscating terrorist assets: Special Recommendation III
  - International cooperation: Special Recommendation V

At the end of Module 2, you should be able to

- identify relevant international conventions, resolutions, and instruments;
- describe the objectives of international convention and resolutions;
- discuss the legal framework for money laundering and terrorist financing;
- describe what authorities need to consider when they establish an AML/CFT legal framework; and
- identify the elements of international cooperation needed to satisfy international standards.
What are the international conventions and treaties that deal with AML/CFT?

How much do you know?

What are the international conventions and treaties that deal with AML/CFT?

**QUESTION 1.** The Vienna Convention contains the most widely accepted definition of money laundering and calls upon countries to criminalize the activity on that basis.

a) True  b) False

**QUESTION 2.** The Palermo Convention urges the countries to go beyond drug trafficking as a predicate offense for the crime of money laundering.

a) True  b) False

**QUESTION 3.** UN Security Council Resolution 1373 does not require ratification and implementation by a UN member country to have the force of law in that country.

a) True  b) False

**QUESTION 4.** Countries have discretion in how they may describe predicate offenses for the crime of money laundering.

a) True  b) False

**QUESTION 5.** A person may not be convicted of money laundering if the predicate offense occurs in another country.

a) True  b) False

_FATF's Forty Recommendations on Money Laundering and its nine Special Recommendations on Terrorist Financing constitute the international standards on AML/CFT. The legal framework of a country's AML/CFT regime should be consistent with those standards. Meeting the international standards almost always requires legislative and/or regulatory action (or another form of action, depending upon the legal system of the country). An important part of the necessary action is to remove conflicts between the AML/CFT regime and other national statutes, regulations, and court decisions. If any_

—continued
The international effort to fight crime began with the recognition that drug trafficking—and associated money laundering—were truly international problems and could be addressed effectively only on a multinational basis. The United Nations (UN) was the first international organization to take significant action in this area. The UN is important because of its ability to establish international law. The UN’s effort was later expanded to include many other serious crimes—specifically terrorism and the financing of terrorism. The FATF, the international standard setter for AML/CFT, took into account the international conventions dealing with AML/CFT, as it set about developing international standards for national regimes to fight these crimes.

This section introduces the UN Conventions and Resolutions that are relevant to the fight against money laundering and terrorist financing: the Vienna Convention, the Palermo Convention, the International Convention for the Suppression of the Financing of Terrorism, and Security Council Resolutions 1373 and 1267, including a number of successor resolutions to 1267. UN conventions generally require ratifications or acceptance by a certain number of countries before they come into force. They also require ratification and implementation by a member country before the convention has the force of law in that country. UN Security Council Resolutions, on the other hand, when passed in response to a threat to international peace and security under Chapter VII of the UN charter, are binding upon all member countries and immediately have the force of law in all member countries.

This section also introduces other legal instruments that are relevant because they have been adopted by regional bodies. These instruments should be implemented by a country and have the force of law in that country.
1.1 United Nations Conventions and Resolutions

**United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988)**

As a result of growing concern with increased international drug trafficking and the tremendous amounts of related money entering the banking system, the UN, through its Drug Control Program, initiated an international agreement to combat drug trafficking and the money laundering resulting from it. Although the Vienna Convention does not use the term “money laundering,” it defines the concept and calls upon countries to criminalize the activity. However, the only predicate offenses for money laundering under the convention are crimes related to drug trafficking. The convention does not address preventive aspects of money laundering. The Vienna Convention came into force on November 11, 1990. It serves as a basis for several FATF Recommendations on preventing, detecting, and prosecuting money laundering.

**The International Convention against Transnational Organized Crime (the Palermo Convention, 2000)**

The Palermo Convention, which came into force on September 29, 2003, contains a broad range of provisions to fight international organized crime. Countries that ratify the convention must implement its provisions through passage of domestic laws. Specifically with regard to money laundering, it obliges each ratifying country to:

- criminalize money laundering and include at least all serious crimes (not just drug trafficking) as predicate offenses to money laundering;
- establish regulatory and supervisory regimes to deter and detect all forms of money laundering;
- cooperate and exchange information, both domestically and internationally, and consider the establishment of a financial intelligence unit (FIU); and
- consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across its borders.

**International Convention for the Suppression of the Financing of Terrorism (the SFT Convention, 1999)**

This convention requires ratifying countries to criminalize terrorism, terrorist organizations, and terrorist acts. It applies to the offense of direct involvement or complicity in the intentional and unlawful provision or collection of funds, whether attempted or actual, with the intention or knowledge that any part of the funds may be used to carry out any of the offenses described in the convention, or an act intended to cause death or serious bodily injury to any person not actively involved in armed conflict in order to intimidate a population or to compel a government or an international organization to do or abstain from doing any act. Action in such a manner is an offense whether or not the funds are actually used to carry out any of the proscribed acts. The convention requires each country to take appropriate measures, in accordance with its domestic legal principles, for the detection and freezing, seizure, or forfeiture of funds used or allocated for the purposes of committing the described offenses. The convention came into force on April 10, 2002.

**UN Security Council Resolution 1373 (2001)**

This resolution, which is binding upon all UN member countries, was adopted on September 28, 2001. It obligates all member counties to criminalize actions relating to the financing of terrorism. It also obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorism, including freezing funds or assets of persons, organizations, or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorist groups; and
- cooperate with other countries in criminal investigations and in the sharing of information about planned terrorist acts.

**UN Security Council Resolution 1267 (1999) and its successors**

This resolution, which is binding upon all UN member countries (as are its successors), was originally enacted

---continued---

1. United Nations Conventions and Resolutions

1.1 United Nations Conventions and Resolutions

1. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988)

As a result of growing concern with increased international drug trafficking and the tremendous amounts of related money entering the banking system, the UN, through its Drug Control Program, initiated an international agreement to combat drug trafficking and the money laundering resulting from it. Although the Vienna Convention does not use the term “money laundering,” it defines the concept and calls upon countries to criminalize the activity. However, the only predicate offenses for money laundering under the convention are crimes related to drug trafficking. The convention does not address preventive aspects of money laundering. The Vienna Convention came into force on November 11, 1990. It serves as a basis for several FATF Recommendations on preventing, detecting, and prosecuting money laundering.

**The International Convention against Transnational Organized Crime (the Palermo Convention, 2000)**

The Palermo Convention, which came into force on September 29, 2003, contains a broad range of provisions to fight international organized crime. Countries that ratify the convention must implement its provisions through passage of domestic laws. Specifically with regard to money laundering, it obliges each ratifying country to:

- criminalize money laundering and include at least all serious crimes (not just drug trafficking) as predicate offenses to money laundering;
- establish regulatory and supervisory regimes to deter and detect all forms of money laundering;
- cooperate and exchange information, both domestically and internationally, and consider the establishment of a financial intelligence unit (FIU); and
- consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across its borders.

**International Convention for the Suppression of the Financing of Terrorism (the SFT Convention, 1999)**

This convention requires ratifying countries to criminalize terrorism, terrorist organizations, and terrorist acts. It applies to the offense of direct involvement or complicity in the intentional and unlawful provision or collection of funds, whether attempted or actual, with the intention or knowledge that any part of the funds may be used to carry out any of the offenses described in the convention, or an act intended to cause death or serious bodily injury to any person not actively involved in armed conflict in order to intimidate a population or to compel a government or an international organization to do or abstain from doing any act. Action in such a manner is an offense whether or not the funds are actually used to carry out any of the proscribed acts. The convention requires each country to take appropriate measures, in accordance with its domestic legal principles, for the detection and freezing, seizure, or forfeiture of funds used or allocated for the purposes of committing the described offenses. The convention came into force on April 10, 2002.

**UN Security Council Resolution 1373 (2001)**

This resolution, which is binding upon all UN member countries, was adopted on September 28, 2001. It obligates all member counties to criminalize actions relating to the financing of terrorism. It also obligates countries to:

- deny all forms of support for terrorist groups;
- suppress the provision of safe haven or support for terrorism, including freezing funds or assets of persons, organizations, or entities involved in terrorist acts;
- prohibit active or passive assistance to terrorist groups; and
- cooperate with other countries in criminal investigations and in the sharing of information about planned terrorist acts.

**UN Security Council Resolution 1267 (1999) and its successors**

This resolution, which is binding upon all UN member countries (as are its successors), was originally enacted...
Other legal instruments are relevant to your country depending upon its membership in regional organizations. Look at the groups below to see if your country is a member. Examine the requirements of the documents involved. Some of these documents may provide valuable guidance even if your country is not a member of the group that produced that document.

Not all regional groups have requirements that are separate from, or in addition to, the international standards set up by the FATF. In addition, regional groups often refer their members to model legislations, model regulations, or other instruments of other groups for guidance and best practices.

### Central America and the Caribbean
Kingston Declaration on Money Laundering (November 5–6, 1992)

For more information on the legal instruments listed above, see Appendix A.

### Latin America and the Caribbean
Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD)
Model Regulation Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses

For more information on the legal instruments listed above, see Appendix A.

### Europe
Council of Europe, Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime (Strasbourg, November 8, 1990)
Council of Europe, Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw, May 3, 2005)

For more information on the legal instruments listed above, see Appendix A.
Knowledge check

Which of the following statements are true?

QUESTION 6. The Vienna Convention contains a definition of money laundering and calls upon countries to criminalize the activity.
   a) True  b) False

QUESTION 7. The Palermo Convention contains a broad range of provisions to combat drug trafficking and criminalizes money laundering.
   a) True  b) False

QUESTION 8. Resolution 1373 does not require ratification and implementation by a UN member country to have the force of law in that country.
   a) True  b) False

QUESTION 9. Resolution 1267 requires all member countries to deny all forms of support to terrorist organizations.
   a) True  b) False
Every country should take steps to ensure that its AML/CFT legal framework meets international standards. The FATF, the international standard setter for AML/CFT, recognizes that because each country is different, the legal and institutional measures adopted to meet the standards will reflect the characteristics of individual legal systems. Accordingly, FATF’s international standards are established as principles to permit each country to adopt laws consistent with its own legal precepts and constitution, as well as its own cultural and economic circumstances. The international standards are:

- Criminalization of money laundering on the basis of the Vienna and Palermo Conventions (R1)
- Criminalization of terrorist financing and associated money laundering (R1, SRI, SRII)
- Predicate offenses: criminal offenses to be included as predicate offenses for money laundering and methods for describing them (R1)
- Scope of criminal liability (R2)
- Freezing, seizing, and confiscating proceeds of crimes (R3, SRIII)
- Persons and entities subject to AML/CFT requirements (R5, R12)
- Integrity standards (R23, R24, R33, R34)
- Financial institution secrecy laws consistent with implementation of international standards (R4)
- Interagency cooperation (R31)

Now let us look at each of the above requirements.

2.1 Criminalization of money laundering

Countries need to have a legal framework that criminalizes money laundering. Criminalization serves three principal objectives:

- It creates criminal liability for acts that may seem innocent while in reality they are closely linked to criminal activities.
- It establishes a specific basis for greater international cooperation in this critical law enforcement function.
- It compels compliance with AML/CFT preventive measures (covered in Module 3a).
Criminalization of money laundering should be accomplished on the basis of, and in accordance with, the Vienna and Palermo Conventions, as provided in the first paragraph of FATF Recommendation 1. For more information on Recommendation 1, see Appendix B.

**WHAT CATEGORIES OF ACTIVITY MAKE UP THE CRIMINAL OFFENSE OF MONEY LAUNDERING?**

Under the Vienna Convention (articles 3(1)(b)(i) and (ii) and article 3(1)(c)(i)) and the Palermo Convention (article 6(1)), there are three categories of activity that constitute the criminal offense of money laundering. The first two categories have to be incorporated into domestic law; the third category is not mandatory if it contradicts the country’s fundamental legal principles. The categories are as follows:

1) **Conversion or transfer of property.** The conversion or transfer of property, knowing that such property is the proceeds of a crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offense to evade the legal consequences of his or her action;

2) **Concealment or disguise of property.** The concealment or disguise of the true nature, source, location, disposition, movement, or ownership or rights with respect to property, knowing that such property is the proceeds of crime; and

3) **Acquisition, possession, or use of property**: Subject to the country’s fundamental legal principles, the acquisition, possession, or use of property, knowing, at the time of receipt, that such property is the proceeds of crime.

Countries should also criminalize participation in, association with, or conspiracy to commit, attempt to commit and aiding, abetting, facilitating, and counseling the commission of any of the offenses established in accordance with categories 1, 2, and 3 above, unless this is not allowed in accordance with the fundamental legal principles of the country.

Other requirements related to the criminalization of money laundering are discussed in the following sections.

**2.2 Criminalization of terrorist financing and associated money laundering**

Directly related to the criminalization of money laundering is the criminalization of terrorist financing. FATF Special Recommendation II calls upon each country to criminalize the financing of terrorism, terrorist acts, and terrorist organizations. The crime of terrorist financing is defined in Articles 2(1), (4), and (5) of the UN International Convention for the Suppression of the Financing of Terrorism and in the Interpretative Note of Special Recommendation II. In addition, under this Special Recommendation, countries are to ensure that such offenses are designated as predicate offenses for money laundering (see the
next section for a discussion of predicate offenses). For more information on Special Recommendation II, see Appendix C.

Also related to the criminalization of terrorist financing is Special Recommendation I, which calls upon each country to ratify and implement fully the UN International Convention for the Suppression of the Financing of Terrorism. For more information on FATF Special Recommendation I, see Appendix D.

FATF Recommendation 35, which deals with international cooperation, directs all countries to take immediate steps to become a party to and implement fully all three UN conventions—the Vienna and Palermo conventions, as well as the UN International Convention for the Suppression of the Financing of Terrorism. For more information on FATF Recommendation 35, see Appendix E.

2.3 Predicate offenses for money laundering and methods for describing them

2.3.1 The definition of predicate offense

A predicate offense for money laundering is the underlying criminal activity that generates proceeds that, when “laundered” (see the three categories and definitions described in earlier section), lead to the offense of money laundering. The offense of money laundering cannot be committed without the prior commitment of a predicate offense (or underlying crime). It is useful to designate many crimes as predicate offenses for money laundering, so that the crime of money laundering can be used to fight the underlying crimes. This can be accomplished in a number of ways under the international standards.

How does the FATF treat predicate offenses?

FATF Recommendation 1 contains important concepts for a country to use when designating predicate offenses for money laundering. First, using the language of the Palermo Convention, the FATF calls upon each country to include at least all serious offenses, not just those that are drug related, as in the Vienna Convention.

The FATF describes the types or categories of criminal conduct that should be designated as predicate offenses for money laundering, but leaves to the discretion of each country the specific method of designation. This designation may be accomplished by reference to the following:

- All offenses
- A threshold linked either to (a) a category of serious offenses or (b) the penalty of imprisonment applicable to the predicate offense
- A list of predicate offenses
- A combination of the above three approaches.
2.3.2 THE THRESHOLD APPROACH

When the “threshold approach” is used, the predicate offenses should at a minimum cover all offenses designated as “serious offenses” under national law or should include offenses that are punishable by

- a maximum term of imprisonment of more than one year, for countries with maximum penalties; or
- a minimum term of imprisonment of more than six months, for countries with minimum penalties.

In both cases, the penalties cited are the minimums that apply to “serious offenses” for money laundering purposes under the international standards. Countries may choose to include crimes with less severe penalties as predicate offenses for money laundering. Finally, it should be noted that if the threshold approach is used, it must cover all of the 20 crimes listed as “designated categories of offenses” listed in the next section.

2.3.3 DESIGNATED CATEGORIES OF OFFENSES

FATF Recommendation 1 provides in paragraph four that, regardless of the approach used in designating predicate offenses, each country should (at a minimum) include a “range of offenses within each of the designated categories of offenses.” For the categories listed below, each country may decide, in accordance with its domestic law, how it will define the offenses and what elements of those offenses make them serious:

- Participation in an organized criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint, and hostage-taking
- Robbery or theft
- Smuggling
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation
Two points should be made clear:

1) First, the requirement is to include a range of offenses within each of the designated categories of offense. For example, under the category of “robbery or theft,” it is not sufficient to designate the theft of one type of good, such as vehicles, while excluding other types. On the other hand, exclusions based on the value of the stolen good are acceptable because such a theft could be considered as not “serious.”

2) Second, it is not necessary to have a predicate offense described in precisely the same terms as are used in the above listing from the glossary of the Recommendations. As an example, some countries do not have a crime designated as “fraud,” but do criminalize fraudulent behavior under the category of “theft by artifice” or some other name.

See Appendix B for more information on FATF Recommendation 1.

2.3.4 Financing of Terrorism

The financing of terrorism, terrorist acts, and terrorist organizations should be criminalized as predicate offenses to money laundering. A practical way to undermine the capacity of terrorist organizations is to prevent their funds from entering the global financial system in the first place. Failing that, a country needs legislation to detect when terrorist funds have entered its territory so that the funds can be confiscated or forfeited.

Analysis

Try to answer the following questions:

a) How does your country designate predicate offenses for money laundering?
b) Is this method consistent with the FATF requirements?
c) Are all 20 categories of designated offenses currently covered by your country’s laws?
d) Is there interest in your country for going beyond the minimums provided in the FATF Recommendations?
e) Are there other areas that should be covered as money laundering predicate offenses, based on public policy interests?
2.4 Scope of criminal liability

Countries need to consider several other critical legal issues in their AML/CFT legislation.

2.4.1 Cross-border implications

FATF Recommendation 1, in paragraph five, provides that predicate offenses should extend to criminal conduct that occurred outside the country’s borders, if that conduct constituted an offense in the other country and would have constituted an offense had it occurred domestically.

This is the so-called “dual criminality” standard that is the minimum requirement. In the alternative, a country may require only that the conduct would have constituted a predicate offense had it occurred domestically. The standard used in a country may have important consequences for mutual legal assistance, as discussed in a later section of this module.

2.4.2 State of mind

Several critical legal issues are found in Recommendation 2. See Appendix F for more information on FATF Recommendation 2.

In prosecuting a crime, the perpetrator’s “state of mind” is usually relevant. Did the perpetrator know what he or she was doing when engaging in the criminal conduct? Stated differently, what was the perpetrator’s intent or purpose in committing the offense? With regard to the offense of money laundering, the question, according to the Vienna Convention and the Palermo Convention, is whether the perpetrator knew that the funds being handled were the proceeds of the predicate offense.

What are the different standards for determining “state of mind”?

Countries have various options for determining the state of mind connected with a money laundering offense. For example, a country, through its legislature, may determine that “actual knowledge” about the illicit origins of the proceeds may be necessary. This is the hardest standard to satisfy. An alternative is to establish a “should have known” standard—a form of negligent money laundering. Yet another alternative is to determine that suspicion about the illicit origins of the property is sufficient for conviction. Under this approach, the accused neither had actual knowledge nor should have known about the illicit origins of the proceeds, but instead had suspicions about the origins and chose to remain ignorant of the nature of the proceeds. The accused either “could have known” or was “willfully blind” to the origins of the proceeds.

In any event, the Vienna and Palermo Conventions provide that the required state of mind may be inferred from objective factual circumstances.
Module 2

2.4.3 Legal Person and Corporate Liability

Money laundering often occurs through corporate entities—or “legal persons.” The FATF defines legal persons as any “bodies corporate, foundations, anstalt, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property.”

The concept of legal person or corporate liability for crimes varies greatly among different countries, but the FATF recommends that all such entities should be subject to criminal liability. In the alternative, significant civil or administrative sanctions could be a sufficient substitute in cases where the legal or constitutional framework does not subject corporations to criminal liability. Any measures taken against the legal person should not preclude criminal action against individual officers, employees, agents, or representatives of the legal entity.

2.4.4 Liability for Money Laundering of Perpetrators of Predicate Offenses (Self-Laundering)

Is the person who commits the predicate offense personally liable for money laundering, like the person who actually committed the money laundering?

Some countries do not hold the perpetrator of the predicate offense liable for laundering the proceeds of his or her criminal actions. The rationale is that doing so would amount to double punishment for a single crime. Other countries hold the perpetrator of the predicate offense liable for laundering the ill-gotten proceeds, on the grounds that the conduct and the harm of evasion are distinct from the predicate offense.

“State-of-mind” issues

According to the UN Model Legislation, actual knowledge or “having reason to believe” that property is derived from criminal acts constitutes the so-called “mental element” of money laundering. A broad definition of “state of mind” adopted in the Organization of American States’ (OAS) Model Regulations is that (1) the accused had knowledge that the property constituted proceeds of a criminal activity as defined in the convention; (2) the accused should have known that the property was obtained with the proceeds of criminal activity; or (3) the accused was intentionally ignorant of the nature of the proceeds.

Because of the difficulty inherent in proving the state of mind of a person who is engaging in an activity that appears ordinary on its face, the Vienna and Palermo Conventions, FATF Recommendation 2, and many other legal instruments provide that a country’s law should permit the inference of the required state of mind from objective factual circumstances. If the objective factual circumstances fit the situation, the requisite state of mind has been satisfied.
How does the Palermo Convention treat perpetrator liability for money laundering?
The general international standard derived from the provisions of the Palermo Convention is broad, yet it sends a clear message. The perpetrator should be held liable for laundering the proceeds of his or her own criminal activities, except if this is not allowed due to the fundamental principles of the national legislation.

2.4.5 LAWYERS’ FEES

Because lawyers are now among the designated non-financial businesses and professions (DNFBPs) that must be considered as covered by a country’s AML/CFT regime (see Module 3a), care should be taken when drafting the scope of predicate offenses not to criminalize the receipt of a fee for defending the accused criminal.

Knowledge check

Answer the following questions and explain the basis of your answer:

QUESTION 10. The Vienna and Palermo Conventions define three categories of activities as constituting the crime of money laundering.
   a) True       b) False

QUESTION 11. Countries have discretion in defining the crime of money laundering.
   a) True       b) False

QUESTION 12. To sustain a charge of money laundering, there must be an underlying crime—a predicate offense.
   a) True       b) False
**QUESTION 13.** The FATF provides countries with discretion in describing predicate offenses for money laundering.

   a) True  b) False

---

**QUESTION 14.** Countries must use the exact wording of the 20 designated categories of offenses to describe the predicate offenses.

   a) True  b) False

---

**QUESTION 15.** A person may not be convicted of money laundering if the predicate offense occurs in another country.

   a) True  b) False

---

### 2.5 Freezing, seizing, and confiscating proceeds of crimes

The current international approaches to fighting crimes, including money laundering and terrorist financing, are designed to make these criminal activities unprofitable and keep terrorists from accessing funds. Therefore, effective confiscation laws are indispensable for authorities to deprive criminals of their ill-gotten proceeds and terrorists of their funds, no matter how those funds were derived. Confiscation measures fall into three main areas: freezing, seizing, and actual confiscation of the proceeds of crimes, which are funds or other assets.

Let’s think for a moment about terminology. Consider your own definition of the terms used in confiscation measures—freezing, seizure, and confiscation—and compare your definitions to those given by the FATF.
**What is the freezing of assets?**
The term *freeze* means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.

**What is the seizure of assets?**
The competent judicial authorities or officials responsible for the detection and suppression of money laundering offenses shall be empowered to seize property connected with the offense under investigation as well as any evidentiary items that may make it possible to identify such property.

The term *seize* means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is effected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration, or management of the seized funds or other assets.

**What is confiscation?**
The term *confiscate*, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to the state. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets. Confiscation or forfeiture orders usually are linked to a criminal conviction or court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

Confiscation measures are discussed or contained in two FATF Recommendations: Recommendation 3 on money laundering and Special Recommendation III on terrorist financing.

In Recommendation 3, the FATF encourages countries to adopt a broad interpretation of the confiscation of the proceeds of crime, in accordance with the Vienna and Palermo Conventions. In the past, confiscation was largely confined to instruments used in the crime, such as the weapon used in a murder or attack, or the subject of the crime, such as drugs involved in drug trafficking, as opposed to the proceeds derived from the crime. Such an approach has proved
highly inadequate in light of the use of the proceeds generated from crimes and the ease with which these proceeds can be moved internationally. In addition, criminals are likely to convert specific assets to another form to avoid an order naming particular proceeds and transfer the converted assets beyond the borders of the jurisdiction.

This is why Recommendation 3 requires countries to extend confiscation measures and related provisional measures to property laundered, proceeds from money laundering or predicate offenses, instrumentalities used in or intended for use in the commission of these offenses, or property of corresponding value. For more information on FATF Recommendation 3, see Appendix G.

Special Recommendation (SR) III specifically discusses the concepts of freezing, seizure, and confiscation in relation to terrorist funds. Under Special Recommendation III, indefinite freezing and seizing occur on the authority of UN Security Council Resolutions 1267 (and its successors) and 1373, and of the 1267 Committee. It applies to any assets owned by or under the control of the parties designated pursuant to the UN Security Council resolutions. See Appendix H for more information on FATF Special Recommendation III.

Interpretative Note to Special Recommendation III: Freezing and Confiscating Terrorist Assets states that jurisdictions have two obligations:

- To implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant UN resolutions
- To have measures in place that permit it to seize and confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court

Further detailed guidance is available from the Interpretative Note of Special Recommendation III in Appendix H.

The FATF has identified a set of best practices based on experience to date in many jurisdictions. These may serve as a benchmark for developing institutional, legal, and procedural frameworks for an effective regime to freeze assets used in terrorist financing:

- Establishing effective regimes and competent authorities or courts
- Facilitating communication and cooperation with foreign governments and international institutions
- Facilitating communication with the private sector
- Ensuring adequate compliance, controls, and reporting in the private sector
- Ensuring thorough follow-up investigation; coordination with law enforcement, intelligence, and security authorities; and appropriate feedback to the private sector
Analysis

1) Why do we need confiscation when we have other penalties or measures, such as imprisonment?

A penalty of imprisonment or a fine to individuals would not necessarily deprive criminals of the fruits of crime in the same proportion as confiscating the proceeds of the crime. The same rationale applies to legal persons and corporate entities. Until it is confiscated, property can be transferred and still benefit criminals and terrorists. Unless assets are confiscated, other terrorists will have access to the funds to carry out their activities.

2) What type of property do international instruments encourage countries to subject to confiscation?

Laws that permit the confiscation of direct and indirect proceeds of crime to the greatest extent, including confiscation of assets of comparable value owned by the criminals and terrorists, helps the most to deprive criminals and terrorists of the use of proceeds of criminal activities and terrorist funds.

3) What powers do the competent authorities need to be able to effectively implement confiscation measures?
4) What other measures should be incorporated in the law on confiscation?

Countries need to take measures to protect the rights of (bona fide) third parties because international law on confiscation does not preclude the confiscation of assets in the hands of third parties. Countries should create cooperative mechanisms for enforcing cross-border provisional measures and confiscation orders.

2.6 Persons and entities subject to AML/CFT requirements

In general, the preventive measures of FATF Recommendations 5 through 16, 18, 21, and 22 apply to all “financial institutions,” while only certain of such measures apply, to varying degrees, to “designated non-financial businesses and professions” (see Module 3a). Accordingly, a country’s laws or regulations should specifically make such persons and entities subject to the AML/CFT requirements.

The following boxes restate the definitions of terms found in the glossary to the FATF Recommendations and categorize financial institutions, non-financial businesses, and professions that are subject to AML/CFT requirements. (These are functional definitions; they are not determined by an institution’s legal designation. The test is whether an entity or individual carries out any of the above functions or activities for customers, and not what the business is called or how it is designated.)
Financial institutions

“Financial institution” is defined as any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

- Acceptance of deposits and other repayable funds from the public. This also captures private banking.
- Lending. This includes *inter alia*, consumer credit, mortgage credit, factoring with or without recourse, and finance of commercial transactions (including forfeiting).
- Financial leasing. This does not extend to financial leasing arrangements in relation to consumer products.
- The transfer of money or value. This applies to financial activity in both the formal or informal sector—for example, alternative remittance activity. (See the FATF Web site for the Interpretative Note to Special Recommendation VI.) It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. (See the FATF Web site for the Interpretative Note to Special Recommendation VII.)
- Issuing and managing means of payment—credit and debit cards, checks, traveler’s checks, money orders, bankers’ drafts, electronic money.
- Financial guarantees and commitments.
- Trading in:
  - Money market instruments (checks, bills, CDs, derivatives, and so on)
  - Foreign exchange
  - Exchange, interest rate, and index instruments
  - Transferable securities
  - Commodity futures trading
- Participation in securities issues and the provision of financial services related to such issues.
- Individual and collective portfolio management.
- Safekeeping and administration of cash or liquid securities on behalf of other persons.
- Otherwise investing, administering, or managing funds or money on behalf of other persons.
- Underwriting and placement of life insurance and other investment related insurance. This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).
- Money and currency changing.
2.6.1 Possible exceptions

A country may determine which financial institutions and other businesses and professions are to be covered by the country’s AML/CFT framework and to what extent that framework applies.

There are two bases for exemption from the FATF standards.

The first is where the financial activity is carried out on an occasional or limited basis. For example, possible exceptions could include a hotel that offers very limited foreign exchange to guests on an occasional basis or a travel agency that wires money to clients overseas in emergencies.

The second basis for an exemption is for strictly limited and justified circumstances, provided the country has a rationale for the exception that is based on a proven low risk of money laundering. Presumably, exemptions under this category would be justified in countries where certain types of financial institutions or businesses engage in limited numbers of small-value transactions and, therefore, pose little risk of money laundering. Any such exemptions should also be made part of the legal structure governing AML/CFT requirements.

Non-financial businesses and professions

“Designated non-financial businesses and professions” means:

- Casinos, including Internet casinos
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Lawyers, notaries, other independent legal professionals, and accountants. This refers to sole practitioners, partners, and employed professionals in professional firms. It is not meant to refer to “internal” professionals who are employees of other types of businesses, or to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
- Trust and company service providers refers to all persons and businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
  - Acting as a formation agent of legal persons
  - Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
  - Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal person or arrangement
  - Acting as (or arranging for another person to act as) a trustee of an express trust
  - Acting as (or arranging for another person to act as) a nominee shareholder for another person
2.6.2 Possible additions to persons and entities covered

FATF Recommendation 20 provides that, in addition to the persons and entities covered as non-financial businesses and professions by the FATF Recommendations (unless exempted), countries should consider other businesses and professions for coverage. The basis for the recommendation is that such other businesses and professions pose a money laundering or terrorist financing risk. In the same recommendation, the FATF further encourages countries to develop and use modern and secure money management techniques that are less vulnerable to money laundering. In essence, this suggestion encourages less reliance on cash and more reliance on payment systems that provide complete and accurate information on senders and receivers of funds and make it easy to trace transactions.

Countries should examine their economies to identify any unique features that would cause other businesses or professions to pose a money laundering or terrorist financing risk. For more information on FATF Recommendation 20, see Appendix I.

2.7 Integrity standards

2.7.1 Financial institutions

When criminals control financial institutions or hold senior management positions, countries find it exceedingly difficult to prevent and detect money laundering. Accordingly, FATF Recommendation 23 provides that financial institutions should be subject to adequate supervision and regulation to ascertain that they are effectively implementing the FATF Recommendations. In this regard, the laws and regulatory measures of a country should be written so that competent authorities can prevent criminals and their associates from owning or controlling significant investments, including beneficial interests, in any of the country’s covered financial institutions. Similarly, convicted criminals should be prevented from holding any significant management position with such financial institutions, including positions on the board of directors, executive or supervisory board, or comparable positions.

For example, a country should establish a licensing structure for owning or holding a significant interest in, or beneficial ownership of, a financial institution. Similarly, there should be an effective mechanism to withdraw the license of a financial institution on the basis of substantial irregularities relating to money laundering or the financing of terrorism. The withdrawal of the license should also occur if the financial institution fails to maintain standards of integrity when its large shareholders or management officials change.

For financial institutions subject to regulation under the Core Principles,6 prudential regulation and supervision, including licensing requirements, should be

---

6 “Core Principles” refers to the Core Principles for Effective Banking Supervision, issued by the Basel Committee on Banking Supervision; the Objectives and Principles for Securities Regulation, issued by the International Organization of Securities Commissions; and the Insurance Supervisory Principles, issued by the International Association of Insurance Supervisors.
employed. Other types of financial institutions should be licensed or registered and appropriately regulated according to the risk of money laundering or terrorist financing. For more information on FATF Recommendation 23, see Appendix J.

### 2.7.2 Designated Non-Financial Businesses and Professions (DNFBPs)

Under FATF Recommendation 24, DNFBPs, and any other covered entities and persons, should be subject to appropriate supervision and regulation for purposes of ensuring compliance with AML/CFT requirements. Like financial institutions, casinos should be licensed: criminals and their associates should be prevented from owning or controlling significant investments, beneficial ownership interests, and significant management positions in casinos. Other types of non-financial businesses and professions should be subject to effective systems for monitoring and assuring compliance with AML/CFT requirements if and only if they pose risk of money laundering or terrorist financing. These functions may be performed by a governmental authority or by a self-regulatory organization, if there is sufficient authority to assure compliance. For more information on FATF Recommendation 24, see Appendix K.

### 2.7.3 Integrity of Legal Persons and Arrangements

FATF Recommendations 33 and 34 extend the scope of Recommendation 23 to legal persons and legal arrangements. FATF Recommendation 33 requires that countries should take measures to prevent the unlawful use of legal persons by money launderers, in particular that countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money launderers. Recommendation 34 requires that countries should take measures to prevent the unlawful use of legal arrangements by money launderers. For more information on FATF Recommendation 33, see Appendix L. For more information on FATF Recommendation 34, see Appendix M.

### 2.8 Laws consistent with implementation of international standards

Many countries have very strict bank privacy or secrecy laws that either pre-empt or prevent the effective implementation of a number of FATF Recommendations. This is particularly true for certain investigations and disclosures that are essential for an effective AML/CFT regime. To overcome such provisions, FATF Recommendation 4 specifically provides that countries should make certain that their financial institution secrecy laws do not inhibit implementation of any of the FATF Recommendations.
While this Recommendation is specific to secrecy laws, you will want to look at the overall structure of your country’s legal system to see if there are any conflicts with other laws that would inhibit implementation of any of the FATF Recommendations.

FATF Recommendation 4 states: “countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.” 

2.9 Interagency cooperation

An effective AML/CFT regime requires that supervisors of financial institutions, law enforcement authorities, prosecutors, and the staff of the FIU should be able to cooperate with each other and, depending upon the country’s legal system, coordinate their efforts regarding AML/CFT matters. Recognizing this, the FATF makes interagency cooperation a requirement under Recommendation 31. Countries should ensure that there are mechanisms in place to enable its agencies to cooperate and coordinate their policies and activities to combat money laundering and terrorist financing. These mechanisms are discussed in Module 5.

In many cases, however, it may not be sufficient for agencies simply to want to cooperate. They may, in fact, be precluded from doing so by law or under their authorizing charter. As a consequence, it may be necessary to authorize them legislatively (or by other equally effective means) to cooperate and coordinate with each other. You should examine the operating laws and rules governing the agencies involved in AML/CFT in your country to determine whether legislative or other action is necessary to authorize coordination and cooperative efforts. For more information on Recommendation 31, see Appendix N.
What are the legal issues related to international cooperation?

In the context of fighting money laundering from the global standpoint, rapid exchanges of information and effective cooperation among the various agencies within a country and counterparts from other countries throughout the world have become a prerequisite to success.

International cooperation is discussed in detail in Module 5. In this section, we will consider only the legal elements affecting such cooperation. The following subtopics are important in understanding and enhancing international cooperation.

3.1. Mutual legal assistance (Recommendation 35, 36, and 37 and Special Recommendation V)
3.2. International aspects of confiscation (Recommendation 38)
3.3. Extradition (Recommendation 39 and Special Recommendation V)
3.4. Other forms of international cooperation (Recommendation 40)

3.1 Mutual legal assistance

As noted previously, FATF Recommendation 35 provides that each country should take immediate steps to become a party to and implement fully the Vienna and Palermo Conventions and the UN International Convention for the Suppression of the Financing of Terrorism.

Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

FATF Recommendation 36 provides that countries should provide the widest possible range of mutual legal assistance with other jurisdictions for purposes of information exchange, investigations, and court proceedings connected with money laundering and terrorist financing.

Mutual assistance may include the following:

- Taking evidence or statements from persons
- Assisting in making detained persons or others available to the judicial authorities of the requesting state to give evidence or assist in investigations
- Service of judicial documents
• Carrying out searches and seizures and freezing
• Examining objects and sites
• Providing information, evidentiary items, and expert evaluations
• Providing originals or certified copies of relevant documents and records, including bank, financial, corporate, and business records
• Identifying or tracing proceeds of crime, property, instrumentalities, or other things for evidentiary purposes

For more information on FATF Recommendation 36, see Appendix O.

FATF Recommendation 37 also provides that mutual legal assistance should be rendered even if the standard of dual criminality is not met—that is, if the offense in question was not an offense in one of the countries. If dual criminality is required under the country’s legal system, it should be interpreted in a way that looks at the conduct involved in the underlying offense, and not at the specific terminology used. For more information on FATF Recommendation 37, see Appendix P.

Special Recommendation V provides that each country should afford other countries, through mutual legal assistance or other mechanisms, the greatest possible assistance in connection with criminal and civil enforcement and administrative investigations, inquiries, and proceedings related to the financing of terrorism and terrorists acts and organizations. For more information on FATF Special Recommendation V, see Appendix Q.

3.2 International aspects of confiscation

Establishing an effective confiscation regime for domestic purposes is only the first step toward eliminating the profitability at the heart of so many international money laundering activities. The second necessary step, and one vital to the overall success of this effort, is creating cooperative mechanisms for enforcing cross-border confiscation orders. Countries should consider enabling the relevant authorities to implement confiscation requests from other countries, employing such measures as the tracing, identification, freezing, seizing, and ultimately, the confiscation of property.

As an incentive for expeditious action and international cooperation, countries may wish to consider establishing asset-sharing arrangements. The general principle in the disposal of confiscated assets is that such disposal should be subject to the domestic laws and regulations of the country that executed the confiscation order. The international statements, including FATF Recommendation 38, encourage countries to enter into mutual arrangements that provide for the sharing of the confiscated property among all the countries that cooperated in the investigation and confiscation process. For more information on FATF Recommendation 38, see Appendix R.
3.3 Extradition
FATF Recommendation 39 provides that each country should recognize money laundering as an extraditable offense. Countries should have procedures in place to extradite, where possible, individuals charged with money laundering or related offenses.

Subject to its legal framework, each country may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, extraditing their nationals, or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.

In addition, where a country’s laws prohibit extradition solely on nationality grounds, the country should, at the request of the foreign country seeking extradition, submit the case promptly to its competent authorities for prosecution. For more information on FATF Recommendation 39, see Appendix S.

Similarly, FATF Special Recommendation V requires countries to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts, or terrorist organizations and to have procedures in place to extradite such individuals. For more information on FATF Special Recommendation V, see Appendix Q.

3.4 Other forms of international cooperation
In addition to the foregoing mechanisms, FATF Recommendation 40 urges all countries to provide the widest range of international cooperation to their foreign counterparts. Specifically, such cooperative efforts should include:

- Not refusing assistance solely because it also involves fiscal (tax) matters
- Not withholding cooperation on grounds of secrecy or confidentiality
- Permitting competent authorities to conduct inquiries on behalf of foreign counterparts

In addition, safeguards should be put in place to assure confidentiality and privacy, consistent with the authorized use of the information exchanged. For more information on FATF Recommendation 40, see Appendix T.

Analysis
Let us now consider how some of the issues discussed above apply to your country. Some suggestions have been made to enable you to construct your thoughts.

1) What laws and regulations in your country apply to money laundering?
2) What laws and regulations in your country apply to terrorist financing?

Suggestions: Consider whether the AML laws and regulations are concentrated in one section of your legal code or are scattered among several sections. Are the criminal provisions part of the criminal code?

3) Do you know whether these laws satisfy all of the required international standards?

Suggestions: Do the CFT provisions stand alone, or are they part of other statutes and regulations?

3) Do you know whether these laws satisfy all of the required international standards?

Suggestions: Has your country had an assessment? If not, you may use the questionnaire and methodology documents to test the existence and the efficacy of the laws.

4) How effective have your country’s laws been in fighting money laundering and terrorist financing?

Suggestions: Are there statistics on Suspicious Transaction Reports (STRs), investigations, prosecutions, confiscations, interagency cooperation, and international cooperation?
5) If they have not been effective, can you describe the problems?

Suggestions: Have the problems been in certain cases? Have the problems been with the legal authority? Have the problems been with resources?

6) Are there other problems that should be addressed, and why?

Suggestions: Is there an FIU? Do different authorities work together?
Check the following sources, and others, for the latest models that may be available for you to draft AML/CFT legislation:

- United Nations Office on Drugs and Crime (UNODC)
- International Monetary Fund (IMF)
- Commonwealth Secretariat
- Organization of American States (OAS)

**Check your understanding**

**QUESTION 16.** The Vienna Convention contains a broad range of provisions to fight organized crime.

a) True  

b) False

**QUESTION 17.** The Palermo Convention has the force of law in all member countries of the UN.

a) True  

b) False

**QUESTION 18.** To be convicted of money laundering, the perpetrator must also be convicted of the predicate offense.

a) True  

b) False

**Summary**

In this module, we discussed

- relevant international conventions and treaties;  
- the objectives of those conventions and treaties;  
- legal and institutional requirements in AML/CFT;  
- issues to consider in criminalizing money laundering and terrorist financing;  
- provisional and confiscation measures in AML/CFT;  
- individuals and entities subject to AML/CFT laws and regulations; and  
- legal issues in international and interagency cooperation.
Appendix A: References

FATF Recommendations

  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- *Special Recommendations on Terrorist Financing* (FATF, October 2004)

Useful Web sites

- Model Laws: International Money Laundering Information Network (IMoLIN)
- Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD)
  http://www.cicad.oas.org/
- United Nations (UN)
  http://www.un.org
- United Nations Treaty Collection: Conventions on Terrorism (UN)
  http://untreaty.un.org/English/Terrorism.asp

Reference Documents

  http://www.fatf-gafi.org/dataoecd/30/43/34242709.pdf
- Interpretative Note to Special Recommendation III: Freezing and Confiscating Terrorist Assets (FATF, October 2004)
- *United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: Vienna Convention* (UN, 1988)
  http://www.unodc.org/adhoc/palermo/convmain.html
• Revised CFATF 19 Recommendations (CFATF, October 1999)
• Kingston Declaration on Money Laundering (CFATF, November 1992)
• Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime: The Strasbourg Convention (Council of Europe, September 1990)
• Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism: The Warsaw Convention (Council of Europe, May 2005)
• Riga Declaration on the Fight against Money Laundering (European Commission, November 1996)
  http://www.imolin.org/imolin/en/EUdir01e.html

Reference Documents (Model Legislation)
• UNODC Model Money Laundering, Proceeds of Crime, and Terrorist Financing Bill 2003 (UNODC 2003) [for common law systems]
  http://www.imolin.org/imolin/en/poctf03.html
• Model legislation on laundering, confiscation, and international cooperation in relation to the proceeds of crime (UN, 1999) [for civil law systems]
• Mutual assistance and international cooperation in criminal matters (UN, 1998) [for common law systems]
• United Nations Model Foreign Evidence Bill, 2000 (UN, 2000) [for common law systems]
• United Nations Model Extradition (Amendment) Bill 2000 (UN, 2000) [for common law systems]
• Commonwealth Model Law for the Prohibition of Money Laundering & Supporting Documentation (Commonwealth Secretariat, 1996)
• Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses (OAS/CICAD, July 2002)
Recommendation 1

Countries should criminalise money laundering on the basis of UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and UN Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offences under their national law or should include offences that are punishable by a maximum penalty of more than one year’s imprisonment or for those countries that have a minimum threshold for offences in their legal system, predicate offences should include all offences that are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offences within each of the designated categories of offences.

Predicate offences for money laundering should extend to conduct that occurred in another country that constitutes an offence in that country and that would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.
Appendix C: FATF Special Recommendation II

Each country should criminalise the financing of terrorism, terrorist acts, and terrorist organizations. Countries should ensure that such offences are designated as money laundering predicate offences.

Interpretative Note to Special Recommendation II: Criminalising the financing of terrorism and associated money laundering

Objective

1) Special Recommendation II was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and inter alia money laundering, another objective of Special Recommendation II is to emphasize this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. The basis for criminalising terrorist financing should be the United Nations International Convention for the Suppression of the Financing of Terrorism, 1999 [1].

Definitions

2) For the purposes of Special Recommendation II and this Interpretative Note, the following definitions apply:

a) The term *funds* refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, letters of credit.

b) The term *terrorist* refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.

e) The term terrorist organisation refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Characteristics of the Terrorist Financing Offence

3) Terrorist financing offences should extend to any person who willfully provides or collects 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: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.

4) Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.

5) Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.

6) Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).
7) It should also be an offence to attempt to commit the offence of terrorist financing.

8) It should also be an offence to engage in any of the following types of conduct:
   a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
   b) Organising or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note;
   c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offence; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offence.

9) Terrorist financing offences should be predicate offences for money laundering.

10) Terrorist financing offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organization(s) is located or the terrorist act(s) occurred/will occur.

11) The law should permit the intentional element of the terrorist financing offence to be inferred from objective factual circumstances.

12) Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.

13) Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil or administrative proceedings in countries in which more than one form of liability is available.

14) Natural and legal persons should be subject to effective, proportionate, and dissuasive criminal, civil or administrative sanctions for terrorist financing.

[1] Although the UN Convention had not yet come into force at the time that Special Recommendation II was originally issued in October 2001—and thus is not cited in the Special Recommendation itself—the intent of the FATF has been from the issuance of Special Recommendation II to reiterate and reinforce the criminalization standard as set forth in the Convention (in particular, Article 2). The Convention came into force in April 2003.
Guidance Notes by FATF (Excerpt)

**SPECIAL RECOMMENDATION II: CRIMINALISING THE FINANCING OF TERRORISM AND ASSOCIATED MONEY LAUNDERING**

This Recommendation contains two elements:

- Jurisdictions should criminalise “the financing of terrorism, of terrorist acts and of terrorist organisations”; and
- Jurisdictions should establish terrorist financing offences as predicate offences for money laundering.

In implementing SR II, jurisdictions must either establish specific criminal offences for terrorist financing activities, or they must be able to cite existing criminal offences that may be directly applied to such cases. The terms *financing of terrorism* or *financing of terrorist acts* refer to the activities described in the UN Convention (Article 2) and S/RES/1373(2001), paragraph 1b (see the UN website at http://www.un.org/documents/scres.htm for text of this Resolution). It should be noted that each jurisdiction should also ensure that terrorist financing offences apply as predicate offences even when carried out in another state. This corollary interpretation of SR II is then consistent with FATF Recommendation 4.

FATF Recommendation 4 already calls for jurisdictions to designate “serious offences” as predicates for the offence of money laundering. Special Recommendation II builds on Recommendation 4 by requiring that, given the gravity of terrorist financing offences, terrorism financing offences should be specifically included among the predicates for money laundering. For the full text of the FATF Forty Recommendations, along with their Interpretative Notes, see the FATF website at http://www.fatfgafi.org/40Recs_en.htm.

Finally, as in general with other predicates for money laundering, jurisdictions should ensure that terrorist financing offences are predicate offences even if they are committed in a jurisdiction different from the one in which the money laundering offence is being applied.
Each country should take immediate steps to ratify and to implement fully the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

Guidance Notes by the FATF (Excerpt)

**SPECIAL RECOMMENDATION I: RATIFICATION AND IMPLEMENTATION OF UN INSTRUMENTS**

This Recommendation contains six elements:

- Jurisdictions should ratify and fully implement the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism, and

For the purposes of this special Recommendation, **ratification** means having carried out any necessary national legislative or executive procedures to approve the UN Convention and having delivered appropriate ratification instruments to the United Nations. **Implementation** as used here means having put measures in place to bring the requirements indicated in the UN Convention and UNSC Resolutions into effect. The measures may be established by law, regulation, directive, decree or any other appropriate legislative or executive act according to national law.

The UN Convention was open for signature from 10 January 2000 to 31 December 2001, and upon signature is subject to ratification, acceptance or approval. Ratification, acceptance or approval instruments **must** be deposited with the Secretary-General of the United Nations in New York. Those countries that have not signed the Convention may accede to it (see Article 25 of the Convention).

The full text of the UN Convention may be consulted at [http://untreaty.un.org/English/Terrorism.asp](http://untreaty.un.org/English/Terrorism.asp). As of 19 March 2002, 132 countries have signed, and 24...
have deposited ratification instruments. On 10 March 2002, the UN Convention reached the minimum number of ratifications (22) stipulated as necessary for it to come into effect. The effective date of the convention is 10 April 2002. The Web page containing information on the status of the Convention is located on the UN website at http://untreaty.un.org/ENGLISH/status/Chapter_xviii/treaty11.asp.


Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.
Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.
Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State's ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.
Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or is used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

**Interpretative Note to Special Recommendation III: Freezing and Confiscating Terrorist Assets**

**Objectives**

1) FATF Special Recommendation III consists of two obligations. The first requires jurisdictions to implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant United Nations resolutions. The second obligation of Special Recommendation III is to have measures in place that permit a jurisdiction to seize or confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court.

2) The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative, while the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.

**Scope**

3) Special Recommendation III is intended, with regard to its first requirement, to complement the obligations in the context of the United Nations Security Council resolutions relating to the prevention and suppression of
the financing of terrorist acts—S/RES/1267(1999) and its successor resolutions,7 S/RES/1373(2001) and any prospective resolutions related to the freezing, or if appropriate seizure, of terrorist assets. It should be stressed that none of the obligations in Special Recommendation III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil, or administrative investigation or proceeding.8 The focus of Special Recommendation III instead is on the preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups.

4) S/RES/1267(1999) and S/RES/1373(2001) differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations.

5) S/RES/1267(1999) and its successor resolutions obligate jurisdictions to freeze without delay the funds or other assets owned or controlled by Al-Qaida, the Taliban, Usama bin Laden, or persons and entities associated with them as designated by the UN Al-Qaida and Taliban Sanctions Committee established pursuant to United Nations Security Council Resolution 1267 (the Al-Qaida and Taliban Sanctions Committee). This includes funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons’ benefit, by their nationals or by any person within their territory. The Al-Qaida and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999). All jurisdictions that are members of the UN are obligated by S/RES/1267(1999) to freeze the assets of persons and entities so designated by the Al-Qaida and Taliban Sanctions Committee.9

6) S/RES/1373(2001) obligates jurisdictions10 to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of

---


8 For instance, both the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) and UN Convention against Transnational Organized Crime (2000) contain obligations regarding freezing, seizure, and confiscation in the context of combating transnational crime. Those obligations exist separately and apart from obligations that are set forth in S/RES/1267(1999), S/RES/1373(2001), and Special Recommendation III.

9 When the UNSC acts under Chapter VII of the UN Charter, the resolutions it issues are mandatory for all UN members.

10 The UNSC was acting under Chapter VII of the UN Charter in issuing S/RES/1373(2001) (see previous footnote).
persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective co-operation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organisation, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

**DEFINITIONS**

7) For the purposes of Special Recommendation III and this Interpretive Note, the following definitions apply:

a) The term freeze means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.

b) The term seize means to prohibit the transfer, conversion, disposition or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is affected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration, or management of the seized funds or other assets.

c) The term confiscate, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the state. In this case,
the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets.\textsuperscript{11}

d) The term \textit{funds or other assets} means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, travellers cheques, bank cheques, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends or other income on or value accruing from or generated by such funds or other assets.

e) The term \textit{terrorist} refers to any natural person who: (i) commits, or attempts to commit, terrorist acts\textsuperscript{12} by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts or terrorist financing; (iii) organises or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.

f) The phrase \textit{those who finance terrorism} refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.

g) The term \textit{terrorist organisation} refers to any legal person, group, undertaking or other entity owned or controlled directly or indirectly by a terrorist(s).

\textsuperscript{11} Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.

h) The term designated persons refers to those persons or entities designated by the Al-Qaida and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).

i) The phrase without delay, for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaida and Taliban Sanctions Committee. For the purposes of S/RES/1373(2001), the phrase without delay means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organisation. The phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Freezing without delay terrorist-related funds or other assets

8) In order to fulfill the preventive intent of Special Recommendation III, jurisdictions should establish the necessary authority and adopt the following standards and procedures to freeze the funds or other assets of terrorists, those who finance terrorism, and terrorist organisations in accordance with both S/RES/1267(1999) and S/RES/1373(2001):

a) Authority to freeze, unfreeze and prohibit dealing in funds or other assets of designated persons. Jurisdictions should prohibit by enforceable means the transfer, conversion, disposition or movement of funds or other assets. Options for providing the authority to freeze and unfreeze terrorist funds or other assets include:

(i) empowering or designating a competent authority or a court to issue, administer and enforce freezing and unfreezing actions under relevant mechanisms, or
(ii) enacting legislation that places responsibility for freezing the funds or other assets of designated persons publicly identified by a competent authority or a court on the person or entity holding the funds or other assets and subjecting them to sanctions for non-compliance.

The authority to freeze and unfreeze funds or other assets should also extend to funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by such terrorists, those who finance terrorism, or terrorist organisations.

Whatever option is chosen there should be clearly identifiable competent authorities responsible for enforcing the measures.

The competent authorities shall ensure that their nationals or any persons and entities within their territories are prohibited from making any funds or other assets, economic resources, or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit
of: designated persons, terrorists; those who finance terrorism; terrorist organisations; entities owned or controlled, directly or indirectly, by such persons or entities; and persons and entities acting on behalf of or at the direction of such persons or entities.

b) Freezing procedures. Jurisdictions should develop and implement procedures to freeze the funds or other assets specified in paragraph (c) below without delay and without giving prior notice to the persons or entities concerned. Persons or entities holding such funds or other assets should be required by law to freeze them and should furthermore be subject to sanctions for noncompliance with this requirement. Any delay between the official receipt of information provided in support of a designation and the actual freezing of the funds or other assets of designated persons undermines the effectiveness of designation by affording designated persons time to remove funds or other assets from identifiable accounts and places. Consequently, these procedures must ensure (i) the prompt determination whether reasonable grounds or a reasonable basis exists to initiate an action under a freezing mechanism and (ii) the subsequent freezing of funds or other assets without delay upon determination that such grounds or basis for freezing exist. Jurisdictions should develop efficient and effective systems for communicating actions taken under their freezing mechanisms to the financial sector immediately upon taking such action. As well, they should provide clear guidance, particularly financial institutions and other persons or entities that may be holding targeted funds or other assets on obligations in taking action under freezing mechanisms.

c) Funds or other assets to be frozen or, if appropriate, seized. Under Special Recommendation III, funds or other assets to be frozen include those subject to freezing under S/RES/1267(1999) and S/RES/1373(2001). Such funds or other assets would also include those wholly or jointly owned or controlled, directly or indirectly, by designated persons. In accordance with their obligations under the United Nations International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention (1999)), jurisdictions should be able to freeze or, if appropriate, seize any funds or other assets that they identify, detect and verify, in accordance with applicable legal principles, as being used by, allocated for, or being made available to terrorists, those who finance terrorists or terrorist organisations. Freezing or seizing under the Terrorist Financing Convention (1999) may be conducted by freezing or seizing in the context of a criminal investigation or proceeding. Freezing action taken under Special Recommendation III shall be without prejudice to the rights of third parties acting in good faith.

d) De-listing and unfreezing procedures. Jurisdictions should develop and implement publicly known procedures to consider de-listing requests upon satisfaction of certain criteria consistent with international obliga-
tions and applicable legal principles, and to unfreeze the funds or other assets of de-listed persons or entities in a timely manner. For persons and entities designated under S/RES/1267(1999), such procedures and criteria should be in accordance with procedures adopted by the Al-Qaida and Taliban Sanctions Committee under S/RES/1267(1999).

e) Unfreezing upon verification of identity. For persons or entities with the same or similar name as designated persons, who are inadvertently affected by a freezing mechanism, jurisdictions should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner upon verification that the person or entity involved is not a designated person.

f) Providing access to frozen funds or other assets in certain circumstances. Where jurisdictions have determined that funds or other assets, which are otherwise subject to freezing pursuant to the obligations under S/RES/1267(1999), are necessary for basic expenses; for the payment of certain types of fees, expenses and service charges; or for extraordinary expenses, jurisdictions should authorize access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and subject to approval of the Al-Qaida and Taliban Sanctions Committee. On the same grounds, jurisdictions may authorize access to funds or other assets, if freezing measures are applied pursuant to S/RES/1373(2001).

g) Remedies. Jurisdictions should provide for a mechanism through which a person or an entity that is the target of a freezing mechanism in the context of terrorist financing can challenge that measure with a view to having it reviewed by a competent authority or a court.

h) Sanctions. Jurisdictions should adopt appropriate measures to monitor effectively the compliance with relevant legislation, rules, or regulations governing freezing mechanisms by financial institutions and other persons or entities that may be holding funds or other assets as indicated in paragraph 8(c) above. Failure to comply with such legislation, rules, or regulations should be subject to civil, administrative or criminal sanctions.

**Seizure and Confiscation**

9) Consistent with FATF Recommendation 3, jurisdictions should adopt measures similar to those set forth in Article V of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), Articles 12 to 14 of the United Nations Convention on Transnational Organised Crime (2000), and Article 8 of the Terrorist Financing Convention (1999), including legislative measures, to enable their courts or competent authorities to seize and confiscate terrorist funds or other assets.

---

13 See Article 1, S/RES/1452(2002) for the specific types of expenses that are covered.
**Guidance Notes by the FATF (Excerpt)**

**SPECIAL RECOMMENDATION III: FREEZING AND CONFISCATING TERRORIST ASSETS**

This recommendation contains three major elements:

- Jurisdictions should have the authority to **freeze** funds or assets of (a) terrorists and terrorist organisations and (b) those who finance terrorist acts or terrorist organisations;
- They should have the authority to **seiz[e]** (a) the proceeds of terrorism or of terrorist acts, (b) the property used in terrorism, in terrorist acts or by terrorist organizations, and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organisations; and
- They should have the authority to **confiscate** (a) the proceeds of terrorism or of terrorist acts; (b) the property used in terrorism, in terrorist acts or by terrorist organizations and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organisations.

The term *measures*, as used in SR III, refers to explicit (legislative or regulatory) provisions or “executive powers” that permit the three types of action. As with the preceding Recommendation, it is not necessary that the texts authorising these powers mention terrorist financing in particular. However, jurisdictions with already existing laws must be able to cite specific provisions that permit them to freeze, to seize or to confiscate terrorist related funds and assets within the national legal/judicial context.

The definitions of the concepts of **freezing**, **seizure** and **confiscation** vary from one jurisdiction to another. For the purposes of general guidance, the following descriptions of these terms are provided:

**Freezing:** In the context of this Recommendation, a competent government or judicial authority must be able to freeze, to block or to restrain specific funds or assets and thus prevent them from being moved or disposed of. The assets/funds remain the property of the original owner and may continue to be administered by the financial institution or other management arrangement designated by the owner.

**Seizure:** As with freezing, competent government or judicial authorities must be able to take action or to issue an order that allows them to take control of specified funds or assets. The assets/funds remain the property of the original owner, although the competent authority will often take over possession, administration, or management of the assets/funds.

**Confiscation (or forfeiture):** Confiscation or forfeiture takes place when competent government or judicial authorities order that the ownership of specified funds or assets be transferred to the State. In this case, the original owner loses all rights to the property. Confiscation or forfeiture orders are usually linked to a
criminal conviction and a court decision whereby the property is determined to have been derived from or intended for use in a violation of the law.

With regard to freezing in the context of SR III, the terms *terrorists, those who finance terrorism* and *terrorist organisations* refer to individuals and entities identified pursuant to S/RES/1267 (1999) and S/RES/1390 (2002), as well as to any other individuals and entities designated as such by individual national governments.
Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.
Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory 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 a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and that are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing, should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

**Interpretative Note to Recommendation 23**

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and nonbanks in particular) from an FATF point of view. Hence, where shareholder suitability (or “fit and proper”) tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.
Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist financing measures. At a minimum:
   • casinos should be licensed;
   • competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;
   • competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organization, provided that such an organization can ensure that its members comply with their obligations to combat money laundering and terrorist financing.
Countries should take measures to prevent the unlawful use of legal persons by money launderers. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities. In particular, countries that have legal persons that are able to issue bearer shares should take appropriate measures to ensure that they are not misused for money laundering and be able to demonstrate the adequacy of those measures. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.
Appendix M: FATF Recommendation 34

Countries should take measures to prevent the unlawful use of legal arrangements by money launderers. In particular, countries should ensure that there is adequate, accurate and timely information on express trusts, including information on the settler, trustee and beneficiaries, that can be obtained or accessed in a timely fashion by competent authorities. Countries could consider measures to facilitate access to beneficial ownership and control information to financial institutions undertaking the requirements set out in Recommendation 5.
Appendix N: FATF Recommendation 31

Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place that enable them to co-operate, and where appropriate co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.
Appendix O:
FATF Recommendation 36

Countries should rapidly, constructively and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions and related proceedings. In particular, countries should:

- not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance;
- ensure that they have clear and efficient processes for the execution of mutual legal assistance requests;
- not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters; and
- not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.
Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied, regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.
Appendix Q: FATF Special Recommendation V

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

Guidance Notes by the FATF (Excerpt)

**SR V: INTERNATIONAL CO-OPERATION**

This Recommendation contains five elements:

- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions through **mutual legal assistance mechanisms**;
- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions by means **other than through mutual legal assistance mechanisms**;
- Jurisdictions should have specific measures to permit the denial of “safe haven” to individuals involved in terrorist financing;
- Jurisdictions should have procedures that permit the extradition of individuals involved in terrorist financing; and
- Jurisdictions should have provisions or procedures to ensure that “claims of political motivation are not recognised as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing.”

To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made for some questions in the SAQTF between international co-operation through **mutual legal assistance** mechanisms on the one hand and information exchange through means **other than through mutual legal assistance**.
For the purposes of SR V, the term *mutual legal assistance* means the power to provide a full range of both non-coercive legal assistance, including the taking of evidence, the production of documents for investigation or as evidence, the search and seizure of documents or things relevant to criminal proceedings or to a criminal investigation, and the ability to enforce a foreign restraint, seizure, forfeiture or confiscation order in a criminal matter. In this instance, mutual legal assistance would also include information exchange through rogatory commissions (that is, from the judicial authorities in one jurisdiction to those in another).

Exchange of information by means *other than through mutual legal assistance* includes any arrangement other than those described in the preceding paragraph. Under this category should be included exchanges that take place between FIUs or other agencies that communicate bilaterally on the basis of memoranda of understanding (MOUs), exchanges of letters, and so on.

With regard to the last three elements of SR V, these concepts should be understood as referred to in the relevant UN documents. These are S/RES/1373 (2001), paragraph 2c (for denial of safe haven); the UN Convention, Article 11 (for extradition); and the UN Convention, Article 14 (for rejection of claims of political motivation as related to extradition). The text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism.asp; the text of S/RES/1373 (2001) may be accessed at http://www.un.org/documents/scres.htm.

The term *civil enforcement* as used in SR V is intended to refer only to the type of investigations, inquiries or procedures conducted by regulatory or administrative authorities that have been empowered in certain jurisdictions to carry out such activities in relation to terrorist financing. *Civil enforcement* is not meant to include civil procedures and related actions as understood in civil law jurisdictions.
Appendix R: FATF Recommendation 38

There should be authority to take expeditious action in response to requests by foreign countries to identify, freeze, seize and confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value. There should also be arrangements for co-ordinating seizure and confiscation proceedings, which may include the sharing of confiscated assets.

Interpretative Note to Recommendation 38

Countries should consider:

a) Establishing an asset forfeiture fund in its respective country into which all or a portion of confiscated property will be deposited for law enforcement, health, education, or other appropriate purposes.

b) Taking such measures as may be necessary to enable it to share among or between other countries confiscated property, in particular, when confiscation is directly or indirectly a result of coordinated law enforcement actions.
Countries should recognize money laundering as an extraditable offence. Each country should either extradite its own nationals, or where a country does not do so solely on the grounds of nationality, that country should, at the request of the country seeking extradition, submit the case without undue delay to its competent authorities for the purpose of prosecution of the offences set forth in the request. Those authorities should make their decision and conduct their proceedings in the same manner as in the case of any other offence of a serious nature under the domestic law of that country. The countries concerned should cooperate with each other, in particular on procedural and evidentiary aspects, to ensure the efficiency of such prosecutions.

Subject to their legal frameworks, countries may consider simplifying extradition by allowing direct transmission of extradition requests between appropriate ministries, extraditing persons based only on warrants of arrests or judgments, and/or introducing a simplified extradition of consenting persons who waive formal extradition proceedings.
Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.
b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide cooperation.
c) Competent authorities should be able to conduct inquiries and where possible, investigations, on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

**Interpretative Note to Recommendation 40**

1) For the purposes of this Recommendation:
   - “Counterparts” refers to authorities that exercise similar responsibilities and functions.
   - “Competent authority” refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.
2) Depending upon the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3) The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4) FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions to obtain relevant information.
Module 2 Answers

Answer 1
True

Answer 2
True

Answer 3
True

Answer 4
True

Answer 5
False

Answer 6
True. The Vienna Convention contains the basic definition of money laundering, even though it does not use the term.

Answer 7
True, at least technically. The purpose of the convention is to combat more than drug trafficking. The Palermo Convention contains a broad range of provisions to fight all organized crime, including drug trafficking. It also criminalizes money laundering.

Answer 8
True. UN Security Council Resolutions do not require ratification and implementation by the UN member country to have the force of law within that country.

Answer 9
False. UN Security Council Resolution 1267 deals with freezing of assets of terrorists.

Answer 10
True. These conventions define three categories. The first two are mandatory; the third depends on a country’s legal system.

1. Conversion or transfer of property, 2. Concealment or disguise of property, 3. Acquisition, possession, or use of property.
Answer 11
False. Money laundering should be criminalized on the basis of the Vienna and Palermo Conventions, which provide specific definitions for the crime of money laundering.

Answer 12
True. The crime of money laundering depends on the existence of criminal proceeds to conceal, disguise, and so forth. Conviction for the predicate offense should not be required for conviction for money laundering.

Answer 13
True. The FATF provides great discretion in the designation of predicate offenses for money laundering.

Answer 14
False. The use of a specific name or category is not required, provided that the nature of the crime is covered somewhere as part of another predicate offense.

Answer 15
False. The location of the predicate offense should not affect the likelihood of conviction for money laundering. The question is usually whether the underlying crime is a crime in the country where the money laundering occurs. It may need to be a crime in both countries.

Answer 16
False. The Vienna Convention contains only provisions to combat drug trafficking and associated money laundering.

Answer 17
False. UN Conventions need to be ratified and implemented in a country before having the force of law there.

Answer 18
False. Money laundering is separate from the underlying crime; often, a person is convicted of money laundering without being convicted of, or even being connected to, the underlying crime.
Money laundering and the financing of terrorism are global problems that not only threaten a country's security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The *Combating Money Laundering and the Financing of Terrorism* training program was developed by the World Bank's Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

**Module 1:** Effects on Economic Development and International Standards
**Module 2:** Legal Requirements to Meet International Standards
**Module 3a:** Regulatory and Institutional Requirements for AML/CFT
**Module 3b:** Compliance Requirements for Financial Institutions
**Module 4:** Building an Effective Financial Intelligence Unit
**Module 5:** Domestic (Inter-Agency) and International Cooperation
**Module 6:** Combating the Financing of Terrorism
**Module 7:** Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti–Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Regulatory and Institutional Requirements for AML/CFT

Workbook

THE WORLD BANK
Regulatory and Institutional Requirements for AML/CFT

Workbook

THE WORLD BANK
Washington, D.C.
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit
Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation
Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism
Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing
Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments
The initial work for this training program was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 3a was further written and developed by Manuel Vasquez, International Monetary Fund. The draft was reviewed by John McDowell, the World Bank and Thomas Grahn, Financial Supervisory Authority of Sweden. Pedagogical guidance was provided by Sheila Jagannathan, and peer review was conducted by Emiko Todoroki, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Cedric Mousset, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations” (2003) and “Special Recommendations on Terrorist Financing” (2005); and Paul Allan Schott, Reference Guide to Anti–Money Laundering and Combating the Financing of Terrorism, Second Edition, the World Bank, 2004.

Capacity Enhancement Program on Anti–Money Laundering and Combating the Financing of Terrorism
Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Regulatory and Institutional Requirements for AML/CFT

Module 3a introduces the regulatory and institutional requirements for anti-money laundering and combating the financing of terrorism (AML/CFT). While the module primarily focuses on financial institutions, it also tries to address relevant requirements of designated non-financial businesses and professions (DNFBPs). The module addresses the following issues:

1. **Responsibility for effective supervision** 3

2. **Institutions subject to AML/CFT compliance** 8
   2.1 What types of institutions? 8
   2.2 Should other businesses or professions be covered by AML/CFT requirements? 10

3. **The principal regulatory and institutional requirements** 11
   3.1 Impediments and gateways for disclosure of information 13
   3.2 Customer identification and due diligence 15
   3.3 Record-keeping requirements 24
   3.4 Monitoring and reporting suspicious transactions 27
   3.5 Risk-based approach 29
   3.6 Suspicious transaction reporting (STR) 30
   3.7 Cash transaction reports (CTRs) 35

4. **Internal audit and compliance programs** 36
   4.1 The role of the board/senior management 36
   4.2 What should the board/senior management do? 37
   4.3 Appointment of AML/CFT compliance officer/money laundering reporting officer 37
   4.4 Ongoing employee training program 38
   4.5 Compliance and internal audit to test the system 39

5. **Professional associations: what are their roles?** 40
   5.1 Providing training 40
   5.2 Develop cooperation and understanding 40
6. Enforcement of AML/CFT requirements

This module mainly, though not exclusively, discusses the following Financial Action Task Force (FATF) Recommendations:

- AML/CFT institutional measures by financial institutions, and non-financial businesses and professions (DNFBPs) to prevent money laundering and terrorist financing, including suspicious transaction/activity reporting: Recommendations 4–25
- Necessary institutional and follow-up measures for combating money laundering and terrorist financing: Recommendations 28 and 29
- Reporting suspicious transactions related to terrorism: Special Recommendation IV

At the end of Module 3a, you should be able to

- explain the powers and responsibilities the supervisory authorities should have to supervise effectively financial and non-financial institutions, and what types of supervisory arrangements exist;
- identify financial institutions, non-financial institutions, and professionals that should be subject to AML/CFT laws and regulations;
- describe the necessary systems and controls that allow financial institutions to comply with AML/CFT laws, regulations, and guidelines; and
- explain what should be reported to the FIU and the financial supervisory authorities.
Responsibility for effective supervision

How much do you know?

**QUESTION 1.** Choose the correct word to complete the sentence:

The FATF Recommendations are the ________________ standards that the countries should adopt.

a) Minimum  b) Maximum

**QUESTION 2.** What types of institutions are subject to AML/CFT compliance?

a) Financial institutions
b) Designated non-financial businesses and professions (DNFBPs)
c) Both

**QUESTION 3.** The FATF Recommendations do not allow any discretion to the countries in terms of selection of their financial institutions for AML/CFT compliance.

a) True  b) False

**QUESTION 4.** The FATF has recommended the same level of due diligence for all customers.

a) True  b) False

**QUESTION 5.** Suspicious transaction/activity reports (STRs/SARs) should be filed by all institutions and persons covered by the local AML/CFT law.

a) True  b) False

Who determines the agencies responsible for supervision?

The laws and regulations of each country determine the competent authority, or authorities, responsible for the supervision of financial institutions’ compliance with AML/CFT requirements. In some cases, this responsibility is shared between the financial sector supervisory agencies and other authorities, such as
Module 3a

the country’s financial intelligence unit (FIU), particularly in nonprudentially regulated sectors like DNFBPs. Irrespective of the agencies involved, supervisory authorities should have adequate powers and resources, including, where appropriate, the authority to conduct inspections and impose and enforce sanctions for noncompliance with the applicable AML/CFT requirements.

How many agencies are required?
In light of the widening scope of financial institutions and other non-financial businesses and professions now subject to AML/CFT requirements, more than one body is usually needed to supervise AML/CFT compliance. However, each country’s degree of economic sophistication determines the structure and organization of the AML/CFT supervisory regime. Where multiple organizations are involved, close coordination and collaboration are mandatory.

How should such supervision begin?
Supervision of financial institutions for compliance with the AML/CFT sector should start at the licensing or authorization to engage in business stage for financial institutions. Authorization to conduct financial and other relevant businesses should be provided after stringent due diligence that determines that the owners and controllers of financial institutions are “fit and proper” persons. A review of the integrity of existing financial institutions should also be conducted to determine if the organization is fit and proper to continue to engage in business. This will hinder criminal ownership or control of financial institutions and ensure that honest and competent persons hold these sensitive positions. Ongoing, risk-focused supervision (detailed in FATF Recommendations 23 and 24) of AML/CFT risk management systems should follow periodically to make certain that internal policies, controls, and procedures are adequate. Such policies and controls should apply on a consolidated basis in cases of financial/business groups, including cross-border operations. For a discussion of these issues, please refer to the Consolidated KYC Risk Management, issued by the Basel Committee on Banking Supervision (October 2004).

What are the powers and resources that the financial supervisory authorities should have?
- Legal authority to license and supervise financial institutions on an ongoing basis
- Ability to conduct AML/CFT supervision that is risk focused
- Not to be restricted by secrecy laws from access to information under the control of supervised institutions
- Authority to cooperate and share information with competent domestic and international authorities
- Adequate staff and budget to conduct periodic inspections of financial institutions
- Authority to enforce effective, proportionate, and dissuasive sanctions against financial institutions
- Protection against legal and administrative liability when discharging their functions in good faith
- Proper training for staff on supervisory skills

The above list is not exhaustive and will vary according to the legal framework and institutional capacity of each country. Below are examples of authorities with AML/CFT supervisory responsibility in the financial sector in some countries.

FATF Recommendation 23 requires that financial institutions be subject to adequate regulation and supervision. In this regard, Recommendation 29 states that supervisors are required to have adequate powers to conduct inspections and request information. In addition, Recommendation 25 suggests that the competent authorities provide guidelines and feedback to financial institutions and DNFBPs. For more information on FATF Recommendation 23, see Appendix B. For more information on FATF Recommendation 29, see Appendix C. For more information on FATF Recommendation 25, see Appendix D.

In addition to the FATF Forty Recommendations, the International Organization of Securities Commissions (IOSCO) and the International Association of
Insurance Supervisors (IAIS) have also issued various standards, guidelines, and/or papers relating to AML/CFT. In all of these standards and papers, supervisors are required to play a key role in safeguarding against criminal abuse of the financial sector. These standards complement the FATF Recommendations and, in the case of IAIS Core Principle 28, make specific reference to compliance with the FATF Recommendations.

**International standard setters**

**Banking Sector: Basel Committee on Banking Supervision (Basel Committee)—Core Principles for Effective Banking Supervision**

Core principle (CP) No. 18 (one of 25 core principles for effective banking supervision issued by the Basel Committee) specifically deals with AML controls in the banking sector and the role of regulators. The Basel Committee has issued guidelines for banks and their supervisors on AML and customer due diligence (CDD) processes. It also has issued a detailed paper on CDD for use in screening existing and prospective banking clients. Both documents have influenced in some respects the development of the preventive measures contained in the revised FATF Recommendations.

According to the Basel Committee, national supervisors should play a key role in promoting sound ethical banking practices that prevent money laundering. In particular, they should ensure that banks have adequate policies, controls, and procedures in such areas as customer acceptance, customer identification, record keeping, ongoing monitoring of customer transactions (particularly for high-risk accounts), and risk management. For further information on the Basel Committee with respect to AML/CFT, please refer to:

- Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (December 1988)
- Core Principles for Effective Banking Supervision (September 1997)
- Core Principles Methodology (October 1999)
- CDD for Banks (October 2001)

**Securities Sector: International Organization of Securities Commissions (IOSCO)—Objectives and Principles for Securities Regulation**

According to the IOSCO, securities regulators should consider the sufficiency of domestic legislation to address the risks of money laundering. Regulators should also require that market intermediaries have in place policies and procedures designed to minimize the risk of the use of an intermediary’s business as a vehicle for money laundering. For more information, please refer to:

- A Resolution on Money Laundering (October 1992)
- Initiatives by BCBS, IAIS, and IOSCO to combat money laundering and the financing of terrorism (June 2003)
- Principles on Client Identification and Beneficial Ownership for the Securities Industry (May 2004)

**Insurance Sector: International Association of Insurance Supervisors (IAIS)—Insurance Supervisory Principles**

IAIS seeks to establish international standards on insurance supervision and conducts training seminars for insurance supervisors from emerging markets. It also seeks to coordinate its efforts with other global financial regulators, particularly those from the banking and securities industries. IAIS encourages members to comply with its insurance supervisory principles and has developed a self-assessment program for members. Insurance CP 28 on AML/CFT states that “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).”
Knowledge check

QUESTION 6. Briefly describe what supervisors need at their disposal to carry out effective supervision of financial institutions for AML/CFT. Provide your answer in the space below.

Supervision of DNFBPs

Supervision of DNFBPs on AML/CFT is a new requirement under the revised 40 Recommendations issued by the FATF in 2003. Thus, many countries including FATF members have been figuring out the best way to supervise and monitor DNFBPs. Casinos (including Internet casinos) are subject to a comprehensive regulatory and supervisory regime concerning AML/CFT requirements, similar to that for financial institutions. For example, casinos should be licensed, supervised, and monitored by a designated competent authority that should have enforcement powers. On the other hand, other DNFBPs should be subject to effective systems for monitoring and ensuring compliance with AML/CFT requirements and this could be performed on a risk-sensitive basis. Monitoring and supervision of other DNFBPs could be undertaken either by a designated competent authority or self-regulatory organization.
2.1 What types of institutions?

The categories of financial institutions, businesses, and professions covered under national AML/CFT regimes vary from country to country. There is broad coverage in some countries, but in others the coverage may be limited. For instance, in countries where only limited financial activities are being undertaken in securities markets, regulators may decide, based on risk measurement, how much AML/CFT compliance should be required of securities brokers and dealers to be in line with the FATF Recommendations. Since the revised FATF Recommendations were adopted in 2003, the definition of “financial institution” and, thereby, the institutions covered by FATF requirements, has been broadened. In addition, DNFBPs are now subject to specific FATF Recommendations. The FATF Recommendations allow countries to consider the degree of risk of money laundering and terrorist financing in deciding to what extent the FATF Recommendations should be applied for particular types of financial institutions or for particular types of customers, products, and transactions. Such determinations, however, require the national authorities to have an adequate mechanism by which to assess those risks.

Lists of the types of financial institutions and other businesses and persons required to comply with AML/CFT measures appear below; please refer to the following:

**Financial institutions**

“Financial institutions” means any person or entity that conducts as a business one or more of the following activities or operations for or on behalf of a customer:

- Acceptance of deposits and other repayable funds from the public
- Lending
- Financial leasing
- The transfer of money or value
- Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller’s cheques, money orders and bankers’ drafts, electronic money)
- Financial guarantees and commitments
• Trading in
  • money market instruments (cheques, bills, CDs, derivatives, etc.);
  • foreign exchange;
  • exchange, interest rate, and index instruments;
  • transferable securities; or
  • commodity futures trading.

• Participation in securities issues and the provision of financial services related to such issues
• Individual and collective portfolio management
• Safekeeping and administration of cash or liquid securities on behalf of other persons
• Otherwise investing, administering or managing funds or money on behalf of other persons
• Underwriting and placement of life insurance and other investment-related insurance
• Money and currency changing

**Designated non-financial businesses and professions**

“Designated non-financial businesses and professions” means:

• Casinos (and internet casinos).
• Real estate agents.
• Dealers in precious metals.
• Dealers in precious stones.
• Lawyers, notaries, other independent legal professionals and accountants. This refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to “internal” professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
• Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:
  • acting as a formation agent of legal persons;
  • acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
  • providing a registered office, business address, or accommodation; correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
  • acting as (or arranging for another person to act as) a trustee of an express trust; or
  • acting as (or arranging for another person to act as) a nominee shareholder for another person.
2.2 Should other businesses or professions be covered by AML/CFT requirements?

FATF Recommendation 24 stresses that DNFBPs should be subject to certain FATF regulatory measures. That recommendation also specifies that there should be appropriate supervision for all DNFBPs.

FATF Recommendation 20 encourages countries to consider other businesses and professions, in addition to DNFBPs listed above, that should be subject to the FATF Recommendations when they pose a money laundering or terrorist financing risk.

It will be a tremendous challenge for the authorities to identify areas and sectors that pose critical risks and should be, therefore, subject to AML/CFT requirements and supervision. Unfortunately, not all countries have systems in place to allow for this kind of risk identification. And even where the AML/CFT requirements cover sectors outside the traditional financial and DNFBP sectors, there will be questions as to what agency is responsible for compliance supervision. For more information on FATF Recommendation 24, see Appendix E. For more information on FATF Recommendation 20, see Appendix F.

Knowledge check

QUESTION 7. Where applicable, identify the three principal sectors covered by the FATF Recommendations and your country’s AML/CFT laws. Provide your answers in the space below.

________________________________________
________________________________________
________________________________________

QUESTION 8. For those sectors that are covered by the AML/CFT laws in your country, describe briefly the agency responsible for supervision of compliance with AML/CFT requirements. In your opinion are supervision and compliance successful?

________________________________________
________________________________________
________________________________________
The revised FATF 40 Recommendations (June 2003) specify the measures that financial institutions and DNFBPs are required to take to prevent, detect, and report money laundering and terrorist financing. These measures require, in certain cases, that supervisory authorities take a compliance monitoring and enforcement role with respect to the persons and institutions they supervise for AML/CFT. The following table outlines the key areas covered by the FATF Recommendations.

### Summary of regulatory and institutional requirements

<table>
<thead>
<tr>
<th>Module reference</th>
<th>Required measures</th>
<th>FATF &amp; other references</th>
</tr>
</thead>
</table>
| 3.1 Impediments and gateways for disclosure of information | Countries' financial secrecy laws should not inhibit the implementation of the FATF Recommendations. This means, *inter alia*, that where legitimate privacy laws exist restricting access to or disclosure of information, appropriate gateways should be in place to facilitate investigations and prosecution of money laundering/financing terrorism offenses. There should be a legal base that allows unfettered access to information by financial supervisors, FIUs, and other competent authorities. | FATF Recommendation: 4  
IAIS ICP: 1, 2, 3, 4, 5, 10, 16, 28  
IOSCO CP: 8.2, 8.3, 8.4, 9.3, 9.4, 11                                                                 |
| 3.2 Customer identification and due diligence | Financial institutions should obtain and verify the identity of clients including, where necessary, information on their business, profession, and source of funds and wealth. For higher-risk clients, financial institutions should apply enhanced due diligence, for example, for politically exposed persons (PEPs). CDD should extend to those persons acting on behalf of customers or otherwise intermediary clients. | FATF Recommendation: 5, 6, 7, 8, 9, 12, 18, 21, 22  
Basel Committee CDD paper and CP Methodology: 18.4; 18.5  
IAIS ICP: 10, 28  
IOSCO CP: 12.5                                                                 |
| 3.3 Record-keeping requirements | Maintaining records of customer identity and transactions for a minimum of five years is an important requirement for the prevention and detection of money laundering and terrorist financing. Such records should be sufficient to provide supervisors, FIUs, investigators, and/or prosecutors with a financial trail to investigate and prosecute financial crime, and to facilitate the seizure and confiscation of illicit property. The commencement of the retention period should be clearly defined, which could be the date when an account is closed, the date of the last transaction, or the date a relationship was terminated. There may be situations where records should be kept for longer periods, such as when the competent authorities so request to facilitate an investigation or prosecution. In addition, contractual obligations, for example, for life insurance policies, may already require longer retention periods. | FATF Recommendation: 10, 12  
Basel Committee CDD paper and CP Methodology: 18.4  
IAIS ICP: 10, 28  
IOSCO CP: 12.5                                                                 |
### Summary of regulatory and institutional requirements—continued

<table>
<thead>
<tr>
<th>Module reference</th>
<th>Required measures</th>
<th>FATF &amp; other references</th>
</tr>
</thead>
</table>
| 3.4 Monitoring and reporting of suspicious transactions | Financial institutions have an obligation to report suspicious activities where there are reasonable grounds to believe that funds are the proceeds of crime or may be linked to terrorist activity. Reporting of suspicious activity is made to the FIU. There could also be instances where the supervisor of the reporting institution may also be informed of cases that are material to the safety and soundness of the institution. It is important that the laws, regulations, and guidelines provide clear directions on the obligations to report suspicious activities to differentiate between unusual and suspicious activities, and reporting of large cash transactions (so-called “benchmark reporting”). Guidance on avoidance of tipping off subjects of reports should also be provided. | FATF Recommendation: 8, 11, 13, 14, 16, 19, and Special Recommendation IV  
Basel Committee CDD paper and CP Methodology: 18.3, 18.4, 18.10 |
| 4. Internal audit and compliance programs | Institutions covered by AML/CFT laws should establish and maintain internal policies, procedures, and controls to prevent themselves from being used for purposes of money laundering and terrorist financing. This should include an appropriate compliance function and an audit function, including the appointment of an AML/CFT compliance officer. It is the responsibility of the designated supervisors to monitor compliance with AML/CFT laws, policies, and controls in the applicable institutions, businesses, and professions and to take appropriate enforcement action for noncompliance. | FATF Recommendation: 15, 16  
Basel Committee CDD paper and CP Methodology: 18.8 |
3.1 Impediments and gateways for disclosure of information

**Impediments**

Although most financial laws contain provisions protecting the confidentiality of information held by financial institutions, they should not act as an impediment to access and disclosure by supervisors, FIUs, law enforcement, and other competent authorities. Supervisors and other competent authorities should have sufficient and, in the case of financial sector supervisors, unfettered access to customer information and all other relevant information required for the proper discharge of their functions. Such information should be handled with utmost care by the recipients to preserve confidentiality and should be safeguarded against unauthorized use.

Efficient gateways should exist in law, or through other mechanisms, to allow for cooperation and information sharing among competent authorities domestically and internationally, including supervisory agencies. In some countries, information sharing among financial institutions may also be allowed or required. Financial institutions and staff that provide information to the authorities and file suspicious activity reports to the FIUs should be provided legal protection against criminal, civil, and administrative liability when they act in accordance with the law and in good faith. Similar protections should be extended for supervisory agencies and their staff when they share information.

FATF Recommendation 4 requires that financial institution secrecy laws should not inhibit implementation of the FATF Recommendations. Recommendation 28 also requires that countries should have powers to be able to compel the production of transaction records; identification data obtained through the CDD process; account files and business correspondence; and other records, documents, or information held or maintained by financial institutions and other businesses or persons when conducting investigations of money laundering, financing of terrorism, and other underlying predicate offenses. For more information on FATF Recommendation 4, see Appendix G. For more information on FATF Recommendation 28, see Appendix H.
Country X is fast becoming a major tourist destination, particularly for world-class divers who explore its vast coral reefs and offshore islands. The authorities are concerned that the expansion in tourism could also attract criminals and money launderers; investments in the booming hotel and casino industry will be attractive to these criminals. General elections are planned to take place within the next three months and the minister of finance, under whose portfolio the Central Bank and the FIU fall, would like to make crime fighting a main issue in his political campaign. The minister is particularly concerned that some political opponents may be associated with certain criminal groups and is determined to prevent drug traffickers and money launderers from taking control of the country’s government. The minister has therefore called on the governor of the Central Bank and the head of the FIU for any information they may have on two political opponents and their business associates, whom it is believed may have criminal connections. The minister of finance also wants these institutions to request and provide bank account information on these individuals.
Knowledge check

Based on the preceding case study, please provide appropriate responses to the following questions using the space provided:

QUESTION 9. Should the governor of the Central Bank or the head of the FIU, or neither, provide the desired information about the two individuals to the minister of finance?

QUESTION 10. If neither the Central Bank nor the FIU has the requested information, should they obtain it from the banks? If not, why?

QUESTION 11. What are the possible consequences of providing the information to the minister? What if the information is not provided?

3.2 Customer identification and due diligence

Customer identification and due diligence are perhaps the most important controls in preventing criminals from entering the legitimate economy and financial system. The creativity and increasing sophistication of money launderers and the financiers of terrorism require financial institutions and DNFBPs to constantly review and upgrade their preventive systems; this generally starts with effective CDD policies and controls. Evolving international best practices require that CDD controls be risk-based, with higher-risk customers and services screened rigorously before they are accepted as customers. FATF Recommendation 5 deals with CDD. For more information on FATF Recommendation 5, see Appendix I.
3.2.1 How to determine the required level of due diligence

Some customers, such as those requiring one-off transactions, may necessitate less diligence, unless the amount of the transactions is large or there is reasonable basis for suspicion. Businesses that establish long-term business relationships may need more stringent CDD procedures and information requirements and should be monitored during the course of the relationship. Depending on the customer’s category and risk profile, complete and up-to-date information, such as address, background, profession, and sources of funds and wealth, plays a vital role in preventing and detecting money laundering and terrorist financing. The purpose and projected use of financial services and accounts should also be documented. All this information prepares a predictable background for comparison with inconsistent or unusual customer activity. This, in turn, allows the reporting institution to identify suspicious behavior for the FIU.

“Know Your Customer (KYC)” principles

The basic KYC principles are well established in the relevant international standards and papers, such as those issued by the FATF, the Basel Committee, IOSCO, and IAIS. Depending on the nature of their activities, reporting institutions are required to obtain and record appropriate and verifiable information about their customers' identity, as well as on their business and financial activities. An institution’s KYC policy should be part of an integrated AML/CFT control policy that is focused on the principal ML/FT risks facing that institution. Therefore, it should take into account not only the individual clients’ risk profile, but other risk factors, such as the business sector, geographic region, and jurisdiction where clients live or conduct business. The policy should also consider special types of clients, such as intermediaries, introducers, and other regulated entities. The new international standards now also require enhanced due diligence for PEPs and in relation to cross-border correspondent banking and other similar relationships. Similar processes should also be applied to high-risk products and services, especially where there is no face-to-face contact with the clients. Clients who are involved in complex transactions that are not transparent (as to the underlying promoters or beneficiaries, for example) could also present higher money laundering/terrorist financing risks and form part of a risk-based policy.

Additional information on KYC can be found at:

- Basel Committee on Banking Supervision, “Customer Due Diligence for Banks,” October 2001
- IAIS, Insurance Core Principles 28 on AML/CFT

Knowledge check

QUESTION 12. Who are we referring to when we talk about a “customer”?
**QUESTION 13.** A lawyer wants to open a deposit account at a bank in the name of company XYZ Ltd. What questions should the bank ask to determine the type of customer identification and due diligence procedures to apply?

**QUESTION 14.** Assume the lawyer mentioned above is acting in the capacity of trustee: what questions can be asked and what due diligence procedures should apply?

### 3.2.2 CUSTOMER ACCEPTANCE AND IDENTIFICATION PROCEDURES

The thoroughness of customer identification and due diligence should depend on the risks involved. The regulatory regimes of a country may allow its financial institutions to apply reduced or simplified measures of CDD for customers who fall in low-risk categories. However, when an institution is allowed to apply reduced or simplified due diligence procedures, it must be able to justify to the regulators and/or other competent authorities that there are adequate mechanisms in place to identify, measure the level of, and manage such risk. Absence of such risk evaluation mechanisms may expose institutions to undue ML/FT risk, and subject it to regulatory or legal action by the authorities.

A basic customer acceptance and identification policy should provide the following at a minimum:

- Procedures for acceptance and approval of new customers
- Identification and verification of identity for new and, when necessary, existing customers
- Identification and verification of any beneficial owner, including reasonable measures to understand the ownership and control structure of legal persons and arrangements
- Enhanced due diligence for higher-risk customers, sectors, products, and services

Read the following sections for further discussion of the above.
Procedures for acceptance and approval of new customers

Clear procedures should be in place for new client acceptance. Those procedures should include approval by senior officers for higher-risk client relationships and transactions. Enhanced due diligence is also required for such clients.

Identification and verification of identity for new and, when necessary, existing customers

Financial institutions should verify a new customer’s identity by requesting official documents issued by appropriate authorities (passport, driver’s license, personal identification, or tax identification document). Accounts in anonymous or fictitious names must not be allowed.

Identification and verification of any beneficial owner, including reasonable measures to understand the ownership and control structure of legal persons and arrangements

Where a customer is representing a third party or beneficiary (as with trusts, nominees, fiduciary accounts, corporations, and other intermediaries), financial institutions need to take reasonable measures to verify the identity and nature of the persons or organizations on whose behalf an account is being opened or for whom a transaction is being completed. Financial institutions can verify the identities of such entities by collecting the following information:

- Name and legal form of customer’s organization
- Address
- Names of directors
- Principal owners or beneficiaries
- Provisions regulating the power to bind the organization
- Persons having the power to bind or to act on behalf of the client
- Information of the purpose and intended nature of the business relationship

Enhanced due diligence for higher-risk customers, sectors, products, and services

To identify high-risk customers, use standard risk indicators, such as

- Industry sector of business activity
- Complexity of proposed business/account activity
- Political position or affiliation and high net worth
- Country of origin or business location
- Complex structures and multiple account relationships
National supervisors are strongly encouraged to issue industry guidelines to assist institutions in developing customer acceptance and identification procedures. However, basic identification and verification may include:

For individuals:

- Identification documentation: official documentation, which is generally more difficult to falsify or reproduce (e.g., passports, driver’s licenses, national identity cards, etc.)
- Evidence of address—utility and telephone bill payment records, rental payment records, property tax documents, trade licenses, etc.
- Bank and professional references (these should be originals, and where necessary, sent directly to the institutions and verified by calling the referring institution or person)
- Copies of salary or wage checks and receipts including, where necessary, employment contracts
- Tax returns
- Other information based upon national custom or practice

For private companies:

- Copies of incorporation certificates and other relevant information, registered office, etc.
- Names of directors, principal shareholders, officers, and anyone authorized to act on behalf of or to bind the company
- Identity of the beneficial owners
- Business purpose
- Where appropriate, copies of current financial accounts (audited if available), tax returns, etc.
- Other information based upon national custom or practice

Please note that it may be necessary for the financial institution, in the case of a company or legal person or entity, to conduct individual CDD on some or all of the directors, principal shareholders, beneficial owners, officers, and anyone authorized to act on its behalf. For publicly traded companies, there should be sufficient public information available to KYC; less-stringent identification and due diligence procedures would be needed compared with unlisted private companies.

There may also be situations where local legislation or regulations allow for a financial institution to rely on the CDD of others, such as a prospective client who is a client of, or is introduced by, an affiliate of the financial institution. The national authorities should describe circumstances under which such reliance would be acceptable and provide clear guidelines for these purposes. In addition, national regulations or guidelines may require the financial institution to obtain the CDD information promptly from the service provider for AML/CFT supervision or to support ML/FT investigations and prosecutions.
However, it is important to note that ultimate responsibility for CDD rests with the financial institution holding the customer account and not with the third party or intermediary. Such legal responsibility may not be delegated. In addition, the service provider needs to be in a position to provide such information and evidence of identity to the competent national authorities and needs to be able to so promptly on request.

FATF Recommendation 9 discusses reliance on intermediaries and other third parties for certain elements of the CDD process. For more information on FATF Recommendation 9, please see Appendix J.

Knowledge check

You are a bank officer. Compare and contrast the CDD procedures and information requests you would conduct on the following two prospective clients. Identify the specific types of questions and information requirements for each. Identify the different risk factors the bank should consider that should be addressed in the information requests.

**QUESTION 15.** A plumber wishes to open a checking account. The plumber is a private contractor in the residential housing market.

**QUESTION 16.** A company involved in the import and resale of electronic equipment for the domestic market and re-export, wishes to open a checking account and a letter of credit facility.

3.2.3 **Enhanced Due Diligence**

As mentioned earlier, customer identification and CDD measures depend on the risk attached to a type of customer, product, and transaction. Although countries may allow a reduced or simplified due diligence for customers with a lower-risk profile, enhanced due diligence should be applied to those clients, relationships, products, and services that carry a higher level of risk. FATF Recommendations 6, 7, and 8 identified the following areas that present a higher degree of ML/FT risk:
• Politically exposed persons, their relatives, and affiliates
• Payable-through accounts and correspondent banking, especially where respondent banks are from financial centers with weak supervision and where shell and parallel banking structures are permitted
• Products and services that permit customer or transactional anonymity and where there is no physical contact with clients

Other examples of areas that may present a higher degree of ML/FT risk vary across countries and regions and may include the following:

• Complex account, business, and relationship structures, especially where beneficial ownership and control are not transparent
• Accounts with transactions and counterparties from jurisdictions known for weak legislation and implementation of controls to combat money laundering and terrorist financing
• Customers operating in high-risk industries and businesses, such as casinos, arms and defense, precious metals and stones
• Private banking and high-net-worth customers
• Nonresident clients
• Clients associated with countries and activities that are known to be vulnerable to, or associated with, terrorism and terrorist financing activities—certain types of charities, extreme religious groups, money remitters, informal value transfer systems, etc.

The nature, quality, and quantity of client information required should generally reflect the degree of business, money laundering, and financing of terrorism risk inherent in a customer relationship. More information about a customer is not necessarily better, but it is important that the information can be verified and provides reasonable assurance that the client is the person he or she claims to be.

In developing a risk-based KYC framework, financial institutions can take a number of risk factors into account. (See section 3.2, Customer identification and due diligence.) Often these risk factors are client related and not focused on financial loss issues. These risk factors may be specific to a country, region, economic sector, client category, product, or service. Typical risk indicators may include those transactions and client relationships relating to

• ML/FT typologies, high-risk clients—high-net-worth individuals and politically exposed persons;¹
• high-risk country connections, high-risk industries and activities—arms industry, precious gems and art, casinos, shell banks², bureaux des changes/

¹ The FATF Recommendations define PEPs as those who are or have been entrusted with prominent public functions in 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; and important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those posed by PEPs themselves. The definition is not intended to cover middle-ranking or junior individuals in the foregoing categories.
² Shell banks are licensed banks that incorporated in a jurisdiction, but have no physical presence there, and no affiliation with a regulated banking or financial group. For a more complete definition, see the Basel Committee paper on shell banks: http://www.bis.org/publ/bch95.pdf.
casas de cambio, and money remitters, certain charities and foundations, and so on; and

• nontraditional and complex financial structures and business relationships, intermediary clients, etc.

A number of the FATF Recommendations contain detailed CDD requirements for high-risk customers:

• FATF Recommendation 6 (PEPs)
• FATF Recommendation 7 (correspondent banking and payable-through accounts)
• FATF Recommendation 8 (new and developing technologies, customers with no face-to-face contact)

The recommendations require institutions to apply enhanced due diligence on clients that fall under these categories of clients or services. Supervisors and regulators should likewise take a risk-based approach to checking for compliance with these recommendations.

Other issues that are important to remember include:

• FATF Recommendation 9 (introduced business)
• FATF Recommendation 11 (complex, unusually large transactions and unusual patterns of transactions)
• FATF Recommendation 18 (shell banks)
• FATF Recommendations 21 (transactions with persons from countries with weak AML/CFT regimes)

Recommendation 12 also requires that CDD and record keeping be applied to DNFBPs; however, at this time we are focusing on the core CDD elements. Record-keeping requirements are discussed below, separately, under section 3.3 Record-keeping requirements. For more information on FATF recommendations, see the following Appendices:

Recommendation 6 - Appendix K
Recommendation 7 - Appendix L
Recommendation 8 - Appendix M
Recommendation 9 - Appendix J
Recommendation 12 - Appendix N
Recommendation 18 - Appendix O
Recommendation 21 - Appendix P
Recommendation 22 - Appendix Q
Recommendation 11 - Appendix R

The salient features of CDD are:

• Financial institutions and DNFBPs should look to competent authorities of a country for overall policy and framework guidance for dealing with
ML/FT risks, including the circumstances (based on risk assessment) under which AML/CFT measures should be applied, reduced, or enhanced.

- Financial institutions are expected to identify and verify the identity of a customer.
- Financial institutions may apply reduced or simplified CDD in certain circumstances, but reduced CDD needs to be based on proven low-risk customers.
- Enhanced due diligence measures must be ensured in the circumstances mentioned in the FATF Recommendations.
- Reporting institutions ensure that all the AML/CFT policies and procedures are communicated to its staff and personnel.

Regulatory supervisors determine if financial institutions have adequate policies, practices, and procedures that are consistent with national guidelines in place for combating ML/FT risks. Supervisors also judge the robustness of the risk-assessment systems in financial institutions and determine that customers are categorized consistently based on the findings of risk assessment.

Knowledge check

**QUESTION 17.** You are a bank officer in charge of private banking for high-net-worth individuals from your country and neighboring jurisdictions. Most of your clients have long-established business relationships with your bank and include some of the most prominent business persons and politicians in the region. One of the most popular services provided by your private banking department is investment portfolio management and advice. Traditional banking services, such as deposit and credit card accounts, are also provided to these clients, but are not the main profit drivers.

A prospective client from a neighboring country, Utopia, has requested a meeting with you to discuss establishing a substantial investment account and other services. The prospective client has indicated there are others, well known to him, who are also interested in similar services. A “long-standing” customer of the bank introduced this prospective client to the bank. After a brief discussion with the prospective client, you discover he has been the minister of finance in Utopia for the past 3 years. In the past, Transparency International has rated Utopia poorly for corruption. You are interested in acquiring new business. Your bank’s financial year ends in two months and you need to book at least five more customers to receive the sizable financial bonus and “Private Banker of the Year” award that has eluded you since you joined the bank 10 years ago. You are aware of your bank’s new anti-money laundering policy, enacted six months ago by the Central Bank, requiring scrutiny for new accounts.
In preparing to meet the prospective client, please identify all possible risk factors and prepare a list of documents and information you will need from the client. Also, identify other sources of information that will help you decide whether or not to accept this new client.

### 3.3 Record-keeping requirements

Under FATF Recommendations 10 and 12, financial institutions and DNFBPs should maintain customer identity and transaction records for a **minimum of five years**, or longer if authorized by legislation, regulation, or court order. The five-year period generally commences with the completion of a transaction, the closing of an account, or the termination of a business relationship. Records should be sufficient to permit the reconstruction of individual transactions and be made available promptly on request by the competent authorities. Records provide an important audit and paper trail for regulators, the FIU, police, and prosecution authorities. Consequently, identification and transaction records should be complete and readily available to institutions, for immediate response to requests for data from the competent authorities.

#### 3.3.1 Common types of documents required

- Copies of customer identification and due diligence records, including evidence of verification
- Account files
- Transaction records
- Business correspondence
- Any other information that would be necessary to trace and identify the beneficiaries of accounts or property and that could serve as evidence for the prosecution of criminal activity
3.3.2 Information included in transaction records

- Customers’ names (including documentation related to the beneficial owner)
- Address or other identifying information
- Nature and date of the transaction
- Type and amount of currency involved
- Type of financial instrument used: checks, drafts, wire transfers, credit/debit cards, etc.
- Type and identification number of accounts involved in a transaction, and so forth

Some of the industry-specific record-keeping requirements are discussed in the following sections:

Banking sector record-keeping requirements

The following information is needed to record a customer’s transaction

- Name of the customer and/or beneficiary
- Date and nature of the transaction
- Type and amount of currency involved in the transaction
- Type and identifying number of account
- Other relevant information typically recorded by the financial institution

Insurance sector record-keeping requirements

IAIS maintains its own set of record-keeping requirements. Insurance entities must adhere to the IAIS requirements in addition to the FATF Recommendations. Information needed:

- Identity, address, and so on
- Location completed
- Client’s financial assessment
- Client’s need analysis
- Benefits description
- Copy of documentation used to verify customer’s identity
- Post-sale records associated with the contract through its maturity
- Details of maturity processing and claim settlement
- Benefits payment records and receipts
Securities sector record-keeping requirements

IOSCO has set its own set of record-keeping requirements. “Authorized securities service providers” are required to maintain appropriate records for at least five years after the business relationship has ended. The required information includes:

- Identities of clients and beneficial owners
- All necessary records on transactions, both domestic and international, sufficient to permit reconstruction of individual transactions
- Records must be sufficient to permit reconstruction of individual transactions
- CDD data on clients of trusts


FATF Recommendation 10 addresses record-keeping requirements for financial institutions, and Recommendation 12 specifies the record-keeping requirements that are applicable to DNFBPs. For more information on FATF Recommendation 10, see Appendix S. For more information on FATF Recommendation 12, see Appendix N.

Knowledge check

Distinguish between the types of records that should be maintained for the following two types of customers and transactions:

**QUESTION 18.** A bank customer with an established business relationship of five years who wishes to buy a foreign currency draft to pay for imports.

**QUESTION 19.** Two separate walk-in customers who do not have an established business relationship but wish to buy foreign currency drafts as follows:

1) US$1,000 for vacation travel
2) A series of 10 drafts of US$9,700 each
3.4 Monitoring and reporting suspicious transactions

3.4.1 Who should report?

Under FATF Recommendations 13 and 16, financial institutions and DNFBPs have an obligation to report suspicious transactions and activities to the FIUs. Often reports of suspicious transactions or activity, commonly referred to as STRs or SARs are the combined result of CDD and monitoring processes within an organization. SARs are generated whenever a financial institution knows, suspects, or has reasonable grounds to suspect that funds are the proceeds of crime or are related to terrorist financing activities. Once a suspicion is formed, STRs/SARs should be filed promptly in accordance with domestic law or regulations. Secrecy laws shall not inhibit such reports and the financial institutions and their staff shall be provided legal protection when reporting in good faith. It is also very important that processes be established and staff training provided to prevent tipping off, whether inadvertent or intentional, the subject of a STR/SAR. This is an unauthorized disclosure under FATF Recommendation 14. Tipping off is a criminal offense under a compliant legal system and may, inter alia, include punishment of fines and/or imprisonment for staff and their institutions.

3.4.2 How to improve reporting capacity

Institutions’ ability to report suspicious activity, however, will depend on the adequacy of both CDD and the mechanisms in place for monitoring account and transaction activity. Staff training for all of these issues will be immensely important, as described in the following sections. Likewise, internal guidelines duly communicated to all staff should be in place to enable employees to identify and report to the appropriate official cases of suspected ML/FT. Institutions’ failure to report could expose them to fines and sanctions by the competent authorities, including by the supervisory agencies.

3.4.3 Transaction and account monitoring

Monitoring for unusual and suspicious activity should be an ongoing function of financial institutions and other DNFBPs. They should have appropriate processes in place that allow for the identification of unusual activity and unusual patterns of activity or transactions. Because not all unusual transactions are suspicious, financial institutions and DNFBPs should have the capacity to analyze such transactions to ascertain whether they are consistent with a customer’s profile.
Unusual transactions or activity that cannot be explained on legal or commercial grounds may provide a basis for forming a suspicion and for reporting to the FIU. A reporting institution’s ability to monitor account activity would be largely contingent on the availability and adequacy of its due diligence and record-keeping processes. Weak CDD and record keeping would significantly constrain the ability to develop customer profiles and identify unusual and suspicious activity.

### 3.4.4 HOW TO DEVELOP AN EFFECTIVE MONITORING SYSTEM

The financial regulators or other authority should provide guidelines and examples of suspicious activity as an aid to financial institutions and DNFBPs. Depending on size, need, and complexity of financial institutions and DNFBPs, monitoring of suspicious transactions may be automated, manual, or both. Some financial institutions and DNFBPs use specialized software to detect suspicious transactions or activities; however, the use of such software can only complement managerial oversight and not replace the need for constant monitoring of the accounts of customers. Monitoring mechanisms should be more rigorous in high-risk areas of an institution and supported by adequate information systems to alert management and other appropriate staff (for example, the AML/CFT compliance officer) of suspicious activity. Training of staff in the identification of unusual and suspicious activity should always be an ongoing activity.

**Transaction monitoring**

- A clear policy and the procedures for monitoring and reporting suspicious activity should be communicated to all staff.
- There should be an effective management information system to alert the board, senior management, and compliance officers of significant ML/FT risk factors and cases.
- The system for monitoring transactions should provide for the aggregation of data on transactions, accounts, and clients across product lines and on a group-wide basis, including international operations.
- A monitoring system should provide for the identification of structuring/smurfing and for identifying linked transactions.
- There should be a system for identifying large (especially unusually large) transactions, including those using cash or bearer monetary instruments.
- A monitoring system should enable a review of account activity for turnover and use of unexpected financial instruments to detect unusual transactions or patterns of transactions. Special attention should be given to “pass-through” accounts, that is, those in which debits and credits to an account are roughly the same.
- Wire transfer activity should be monitored to ensure that the amounts involved are commensurate with the needs of customers, especially when they involve transactions with counterparties in high-risk jurisdictions and sectors.
- Credit and debit card operations should be monitored closely. Accounts with high credit limits and cash-secured credit cards should be subject to closer scrutiny.
- Loans and financial guarantees (such as back-to-back lending and standby letters of credit), especially transactions involving the use of entities established in offshore financial centers, should be closely monitored.
3.5 Risk-based approach

Achieving an integrated AML/CFT risk-based system depends mainly on a proper assessment of the relevant risk sectors, products, services, and clients and on the implementation of appropriate risk-focused due diligence. These, in turn, become the foundation for monitoring and compliance mechanisms that allow rigorous screening of high-risk areas and accounts. Without sufficient due diligence and risk profiling of a customer, adequate monitoring for suspicious activity would be impossible.

In June 2007, the FATF issued “Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing: High Level Principles and Procedures” to assist both authorities and the private sector to

- support the development of a common understanding of what the risk-based approach involves;
- outline the high-level principles involved in applying the risk-based approach; and
- indicate good public and private-sector practice in the design and implementation of an effective risk-based approach.

In addition, the Wolfsberg Group has issued guidelines on a risk-based monitoring system. The risk-based monitoring system for banking clients should

- compare the client’s account/transaction history to the client’s specific profile information and a relevant peer group, and/or examine the client’s account/transaction history against established money laundering criteria/scenarios to identify patterns of suspicious activity or anomalies;
- establish a process to compare customer or transaction-specific data against risk-scoring models;
- be capable of recognizing patterns and of “learning” which transactions are normal for a client, rather than designating certain transactions as unusual (for example, not all large transactions are unusual and may easily be explained);
- issue alerts if unusual transactions are identified;
- track alerts to ensure they are appropriately managed within the institution and that suspicious activity is reported to the authorities as required;
- maintain an audit trail for inspection by the institution’s audit function and by bank supervisors; and
- provide appropriate aggregated information and statistics.

FATF Recommendation 11 requires financial institutions to pay special attention to complex and unusual transactions and Recommendation 8 requires financial institutions to pay special attention to new and developing technologies for customers and to have policies and procedures in place for business relationships with no face-to-face contact. For more information on FATF Recommendation 11, see Appendix R. For more information on FATF Recommendation 8, see Appendix M. You may also refer to section 3.2.3, Enhanced due diligence, in this module.
QUESTION 20. Pick a type of financial institution (for example, bank) and identify/list at least five issues or red flags that the financial institution should pay attention to in ongoing transaction monitoring. You may consider focusing on the high-risk areas or high-risk customers of such institutions, for example, deposits for a bank, life insurance policies for an insurer, and so forth. Provide your answer in the space below.

3.6 Suspicious transaction or activity reporting (STR/SAR)

STRs or SARs should be filed by all institutions and persons covered by the local AML/CFT law. This should be a direct mandatory and enforceable obligation. This requirement should be a core element of internal policies and procedures and the substantive result of effective customer identification and due diligence processes. FATF Recommendation 13 and Special Recommendation IV are particularly relevant here, requiring suspicious transactions, including attempted transactions, to be reported promptly to the FIU. Recommendation 16 requires that STR requirements be enforced with regard to the DNFBPs. For more information on FATF Recommendation 13, see Appendix T. For more information on FATF Special Recommendation IV, see Appendix V. For more information on FATF Recommendation 16, see Appendix W.

National regulations or guidelines could provide specific direction concerning the allotted time allowed for reporting suspicious activity, but it should be reported in a reasonably short period after the suspicion is formed. Laws and guidelines usually hold that the reporting institution need not know or establish the underlying predicate crime (for example, drug trafficking, fraud, terrorism) before filing a STR/SAR. Still, every effort should be made to conduct an internal review of the basis for suspicion so that legitimate transactions, even if unusual, are not reported. This would avoid sending unnecessary reports, which could be explained on legal or commercial grounds, to the FIU and reduce the number of low-quality reports. The following approach could help institutions in deciding when STRs/SARs should be filed.
1) Get to know your customer: By applying the KYC principle, you will know each customer’s professional activity, trade, business line, or corporate purpose. Moreover, you will be able to confirm the sources of funds and expected account activity.

2) Inconsistency: This principle—inconsistency—appears in many suspicious transactions because the suspicious transaction is different from the normal, expected activities of the customer. Comparisons with peer groups can help identify inconsistencies in a customer’s financial activities.

These two principles complement each other; staff must know the customer to determine if his or her actions are inconsistent with normal business or personal activities. Unusual transactions are not necessarily suspicious; aside from suspicious amounts, in order for a transaction to be classified as suspicious, the application of fundamental principles such as KYC and inconsistency is required. Suspicions should be brought to the attention of the appropriate official within the organization for necessary review and action.

National authorities should provide reporting entities with examples of potentially suspicious transactions. Such examples will not be exhaustive and must be developed over time. Thus, employees can be educated about conditions or criteria that may make a transaction suspicious and reportable.

Some of the red flags that can enable a financial sector employee to determine suspicious activity are listed in Appendix X.

“Safe harbor” provisions for reporting

FATF Recommendation 14 states that countries should provide immunity from liability for any good faith reporting by a financial institution or officer, director, or employee of a reporting institution. Such safe harbor laws encourage reporting institutions to report all suspicious transactions by protecting reporting institutions and employees from criminal and civil liability when reporting suspicious transactions in good faith to the FIU. Legal provisions should provide reporting institutions and their employees or representatives protection against lawsuits for any alleged violation of confidentiality or secrecy laws, as long as the suspicious report was filed in good faith. For more information on FATF Recommendation 14, see Appendix U.
CASE 1

A) Placement stage:
In a recent money laundering case, an elderly couple visited several islands in the Caribbean on cruise ships. The couple carried a small suitcase filled with cash, approximately US$400,000. After several attempts, the couple succeeded in opening a deposit account in a bank in Utopia. But because the amount exceeded the limit for daily cash deposits by a single customer, a “helpful” bank employee advised them to open a safety deposit box to hold the remaining cash. The customers then instructed the employee to deposit small amounts of cash into their account from the safety deposit box each day, at or just below the bank limit. Through this simple mechanism, large amounts of cash entered the banking system. The funds were then invested, through other financial institutions, in the stock and bond markets of other countries.

QUESTION 21. In this case, who was aiding and abetting the laundering of funds? Is there anything unusual about any of the transactions?

B) Layering stage:
An apparently respectable businessman hires a U.S. attorney to represent him in the purchase of real estate in Utopia. He tells the attorney that funds will be gathered from a number of sources to make up the necessary payment for the Utopia property. Funds are transferred from a variety of sources and held in escrow by the attorney. The property is then purchased with these funds, using
the attorney’s trust account. The Utopian bank receiving the funds considers them legitimate because they seem to be coming from a reputable U.S. law firm. The purchased property can now be resold to unrelated parties and the proceeds from the sale would appear to be perfectly legitimate.

**QUESTION 22.** Why might these funds go unquestioned by the receiving bank? Can you identify any transactions that could give rise to a suspicion of illegal activity?

---

**C) Integration stage:**

A “businessperson” uses a *casa de cambio* (exchange house) in Utopia to wire funds to his brokerage account in the United States; the broker’s account is held in a U.S. bank and his name does not appear on any records. The funds are then wired to a deposit account in a Caribbean offshore bank. Simultaneously, the funds are loaned back to a trading firm controlled by the Utopian national, and there is no apparent relationship between the firm (borrower) and the individual (depositor).

**QUESTION 23.** Identify all the various financial institutions that were placed at risk. Indicate who could have detected the activity as unusual or suspicious and how it could have been done.

---

---
Case 2

ABC Video Company has been dealing with your bank for more than three years and has seen very little growth in profits. Weekly deposits range from $800 to $1,000, depending on the time of year and other cyclical factors. You recently noticed that ABC’s weekly deposits have nearly doubled to an average of $1,900 per week and are more frequent, sometimes twice daily.

QUESTION 24. Should your suspicions be raised by the change in deposit behavior?

__________________________________________________________________________

__________________________________________________________________________

QUESTION 25. What questions should you ask yourself to ascertain if the account is suspicious?

__________________________________________________________________________

__________________________________________________________________________

QUESTION 26. Should you ask the client to explain the change in the amount and number of deposits?

__________________________________________________________________________

__________________________________________________________________________

QUESTION 27. What should you do? Should you visit the business establishment?

__________________________________________________________________________

__________________________________________________________________________
3.7 Cash transaction reports (CTRs)

CTRs are used most often by countries with highly developed financial systems and where it is common for noncash modern technologies to be used for payments (for example, checks, credit/debit cards, e-banking, etc.). Cash transaction reports are also used by cash-based economies, such as Slovenia, Croatia, and Nigeria, to name a few. The usefulness of CTRs in identifying ML/FT varies across countries. Those that elect to employ a CTR system should have the analytical capability and technology to justify its cost. FATF Recommendation 19 provides that countries should consider the feasibility and utility of, but not necessarily impose, a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions, above a fixed amount, to a national central agency with a computerized data base. For more information on FATF Recommendation 19, see Appendix Y.

Where a country has implemented a CTR system, the threshold should be high enough to screen out insignificant transactions, yet low enough to be meaningful. Countries should also make certain categories of clients exempt, such as government agencies, and/or provide higher reporting thresholds for entities that are traditionally cash intensive, such as gas stations and restaurants, from the CTR requirements for transactions. Such exceptions should be reviewed on a regular basis to determine if it is still appropriate in certain circumstances, both as a rule and for specific entities.
Financial institutions and DNFBPs subject to AML/CFT laws should establish and maintain an effective AML/CFT program that includes at least the following:

- Policies, procedures, and controls including screening new employees
- Compliance arrangements, including the appointment of an AML/CFT compliance officer
- Ongoing employee training programs
- Internal audit and, where applicable, external audit functions

The internal compliance program should be documented, approved by the board of directors, and communicated to all levels of the organization. In developing an AML/CFT compliance program, attention should be paid to the size and range of activities, complexity of operations, and the nature and degree of ML/FT risk facing an institution.

FATF Recommendation 15 requires that financial institutions have an internal control program. Recommendation 16 suggests the principle be applied to DNFBPs. For more information on FATF Recommendation 15, see Appendix Z. For more information on FATF Recommendation 16, see Appendix W.

### 4.1 The role of the board/senior management

The board of directors and senior management of financial institutions and DNFBPs should establish, where needed, formal policies, procedures, and controls (PPCs) on AML/CFT that are equal to the risks undertaken and the size and complexity of an institution. PPCs should be communicated to all levels of staff and should foster a culture of compliance throughout the organization. Management commitment to the implementation of these policies should be clearly demonstrated by providing adequate resources for their effective implementation. A strong corporate governance framework within an organization supports AML/CFT controls. Key to instituting a resilient framework is promoting a culture of ethics and integrity when interacting with customers and official agencies. This kind of culture could be supported by codes of conduct/ethics at the institutional and/or sector level. Supervisors for the various reporting entities should actively promote and provide support in the development and dissemination of such codes.
4.2 What should the board/senior management do?

Demonstrating board/senior management commitment to the implementation of an effective AML/CFT compliance program may include, but not be limited to, the following:

- Formulation and implementation of a corporate governance program that emphasizes sound internal controls and ethical behavior throughout the organization. Implementation of this program should start at the top with the board of directors and senior management, who should then set the tone for compliance and good governance for the rest of the organization.
- A comprehensive program that includes internal controls for the approval and monitoring of new clients, accounts, products, and services and then the incorporation of procedures to ensure ongoing CDD, monitoring of account activity, and internal reporting of any unusual and suspicious activities.
- Enhanced CDD and monitoring for higher-risk areas and clients.
- An information system to inform senior management of AML/CFT issues in a timely and transparent manner, including the results of audits and compliance reviews, the discovery of any AML/CFT deficiencies, and corrective action to be taken.
- Clear lines of responsibility for AML/CFT compliance, which can be made a condition of employment and to influence performance evaluations.
- Adequate human and technological resources to guarantee an operative AML/CFT program.

Rigorous screening programs for new staff is another important control mechanism, especially in high-risk jurisdictions. This would promote high ethical standards within an institution. Organizations must use “know your employees (KYE)” as much as they employ KYC rules. Employees promoted or assigned to higher-risk areas of an organization may be asked to undergo intensive screening and training.

4.3 Appointment of AML/CFT compliance officer/money laundering reporting officer

Financial institutions and other DNFBPs should designate a qualified employee, who has day-to-day responsibility for managing all aspects of the AML/CFT compliance program, as its compliance officer. The AML/CFT compliance officer’s main responsibility is to monitor institutional compliance with the AML/CFT laws, regulations and guidelines and internal policies and controls. Where the institution forms part of a financial group or has overseas operations, the AML/CFT compliance program should be applied on a group-wide basis so that all aspects of its operations and product lines, wherever located, are adequately covered.

It is the responsibility of the board of directors and senior management to appoint the person to a level high enough within the organization to be viewed as a senior official and delegate enough authority to the officer to administer a
comprehensive AML/CFT compliance program. In particular, the compliance officer should have unfettered access to all information essential to his or her responsibilities. Finally, the compliance officer acts as the principal point of contact with regulators, the FIU, and other authorities concerned with AML/CFT issues.

4.4 Ongoing employee training program

Financial institutions and other DNFBPs must see that staff is trained on all aspects of the AML/CFT legislative and regulatory requirements, and on internal anti-money laundering policies, procedures, and controls. An effective training program should

- describe the risks of money laundering and terrorist financing schemes, methodologies, and typologies;
- explain AML/CFT laws and other national and regulatory requirements;
- explain an institution’s policies and systems with regard to customer identification, due diligence, monitoring, and reporting suspicious activities, stressing the importance of not tipping off clients;
- offer relevant training; and
- inform employees of the consequences when failing to comply with legal and institutional AML/CFT requirements, including fines, imprisonment, and termination of employment.

Targets should include

- all staff appropriate to their roles within the organization; highlight ML/FT risks inherent in their activities;
- employees and senior management, the Board of Directors in some cases, and especially persons who have contact with customers; and
- intensive and ongoing training for employees who manage and monitor customer accounts/transaction activity, or who handle cash or other monetary instruments.

Training should be ongoing, incorporating trends and developments in an institution’s business risk profile, as well as changes in the AML/CFT legislation. Training on new money laundering schemes and typologies are of the utmost importance when reviewing policies and controls and designing monitoring mechanisms for suspicious activity.
4.5 Compliance and internal audit to test the system

An institution’s internal auditor should be well resourced and enjoy a degree of independence within the organization. The internal audit should

- test the overall integrity and effectiveness of the management systems and the AML/CFT control environment;
- focus on risk-based audit programs and procedures and include sample tests, emphasizing CDD and high-risk markets, operations, products, and services;
- assess the adequacy of the bank’s processes for identifying and reporting suspicious activity;
- communicate the findings to the board and/or senior management in a timely manner; and
- recommend specific corrective action for deficiencies.

External auditors can play an essential part in reviewing the adequacy of AML/CFT controls by communicating their findings and recommendations to management via the annual management letter, which accompanies the audit report. International audit firms risk-focus their audit programs now and conduct intensive reviews of higher-risk areas where controls may be deficient. In some countries external auditors may be expected by law to report incidences of suspected criminal activity uncovered during audits, to the financial sector supervisors or other competent authority. They may want to discuss the results of their audits with supervisory authorities, including AML/CFT control deficiencies in reporting institutions.
Professional and trade associations can play an important role in fostering AML/CFT compliance across the covered sectors. This would create a playing field where peer pressure might be applied to noncompliant institutions to strengthen their AML/CFT mechanisms.

5.1 Providing training

Training is one area where these associations can contribute and make a difference. Although large financial institutions develop institution-specific training programs for staff, it is common for small countries and financial sectors to organize training at the industry level. Consequently, members of the former can benefit from the development and delivery of training programs by professional associations; furthermore, regulator and FIU participation in training programs would enrich discussions and learning.

5.2 Develop cooperation and understanding

By involving industry associations and their regulators, a common understanding of the risks and logical responses could be developed; this involvement would also engender cooperation among the various stakeholders. Industry-wide training programs benefit additionally from scale and scope economies, providing excellent opportunities for cross-sector/cross-institutional sharing of experiences. Notwithstanding such industry efforts, individual institutions would still be called on to provide specific training to their staff on internal policies, procedures, and controls, and the idiosyncratic risks facing them.
Country examples

American Bankers Association (ABA)
The ABA brings together money laundering experts in law, law enforcement, and financial services for seminars.

British Bankers Association (BBA)
The BBA has produced guidance notes for the financial sector since 1990. It also offers a money laundering prevention program in e-learning format.

Swiss Bankers Association (SBA)
The SBA has published a money laundering brochure that illustrates the advanced methods used by Switzerland to fight money laundering. A section of the association’s Web site is dedicated to money laundering issues.

West African Bankers Association
The West African Bankers Association published money laundering guidance in one of its magazines. The information is also available on the association’s Web site.

American Insurance Association (AIA)
The AIA has concerns not only about money laundering and terrorist financing but also with regard to the Terrorist Risk Insurance Act of 2002.

Latin American Association of Insurance Supervisors (ASSAL)
The AASAL exchanges information on legislation, regulatory control, market characteristics, and operational systems in the region. Its goal is to promote technical cooperation in the design of effective policy and supervisory mechanisms.

ASEAN Bankers Association
The ASEAN Bankers Association promotes the development of banking and the financial system in the region, in part by encouraging cooperation among bankers.
Supervisory and/or other competent authorities should have the powers to address a financial institution’s or DNFBP’s failure to meet statutory or regulatory requirements. The powers should be broad enough to compel the imposition of sanctions against institutions, owners, and officials where necessary. FATF Recommendation 17 is particularly relevant here, requiring countries to ensure that effective, proportionate, and dissuasive sanctions, whether criminal, civil, or administrative, are available to deal with natural or legal persons covered by FATF Recommendations. For more information on FATF Recommendation 17, see Appendix AA.

Although the adoption of anti-money laundering and terrorist financing laws will affect the development of a meaningful legal framework, it is by itself insufficient. More critical are legal and regulatory imperatives and credible methods for enforcement. To do otherwise would contribute to a lack of faith in the AML/CFT regime and to apathy in the face of a lack of enforcement. Consequently, to foster compliance, sanctions should be reasonable, proportionate, and dissuasive. Depending on each country’s legal system, sanctions can range from criminal to civil to administrative action by the competent authorities.

In light of a country’s legal system and traditions, the responsibility to monitor and enforce compliance could fall on several agencies. In many countries, the burden is shouldered by supervisory authorities for particular industries or sectors, such as the Central Bank, and supervisors for insurance and securities. In others, the FIU assumes this role, especially for the nonprudentially regulated sectors, such as casinos, real estate agents, jewelers, car dealers, and so on. There may be a call for self-regulatory organizations—namely, in designated professions like law and accounting. Irrespective of who has the obligation, it is vital that the organization/authority has indisputable authority and available resources to discharge its enforcement responsibilities.

Do not underestimate the need for a range of available remedial measures and sanctions to impose on institutions and officials that fail to comply with, or fully implement, AML/CFT requirements. These measures can run the gamut, from simple warnings to criminal charges to revocation of a license to operate, offering flexibility to the enforcement authority to apply the sanction most suited to the unique particulars of a case. Sanctions should also require corrective action if the institution or individual is to remain in business.
Module discussion

Consider the following questions and provide your responses in the spaces below each.

QUESTION 28. What are the main sanctions a supervisory authority can impose on institutions and persons?

QUESTION 29. What are the main sanctions a self-regulatory body can impose on its members?

Check your understanding

QUESTION 30. Provide three reasons why supervisors should be concerned about money laundering and/or terrorist financing risks in the financial system.

QUESTION 31. Identify three to five risks facing financial institutions, that could pose safety and soundness concerns.
**QUESTION 32.** Under what circumstances would financial sector supervisors be required to cooperate and share information with other national and international agencies involved in AML/CFT? Identify the main agencies with which supervisors may be required to cooperate.

**QUESTION 33.** What financial and business sectors do you think pose a higher degree of risk in your country? Identify the five sectors with the highest degree of risk.

**QUESTION 34A.** Review the following bank account for unusual and suspicious activity. Identify at least three red flags that should prompt you to inquire further. These should be easily identified by a simple visual scan of the account.

<table>
<thead>
<tr>
<th>Date</th>
<th>Debits</th>
<th>Credits</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-Jan-00</td>
<td>Beginning Balance</td>
<td></td>
<td>2,500.00</td>
</tr>
<tr>
<td>2-Jan-00</td>
<td>Deposit-cheque</td>
<td>7,523.89</td>
<td>10,023.89</td>
</tr>
<tr>
<td>4-Jan-00</td>
<td>Deposit-cash</td>
<td>9,874.33</td>
<td>17,878.22</td>
</tr>
<tr>
<td>5-Jan-00</td>
<td>Deposit-cash</td>
<td>12,547.89</td>
<td>25,446.11</td>
</tr>
<tr>
<td>5-Jan-00</td>
<td>Wire-in</td>
<td>25,348.19</td>
<td>57,794.30</td>
</tr>
<tr>
<td>9-Jan-00</td>
<td>Cheque</td>
<td>8,756.00</td>
<td>49,036.10</td>
</tr>
<tr>
<td>9-Jan-00</td>
<td>Wire-out</td>
<td>46,713.90</td>
<td>2,324.90</td>
</tr>
<tr>
<td>12-Jan-00</td>
<td>Deposit-cash</td>
<td>11,001.45</td>
<td>21,002.94</td>
</tr>
<tr>
<td>13-Jan-00</td>
<td>Deposit-cash</td>
<td>20,345.83</td>
<td>40,691.67</td>
</tr>
<tr>
<td>14-Jan-00</td>
<td>Wire-out</td>
<td>39,994.35</td>
<td>79,942.42</td>
</tr>
<tr>
<td>15-Jan-00</td>
<td>Deposit-cash</td>
<td>75,345.04</td>
<td>152,677.46</td>
</tr>
<tr>
<td>16-Jan-00</td>
<td>Wire-out</td>
<td>50,113.29</td>
<td>100,636.37</td>
</tr>
<tr>
<td>16-Jan-00</td>
<td>Withdrawal-cash</td>
<td>21,009.00</td>
<td>111,645.17</td>
</tr>
<tr>
<td>20-Jan-00</td>
<td>Deposit-cash</td>
<td>34,197.65</td>
<td>45,582.82</td>
</tr>
<tr>
<td>21-Jan-00</td>
<td>Deposit-cash</td>
<td>14,990.32</td>
<td>60,533.14</td>
</tr>
<tr>
<td>21-Jan-00</td>
<td>Deposit-cash</td>
<td>17,678.00</td>
<td>78,511.14</td>
</tr>
<tr>
<td>23-Jan-00</td>
<td>Wire-in</td>
<td>49,949.00</td>
<td>128,451.14</td>
</tr>
<tr>
<td>24-Jan-00</td>
<td>Wire-out</td>
<td>97,500.45</td>
<td>195,000.69</td>
</tr>
<tr>
<td>25-Jan-00</td>
<td>Withdrawal-cash</td>
<td>26,678.00</td>
<td>4,331.69</td>
</tr>
<tr>
<td>25-Jan-00</td>
<td>Cheque</td>
<td>745.23</td>
<td>3,586.46</td>
</tr>
</tbody>
</table>
QUESTION 34B. Should it be reported to your money laundering reporting officer in your bank? If yes, why?

Summary
In this module, we discussed

- what entities have organizational and administrative authority for effective supervision among relevant sectors;
- what entities and individuals are subject to AML/CFT compliance requirements;
- the regulatory and institutional requirements for financial institutions and DNFBPs; and
- why training is important and the roles of professional associations.
Appendix A: References

FATF Recommendations

  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- *Special Recommendations on Terrorist Financing* (FATF, October 2004)

Useful Web sites

- ASEAN Bankers Association
  http://aseanbankers.org/association/
- American Bankers Association
  http://www.aba.com/
- American Insurance Association
  http://www.aiadc.org/
- Basel Committee on Banking Supervision (BCBS)
  http://www.bis.org/bcbs/index.htm
- British Bankers Association
  http://www.bba.org.uk/
- International Organization of Securities Commissions (IOSCO)
  http://www.iosco.org
- INTERPOL
  http://www.interpol.int/Default.asp
Reference Documents


- Core Principles for Effective Banking Supervision (Basel Core Principles) (BCBS, September 1997)
  http://www.bis.org/publ/bcbsc102.pdf

- Core Principles Methodology (BCBS, October 1999)
  http://www.bis.org/publ/bcbs61.pdf

- Customer Due Diligence for Banks (BCBS, October 2001)
  http://www.bis.org/publ/bcbs85.pdf

- Consolidated KYC Risk Management (BCBS, October 2004)
  http://www.bis.org/publ/bcbs110.pdf


- A Resolution on Money Laundering (IOSCO, October 1992)

- Joint Forum (Initiatives by the BCBS, IAIS, and IOSCO to combat money laundering and the financing of terrorism, June 2003)
Countries should ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations. Competent authorities should take the necessary legal or regulatory 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 a financial institution.

For financial institutions subject to the Core Principles, the regulatory and supervisory measures that apply for prudential purposes and which are also relevant to money laundering, should apply in a similar manner for anti-money laundering and terrorist financing purposes.

Other financial institutions should be licensed or registered and appropriately regulated, and subject to supervision or oversight for anti-money laundering purposes, having regard to the risk of money laundering or terrorist financing in that sector. At a minimum, businesses providing a service of money or value transfer, or of money or currency changing, should be licensed or registered, and subject to effective systems for monitoring and ensuring compliance with national requirements to combat money laundering and terrorist financing.

Interpretative Note to Recommendation 23

Recommendation 23 should not be read as to require the introduction of a system of regular review of licensing of controlling interests in financial institutions merely for anti-money laundering purposes, but as to stress the desirability of suitability review for controlling shareholders in financial institutions (banks and non-banks in particular) from a FATF point of view. Hence, where shareholder suitability (or “fit and proper”) tests exist, the attention of supervisors should be drawn to their relevance for anti-money laundering purposes.
Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

Appendix C: FATF Recommendation 29
Appendix D: 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.

Interpretative Note to Recommendation 25

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.
Appendix E: FATF Recommendation 24

Designated non-financial businesses and professions should be subject to regulatory and supervisory measures as set out below.

a) Casinos should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary anti-money laundering and terrorist financing measures. At a minimum:

- casinos should be licensed;
- competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest, holding a management function in, or being an operator of a casino;
- competent authorities should ensure that casinos are effectively supervised for compliance with requirements to combat money laundering and terrorist financing.

b) Countries should ensure that the other categories of designated non-financial businesses and professions are subject to effective systems for monitoring and ensuring their compliance with requirements to combat money laundering and terrorist financing. This should be performed on a risk-sensitive basis. This may be performed by a government authority or by an appropriate self-regulatory organisation, provided that such an organisation can ensure that its members comply with their obligations to combat money laundering and terrorist financing.
Appendix F: FATF Recommendation 20

Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk.

Countries should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.
Appendix G:
FATF Recommendation 4

Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.
Appendix H: FATF Recommendation 28

When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.
Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.3
b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

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 institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction. The measures that are taken should be consistent with any guidelines issued by

---

3 Reliable, independent source documents, data, or information will hereafter be referred to as “identification” data.
competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction; or should terminate the business relationship; and should consider making a suspicious transaction report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk, and should conduct due diligence on such existing relationships at appropriate times.
Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a)–(c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)–(c) of the CDD process. Financial institutions should 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.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.

**Interpretative Note to Recommendation 9**

This Recommendation does not apply to outsourcing or agency relationships.

This Recommendation also does not apply to relationships, accounts or transactions between financial institutions for their clients. Those relationships are addressed by Recommendations 5 and 7.
Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
b) Obtain senior management approval for establishing business relationships with such customers.
c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship.

Interpretative Note to Recommendation 6
Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.
Appendix L: FATF Recommendation 7

Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, and in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Assess the respondent institution’s anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities of each institution.

e) With respect to “payable-through accounts,” be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.
Appendix M: FATF Recommendation 8

Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.
The customer due diligence and recordkeeping requirements set out in Recommendations 5, 6, and 8 to 11 apply to designated non-financial businesses and professions in the following situations:

a) Casinos—when customers engage in financial transactions equal to or above the applicable designated threshold.
b) Real estate agents—when they are involved in transactions for their client concerning the buying and selling of real estate.
c) Dealers in precious metals and dealers in precious stones—when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.
d) Lawyers, notaries, other independent legal professionals and accountants when they prepare for or carry out transactions for their client concerning the following activities:
   - buying and selling of real estate;
   - managing of client money, securities or other assets;
   - management of bank, savings or securities accounts;
   - organisation of contributions for the creation, operation or management of companies; and
   - creation, operation or management of legal persons or arrangements, and buying and selling of business entities.

e) Trust and company service providers when they prepare for or carry out transactions for a client concerning the activities listed in the definition in the Glossary.

**Interpretative Note to Recommendations 5, 12, and 16**

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3,000.
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.
COUNTRIES SHOULD NOT APPROVE THE ESTABLISHMENT OR ACCEPT THE CONTINUED OPERATION OF SHELL BANKS. FINANCIAL INSTITUTIONS SHOULD REFUSE TO ENTER INTO, OR CONTINUE, A CORRESPONDENT BANKING RELATIONSHIP WITH SHELL BANKS. FINANCIAL INSTITUTIONS SHOULD ALSO GUARD AGAINST ESTABLISHING RELATIONS WITH RESPONDENT FOREIGN FINANCIAL INSTITUTIONS THAT PERMIT THEIR ACCOUNTS TO BE USED BY SHELL BANKS.
Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries that do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.
Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above, are also applied to branches and majority owned subsidiaries located abroad, especially in countries that do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.
Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

**Interpretative Note to Recommendations 10 and 11**

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself; the premium payment and the benefits.
Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

**Interpretative Note to Recommendations 10 and 11**

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself, the premium payment and the benefits.
If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

**Interpretative Note to Recommendation 13**

The reference to criminal activity in Recommendation 13 refers to:

a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or

b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.
Appendix U: FATF Recommendation 14

Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing that a suspicious transaction report (STR) or related information is being reported to the FIU.

Interpretative Note to Recommendation 14

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.
Appendix V:
FATF Special Recommendation IV

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, 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 organisations, they should be required to report promptly their suspicions to the competent authorities.

FATF Guidance Notes

SR IV: Reporting suspicious transactions related to terrorism

This Recommendation contains two major elements:

- Jurisdictions should establish a requirement for making a report to competent authorities when there is a suspicion that funds are linked to terrorist financing; or
- Jurisdictions should establish a requirement for making a report to competent authorities when there are reasonable grounds to suspect that funds are linked to terrorist financing.

For SR IV, the term financial institutions refers to both banks and non-bank financial institutions (NBFIs). In the context of assessing implementation of FATF Recommendations, NBFIs include, as a minimum, the following types of financial services: bureaux de change, stockbrokers, insurance companies and money remittance/transfer services. This definition of financial institutions is also understood to apply to SR IV in order to be consistent with the interpretation of the FATF Forty Recommendations. With regard specifically to SR IV, if other types of professions, businesses or business activities currently fall under anti-money laundering reporting obligations, jurisdictions should also extend terrorist financing reporting requirements to those entities or activities.

The term competent authority, for the purposes of SR IV, is understood to be either the jurisdiction’s financial intelligence unit (FIU) or another central authority that has been designated by the jurisdiction for receiving disclosures related to money laundering.
With regard to the terms *suspect* and *have reasonable grounds to suspect*, the distinction is being made between levels of mental certainty that could form the basis for reporting a transaction. The first term—that is, a requirement to report to competent authorities when a financial institution suspects that funds are derived from or intended for use in terrorist activity—is a subjective standard and transposes the reporting obligation called for in FATF Recommendation 15 to SR IV. The requirement to report transactions when there are reasonable grounds to suspect that the funds are derived from or intended for use in terrorist activity is an objective standard, which is consistent with the intent of Recommendation 15 although somewhat broader. In the context of SR IV, jurisdictions should establish a reporting obligation that may be based either on suspicion or on having reasonable grounds to suspect.
The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

**Interpretative Note to Recommendation 16**

1) It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2) Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.
Interpretative Note to Recommendations 5, 12, and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5) - USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12) - USD/EUR 3,000.
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16) - USD/EUR 15,000. Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.
Appendix X: Red flags

Banking sector

General signs

- **Smurfing**: Customers depositing small amounts of cash on different successive occasions, in such a way that on each occasion the amount involved is not significant, but all together the total equals a very large amount, a practice known as “smurfing”
- Customers not acting on their own behalf and refusing to reveal the true identity of the beneficiary
- Customers and prospective customers providing insufficient, false, or suspicious information, or information that is difficult or expensive to verify
- Customers refusing to provide information that, under normal circumstances, would permit access to credit facilities or other valuable banking services
- Customers holding several accounts and making cash deposits into each, such that the total amount deposited becomes considerable
- Accounts that show virtually no banking activity but are used to receive or pay significant amounts not clearly related to the customer or the customer’s business
- Withdrawals of large amounts from an account previously dormant or inactive, or from an account that has just been credited with a large amount unexpectedly from abroad
- Customers maintaining accounts with several financial institutions in the same city or town, especially the accounts regularly consolidated prior to a request for a transfer of the funds
- The balancing of payments with credits made in cash the same day or the previous day
- Frequent deposits and withdrawals to and from accounts consistently in rounded numbers, especially if inconsistent with the known business activity of the customer
- Customers who together and simultaneously use separate cashiers to carry out substantial operations in cash or foreign currency
- Increased use of safety deposit boxes. Increased banking activity by the persons holding the boxes. The depositing and withdrawal of sealed packages
- Company representatives avoiding contact with the office
• Substantial increases in cash deposits or deposits of negotiable instruments by a professional firm or company using accounts opened in the name of the client or a fiduciary company (such as a trust or nominee company), especially if such deposits are quickly transferred to another client account
• Insufficient use of the normal advantages offered by banks, such as failing to take advantage of higher interest rates for large balances
• Cash deposits by many individuals into the same account without an appropriate explanation
• Purchases or deposits of monetary instruments inconsistent with the business or profession of the customer
• Wire transfer activity that is not consistent with the business or profession of the customer
• Immediate conversions of funds transferred into monetary instruments in the name of third parties
• A large volume of deposits to one or several accounts with frequent transfer of a major portion of the balances to another account(s) at the same or another bank
• Many deposits of cashier’s checks, money orders, or wire transfers
• Simultaneous deposits to a single account made at different branches
• Receipt over a short period of several small deposits through transfers, checks, and money orders, followed immediately by a wire transfer of those funds to another location, town, city, or country, leaving only a small balance in the account
• Frequent sending and receiving of wire transfers, especially to or from countries considered high risks for money laundering (such as major drug producing and drug transit countries), or with strict banking secrecy laws. Special attention is warranted if such operations occur through small or family-run banks, shell banks, or unknown banks
• A discrepancy between the domicile of a customer’s account and the service area of the branch in which the customer normally transacts
• Large deposits by customers who claim that the funds are lottery or casino winnings
• Unusually large deposits or withdrawals of cash by an individual or a legal entity whose apparent business activities are normally carried out using checks and other monetary instruments
• Substantial increases in cash deposits by any person for no apparent reason, especially if such deposits are subsequently transferred within a short time to a destination not normally associated with the customer
• Customers seeking to change large quantities of notes of small denomination for larger ones, or frequently changing large amounts of cash into foreign currency
• Transfers of large amounts of money to or from abroad, with instructions that payment be made in cash
• Deposits of large amounts of cash using night safes, thus avoiding direct contact with bank personnel
• Frequent or large cash exchanges of local currency into foreign currency or vice versa, without any apparent connection with the professional or commercial activity of the customer
• Frequent cash deposits, over the counter or via the night depository, or cash withdrawals of large amounts, without any apparent justification in terms of the type and volume of the business in question
• Proposals for large operations involving the sale of foreign bank notes (usually U.S. dollars) or checks drawn in foreign currency against local currency, made by persons claiming to be intermediaries or commission agents and who on occasion claim to have contacts with the local authorities or the tacit approval of the central bank with respect to the carrying out of such operations
• Frequent deposits of large amounts of foreign currency

**Money Laundering through Loans with or without Collateral**

• Loans without a clear purpose
• Customers unexpectedly paying off problem loans, without indication of the origin of the funds
• Loans completely or partially paid off in cash, foreign currency, or other instruments in which the issuer is not revealed
• Loans repaid with funds deposited in another institution by third parties, the origin of which is unknown or the value of which bears no relation with the customer’s known situation
• A request for a loan backed by assets deposited in the financial entity or by third parties, the source of which is unknown or the value of which has no relation to the situation of the customer
• A request for financing, when the source of the financial contribution of the customer with respect to a business is unclear, particularly if real estate is involved
• Loans guaranteed by third parties with no apparent relation to the customer
• Loans secured by property that will be disbursed in another jurisdiction
• Requests for credit facilities from little-known customers who offer guarantees in cash, financial assets, foreign currency deposits, or foreign bank guarantees, and whose business bears no relation to the object of the operation
• Default on credit used for legal trading activities, or transfer of such credits to another company, person, or entity, without any apparent justification, leaving the bank to enforce the guarantee backing the credit
• Letters of credit documenting imports and exports but with no information regarding the importer or exporter, in violation of established standards
• The use of standby letters of credit to guarantee loans granted by foreign financial entities, without any apparent economic justification
MONEY LAUNDERING THROUGH OFFSHORE ACTIVITIES

- Customers who frequently conduct operations with companies or financial institutions located in countries with strict secrecy laws and without adequate supervisory or regulatory structures
- A customer introduced by a foreign branch, affiliate, or bank based in a country where drug production or trafficking is frequent
- The use of letters of credit and other offshore mechanisms for moving money between countries where such activity bears no relation to the customer’s normal business
- Use of back-to-back loans, where deposits securing the loans are made in offshore entities, while the loans are granted and disbursed to parties in another jurisdiction
- Use by customers of cash-secured international credit cards issued by offshore entities, and frequent use of ATM or other banking facilities to withdraw cash
- The creation of large balances in accounts that are not consistent with the customer’s business, and subsequent transfers to accounts offshore
- Electronic funds transfers, without explanation by customers, involving an immediate deposit and withdrawal from the account or even without passing through an account (for example, through the use of omnibus, suspense, or consolidation accounts)
- Use of “payable-through” accounts, where the beneficiaries of the accounts are unknown or where they are clients of offshore entities with strict secrecy laws
- Frequent requests for traveler’s checks, foreign denomination drafts, or other negotiable instruments without a clear purpose
- Frequent deposits in an account of traveler’s checks or foreign denomination drafts, especially if originating from abroad without a clear purpose
- Frequent deposits to customer accounts originating from casas de cambios in countries with inadequate regulations, especially where the customer is a broker or acting as an intermediary for others
- Customers depositing loan proceeds borrowed from offshore institutions under participation agreements, nominee, or trust arrangements, and where the source of the funds is unknown
- Cash deposits from offshore correspondent banks, where the frequency and volume of deposits are substantial in view of the size, nature, and location of the client bank

ACCOUNTS UNDER INVESTIGATION OR LEGAL PROCEEDINGS

- Accounts under official investigation or served with legal process, seizure, or restraining orders, or other action relating to fraud or money laundering, by competent national or foreign authorities
- Accounts that are the source or receiver of significant funds related to an account or person under investigation or the subject of legal proceedings in
a court or other competent national or foreign authority in connection with fraud or money laundering

- Accounts controlled by the signatory of another account that is under investigation or the subject of legal proceedings by a court or other competent national or foreign authority in connection with fraud or money laundering, in the country or abroad

**Insurance sector**

**Insurance sector—specific signs**

- Application for a policy from a potential client in a distant place where a comparable policy could be provided closer to home
- Application for business outside the policyholder’s normal pattern of business
- Introduction by an agent or intermediary in an unregulated or loosely regulated jurisdiction or where organized criminal activities (such as drug trafficking or terrorist activity) are prevalent
- Missing information or delay in the provision of information to enable verifications
- Transactions involving an undisclosed party
- Early termination of a product, especially at a loss caused by front-end loading, or where cash was tendered or the refund check is made out to a third party
- A transfer of the benefit of a product to an apparently unrelated third party
- Requests for a large purchase of a lump-sum contract, where the policyholder’s experience is with contracts involving small, regular payments
- Attempts to use a third-party check to make a proposed purchase of a policy
- Applicant for insurance shows no concern for the performance of the policy but intense concern over early cancellation of the contract
- Applicant attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by checks or other payment instruments
- Applicant requests to make a lump-sum payment by a wire transfer or with foreign currency
- Applicant is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or information that is difficult or expensive for the institution to verify
- Applicant appears to have policies with several institutions
- Applicant purchases policies in amounts considered beyond the customer’s apparent means
- Applicant establishes a large insurance policy and within a short time cancels the policy and requests the cash value refunded to a third party
- Applicant seeks to borrow the maximum cash value of a single premium policy soon after paying for the policy
- Applicant uses a mailing address outside the insurance supervisor’s jurisdiction and where the home telephone has been disconnected
- “Churning” at the client’s request
MONEY LAUNDERING INVOLVING EMPLOYEES OR OFFICIALS OF FINANCIAL INSTITUTIONS

- Unexplained changes in an employee’s behavior—for example, a lavish lifestyle, avoidance of holidays, association with known drug traffickers or criminals
- Significant and abnormal changes in performance by an employee, such as a large increase in cash sales
- Refusals to accept promotions, transfers, or changes in an employee’s duties and responsibilities
- Arrangements made by an employee to supply the institution’s services or products to an unknown or concealed final beneficiary, contrary to normal operating procedures on identification and source of funds
- An unusually high level of single-premium business
- Use by employees of their own business address for the “delivery of customer documentation”

Securities sector—specific signs

- Lack of concern by customers about risks, commissions, or other transaction costs
- Customers who have difficulty describing the nature of his or her business or lack general knowledge of their industry
- Customers who, for no apparent reason, maintain multiple accounts under a single name or multiple names, with a large number of inter account or third-party transfers
- Purchases of securities to be kept in custody by the financial institution, where the operation appears to be inconsistent with the customer’s business
- Requests from customers for investment handling services, in foreign currency or securities, where the source of funds is not clear or is inconsistent with the customer’s known business
- Security transactions through a trust or similar intermediary, characterized by substantial cash transactions or transactions made through an offshore entity bearing no relation to the customer’s business
- Purchases by customers of bearer shares, especially if issued by offshore entities
- Purchase and sale of financial instruments without any apparent purpose or in unusual circumstances
- Introduction by a broker or intermediary in an unregulated or loosely regulated jurisdiction or where organized crime (drug trafficking, terrorist activity) is prevalent
- Missing information or delay in providing information for verifications
- Transactions involving an undisclosed party
- Customer attempts to use cash to complete a proposed transaction when the transaction would normally be handled by check or another method of payment
• Customers who exhibit unusual concern about the firm’s compliance with government reporting requirements or about the firm’s AML policies, particularly with respect to customers’ identity, type of business, and assets; customers who are reluctant or refuse to reveal any information about business activities, or who furnish unusual or suspect identification or business documents

• Customers who engage in transactions that lack business sense or apparent investment strategy, or that are inconsistent with the customer’s stated business strategy

• Customers who make deposits for the purpose of purchasing a long-term investment, followed shortly thereafter by a request to liquidate the position and transfer of the proceeds from the account

• Accounts that show an unexplained level of account activity with very low levels of securities transactions

• Inactive accounts that suddenly show large investments inconsistent with the normal investment practice of the client or the client’s financial ability

• Clients who attempt to purchase investments with cash

• Clients who wish to purchase investments with money orders, traveler’s checks, cashiers checks, bank drafts, or other bank instruments, especially in amounts that are slightly less than $10,000, where the transaction is inconsistent with the normal investment practice of the client or the client’s financial ability

• Clients who use securities or futures brokerage firms as a place to hold funds that are not being used to trade in securities or futures, where such activity is inconsistent with the normal investment practice of the client or the client’s financial ability

• Clients who are willing to deposit or invest at rates that are not advantageous or competitive

**DNFBPs**

**Accountants**

• Clients who appear to be living beyond their means

• Clients whose business activity is inconsistent with industry averages or financial ratios

• Clients whose checks are inconsistent with sales (indicating unusual payments from unlikely sources)

• Clients who change bookkeepers or accountants yearly

• Clients who are uncertain about the location of company records

• Companies that carry nonexistent or satisfied debt that is continually shown as current on financial statements

• Companies that have no employees, when having no employees is unusual for the type of business

• Companies that are paying unusual consulting fees to offshore companies
• Company records that consistently reflect sales at less than cost, thus putting the company into a loss position, while the company continues to operate without reasonable explanation of the continued loss
• Company shareholder loans that are not consistent with business activity
• Misstatements of business activity that cannot be readily traced through the company books
• Large payments to subsidiaries or similarly controlled companies that are not within the normal course of business
• Companies that acquire large personal and consumer assets (boats, luxury automobiles, personal residences, vacation property) when this type of transaction is inconsistent with the ordinary business practice of the client or the practice prevailing in that particular industry
• Companies that receive invoices from organizations located in countries with inadequate money laundering laws or highly secretive banking and corporate laws (tax havens)

**Real Estate Brokers**

• Clients who arrive at a real estate closing with a significant amount of cash
• Clients who purchase property in the name of a nominee such as an associate or a relative (other than a spouse)
• Clients who do not want to put their name on any document that would connect them with the property, or who use different names on offers to purchase, closing documents, and deposit receipts
• Clients offering unpersuasive explanations for a last-minute substitution of the purchasing party’s name
• Clients who negotiate a purchase for market value or above the asking price, but who then record a lower value on documents, paying the difference under the table
• Clients who sell property below market value but who demand an additional payment under the table
• Clients who make their initial deposit using a check from a third party (other than a spouse or a parent)
• Clients who make a substantial down payment in cash, while the balance is financed by an unusual source or offshore bank
• Clients who purchase personal property under the corporate veil when this type of transaction is inconsistent with the ordinary business practice of the client
• Clients who purchase property without inspecting it
• Clients who purchase multiple properties over a short period and seems to have few concerns about the location, condition, or anticipated repair costs
• Clients who make rental or lease payments in advance using a large amount of cash
• Clients known to have paid large remodeling or home improvement invoices with cash, on a property for which property management services are provided
• Requests for financing, when the source of the customer’s financial contribution to a business is unclear, particularly if real estate is involved

Casinos
• Any casino transaction of $3,000 or more, when an individual receives payment in casino checks made out to third parties or without a specified payee
• Clients who request their winnings check in a third party’s name
• Acquaintances who bet against each other in even-money games, where it appears that they are intentionally losing to one of the party
• Clients who attempt to avoid filing a cash report by breaking up the transaction
• Clients who request checks that are not for gaming winnings
• Clients who inquire about opening an account with the casino or about the possibility of transferring funds to other locations, when the client is not a regular, frequent, or high-volume player
• Clients who purchase large volumes of chips with cash, participate in limited gambling activity with the intention of creating a perception of significant gambling, and then cash in the chips for a casino check
• Clients who exchange small bank notes for large, or who use small bills to purchase chips, vouchers, or checks
• Clients who are known to use multiple names
• Clients who request that their winnings be transferred to the bank account of a third party or to a country known to be a source of drugs, or to a country that has no effective anti-money laundering system

Trusts
• Naming of a foreign individual or legal entity not fully identified to the bank as beneficiary of a trust that owns real or other property
• Contribution of property to a trust without identifying the contributor or the source of the contributor’s funds
• Trusts without a clear purpose, such as “Star” or purpose trusts
• Trusts holding property that consists of companies registered in offshore jurisdictions, especially where shares are in bearer form and the source and amount of company assets are unknown
• Failure of the trust declaration or deed to convey substantive control of trust property to the trustee, and where control rests with other parties, such as the maker of the trust or its beneficiaries
Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.
Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
b) An ongoing employee training programme.
c) An audit function to test the system.

**Interpretative Note to Recommendation 15**

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.
Appendix AA:  
FATF Recommendation 17

Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.
Module 3a Answers

Answer 1
(a) Minimum

Answer 2
(c) Both

Answer 3
(b) False

Answer 4
(b) False

Answer 5
(a) True

Answer 6
To conduct effective supervision for AML/CFT, it is important that there are clear laws and rules as to who is responsible for such supervision. Where supervision is conducted by the traditional supervisory agencies (e.g., Central Bank), the preconditions for effective supervision need to be in place. These include issues such as the operational autonomy of the regulator as well as an appropriate legal framework for supervision that provides reasonable supervisory and enforcement powers and access to information. Supervisors also need to have the necessary resources, both in terms of trained professional staff and funding, to enable proper supervision. Legal protection for the supervisors is also a key element for effective supervision when they carry out their duties in good faith. Supervisory authorities should be given a legal authority to license, supervise, and sanction financial institutions, whenever necessary.

Answer 7
Principal Financial Sectors:

1) Banking sector
2) Insurance sector (life insurance and any other investment-related insurance policies and products)
3) Securities sector including collective investment schemes. This sector is not always present or significant in a large number of developing countries
4) Leasing and finance companies
5) Money remittance and exchange business
6) Other

Other Sectors: DNFBPs
1) Casinos, including Internet casinos
2) Real estate agents
3) Dealers in precious metals and stones
4) Lawyers, notaries, accountants, and other independent legal professionals
5) Trust and Company Services Providers, mainly for offshore financial centers

(See Glossary in the FATF Recommendations for Financial Institutions and Designated Non-financial Businesses and Professions)

**Answer 8**

1) Financial sector supervisors, e.g., Central Bank, Financial Regulatory Commission, Superintendence of Banks and other financial institutions, Securities Commission, Insurance Supervisor, Supervisor for Cooperatives and Credit Unions, Customs and Tax authorities, etc. Please note that some countries have integrated supervisory agencies that supervise the principal financial sectors.

2) Financial Intelligence Unit (FIU). In some countries, the FIU supervises AML/CFT compliance among all covered entities, while in other countries this role is shared with the traditional supervisory agencies and the FIU supervises only those not covered by the supervisors; supervision is not, however, considered a core function of FIUs.

A key issue to consider, irrespective of those who conduct supervision, is the need to establish effective coordination and cooperation among the various agencies involved in AML/CFT efforts.

**Answer 9**

Neither the governor of the Central Bank nor the head of the FIU should provide such information unless it is a legitimate request in accordance with the law. Ordinarily such requests would come from the FIU, police, prosecution, or judicial authorities in accordance with established procedures and the law. Providing such information to the minister, especially if he/she is not authorized to request it under the AML/CFT laws, could open the possibility of legal action against the Central Bank and the FIU. It is obvious that the minister may use the information, by leaking it to the public, to gain political advantage over his/her opponents in the coming election.

Supervisors, including FIUs with supervisory duties, should consider if they have been confronted with similar situations and how it was handled.
**Answer 10**

No, for the reasons cited in answer 9. It may be in breach of the law and would certainly raise questions in the eyes of the financial institutions receiving the request.

**Answer 11**

If the information is provided to the minister and he/she is entitled under the law to receive it, the information will likely be used for political purposes. The Central Bank and the FIU, having advance knowledge of this situation, could be seen as not acting in good faith and would therefore be subject to legal action. Moreover, the credibility and reputation of both the Central Bank and the FIU would be irreparably damaged in the eyes of the financial sector, the public, and other concerned local and international organizations. It would also bring into question the operational autonomy of both institutions, an important prerequisite for their effectiveness and credibility. Additionally, if the information is provided and there is a change in government, it is foreseeable that the incoming administration would take action against officials of both agencies, damaging their viability and effectiveness. At the very least, fining the governor of the Central Bank and the head of the FIU could be justified because they did not act in good faith and probably violated the law.

If the information is not provided, the minister could dismiss or remove both the governor of the Central Bank and the head of the FIU; however, this could be challenged in court.

**Answer 12**

According to the Basel Committee, a “customer” is:

a) a person or entity who maintains an account with a financial institution or on whose behalf an account is maintained (i.e., beneficial owners);

b) beneficiaries of transactions conducted by professional intermediaries (e.g., agents, accountants, lawyers);

c) a person or entity connected with a financial transaction, who can pose a significant risk to the bank.

Depending on the laws, regulations, and guidelines for each country and for purposes of due diligence, “customer” includes occasional customers who do not maintain accounts—e.g., a walk-in client who buys traveler’s checks or drafts. With respect to companies, the “customer” includes those who are authorized to act on behalf of, or have the power to bind, a company. Identification would also be required of “customers” who are principal shareholders or controlling persons in private companies (beneficial owners).
In legal arrangements such as common law trusts, the customer would be the settler of the trust (person transferring property to the trustee), the trustee, and, where applicable, the beneficiaries.

**Answer 13**

For financial institutions conducting KYC, a common challenge is ascertaining whether a customer is acting on his or her own behalf or on behalf of intermediary clients and beneficiaries who are not identified in the documents that are maintained or requested by the financial institution. When there is reason to believe a customer is acting on behalf of another, appropriate due diligence measures should be employed. Because legal entities and arrangements (e.g., corporations, foundations, and trusts) often involve tiered ownership, it is important to establish the ultimate beneficiaries of accounts or transactions. In this case, appropriate due diligence measures should be used to determine the identity of owners and controllers of companies—e.g., parent or controlling entities, including those persons authorized to bind or to act on behalf of such entities.

Accordingly in the case of the above question, the lawyer could be asked in what capacity he or she is acting for the company—e.g., as shareholder, director, or authorized representative. Either way he or she would be identified as a customer. If the lawyer is acting as a representative, the bank should inquire for whom he or she is acting and in what capacity.

**Answer 14**

When clients are acting as trustees, the financial institution should learn the identity of those who contribute assets and those who benefit. Are there other parties involved in the transactions? Who has the power to decide on distributions of trust property? Sometimes there are not specifically named beneficiaries, as in purpose and charitable trusts. The three main parties to a trust relationship, according to common law, are usually the following:

1) Settler: the person who contributes property to the trust
2) Trustee: the person who administers the trust property
3) Beneficiaries: the persons who are identified as benefiting from the property held in trust

Following are examples of the kind of information to request:

- Does the company form part of the trust property?
- What is the purpose of the trust?
- Who is the settler of the trust—that is, who provided the assets/property?
- If known, who are the beneficiaries of the trust?
- What is the source of the property being settled into the trust?
- Copies of the trust documents—e.g., trust deed
Answer 15

It is unlikely the plumber is a high-risk customer given his/her profession and sector. The risk profile could be elevated if the plumber engages in other business or professional activities considered high risk—e.g., he/she is also in the currency exchange business. Possible questions and information could include:

- Identification documents
- Address and place of business if any, including a copy of rent, telephone, utility and/or tax bills, etc., to confirm address
- Copies of past and current business contracts to ascertain source and amount of funds
- Purpose and expected use of the account
- Other, depending on country

Answer 16

This could be a high-risk customer depending on the country and region of operation. More care should be taken with this client because the company deals with individuals from other countries. There should be more concern if this client’s country is on the FATF/NCCT list. Trade-related money laundering is considered significant, and in this case, the re-export business needs closer analysis and scrutiny. In addition to the normal identification of the company, its representative, principal directors, and controlling shareholders, the following information could help establish the risk profile of the client.

- Where is the company incorporated and does it have other affiliates in the country and abroad?
- Has the company issued bearer shares? If so, who has custody of the shares?
- How long has the company been in operation?
- From what country does the company import the equipment?
- To what country does the company export the equipment?
- Does the company re-invoice its exports?
- Does the company use free-trade zone in its import/export business?
- Copy of financial statements
- Other

Answer 17

Risk factors:

- Political person requiring enhanced due diligence—a minister of finance in control of his/her country’s finances
- Country known to be corrupt based on Transparency International rating
- Transaction may have no apparent economic/lawful purpose
Information requirements:

- Because client is a PEP senior management, approval is necessary for the establishment of a business relationship; take reasonable measures to pinpoint the source of wealth and funds and conduct ongoing monitoring of the business relationship.
- Identification documentation
- Evidence of address
- Bankers and professional references
- Copies of salary or wage checks and receipts
- Tax returns
- Other information, depending on country

Other sources of information:

- FATF/NCCT list
- UN sanctions terrorist list
- EU blacklist for country or national blacklist

Questions to ask in addition to normal identification requirements:

- Why did he/she choose your country and bank?
- Salary and other sources of income and wealth. This especially needs to be verified.
- Banking references
- Copy of last tax return and declaration of assets to his/her government, if applicable
- How and from where will the money be transferred to your bank?

Answer 18

The bank should already have all the customer identification records for the client. The records required in this case would be the copy of the draft sold, including the paid copy, and the manner in which it was purchased. It will only be necessary to have sufficient records to reconstruct the paper trail, including who was paid with the bank draft and where it was deposited.

Answer 19

a) This client usually would not raise much concern given the small amount involved. The records about the bank draft would be kept on file along with any form needed to fulfill national requirements. A copy of the person’s identification document would probably be required, along with the purchase documentation.

b) This customer is obviously structuring his/her transactions to avoid the filing of a large transaction report. Structuring large amounts in this fashion should raise a red flag for possible money laundering or other illicit activities, and it should attract the full range of CDD and record keeping. It
would provide a cause for filing a suspicious activity report to the FIU and the report should be kept on file.

**Answer 20**

Banks (deposits):

- High volume of deposits and withdrawals that are inconsistent with the expected turnover
- High use of cash when the business/profession of the client suggests that use of cash should not be the norm
- Numerous small deposits followed by large single withdrawals for no apparent reason
- Large single deposits followed by numerous small withdrawals for no apparent reason
- Use of foreign currency when the business or profession of the client does not indicate a foreign currency source
- Payments out of the account to persons who appear unrelated to the customer’s needs
- Multiple transfers/deposits from other branches of a bank on a periodic basis, followed by large single transfers out of the account
- Others

**Answer 21**

Both the employee and the bank were aiding and abetting money laundering—the former for advising the customers to use a safety deposit box to structure their transactions, bypassing internal bank controls, and the latter for failing to install a satisfactory anti-money laundering program that would detect structuring and unethical actions on the part of an employee.

**Answer 22**

Funds transferred in a lump sum from a known and seemingly reputable U.S. law firm; both the realtor and the bank will benefit from the business transaction. Once the funds are received and the property purchased, none of the parties involved will have a commercial reason to track the turnover of the property and the disposal of sales proceeds. Other institutions, in Utopia or elsewhere, will receive or invest the proceeds from the resale of the property. This scheme is often referred to as a “real estate flip.”

**Answer 23**

1) Utopia *casa de cambio*: This was the first entry point and the place where CDD should be conducted. The funds should not have been wired without first establishing the identity of the customer and the business purpose of the transactions.
2) U.S. broker. The broker should have insisted that the identity of the ordering party be established (not that of the *casa de cambio*), and ascertain if there was a connection between the ordering party and the beneficiary/recipient.

3) The U.S. bank should know if the broker has adequate AML/CFT controls to provide assurance that it knows its clients. The bank should place little or no reliance on the broker if he/she is not covered by the AML/CFT laws. The underlying clients should be identified with certainty or there would be no way to ascertain the legitimacy of transfers to a Caribbean offshore bank account.

4) The Caribbean offshore bank should have questioned the need for an immediate loan against the deposit and verified if there was a connection between the depositor and borrower.

**Answer 24**

Suspicion should not be automatic but does merit a closer look at the account. Comparison with similar video store accounts may be helpful.

**Answer 25**

Why are the deposits more frequent?

**Answer 26**

Yes. Why did “profits” suddenly increase when there was little growth in the past three years? Are there any obvious reasons?

**Answer 27**

This might be a situation where the cash-based business is commingling illicit funds with legitimate bank deposits. The situation calls for further inquiry and research; perhaps a routine visit to the place of business or routine questions about the business operation will clarify the situation. If the change in deposit behavior is unexplained or if explanations/information are unsatisfactory, the bank may consider making a report to the FIU.

**Answer 28**

- A warning, which can include a letter or the use of moral persuasion, for example, in private meetings with the management of an institution
- A monetary fine, the amount being commensurate with the magnitude and frequency of infraction, or dependent on the determination of negligence, recklessness, or willful blindness to the duty to comply
- A prohibition or suspension to hold management or directorship positions in an institution (this can be either temporary or permanent but should be proportionate to the breach)
- A public censure through a statement or advertisement in the media, either electronic or print (naming and shaming strategy)
- Restriction on business activities pending corrective measures, including cease-and-desist orders
- A letter of commitment or memorandum of understanding where the entity or person promises to undertake certain corrective measures
- Cancellation or revocation of authorization to operate, often referred to as the “nuclear option” or the “death penalty”
- Court action

**Answer 29**
- A warning
- Public censure and fine
- Temporary suspension of license to practice or conduct business
- Permanent cancellation of license to practice or conduct business.

**Answer 30**
1) Financial crimes, including money laundering and terrorist financing, damage the reputation of financial systems. This in turn can put the financial condition of those affected at risk and result in losses to the public.
2) Loss of a financial system’s reputation can adversely affect investments, including foreign direct investment.
3) Financial institutions, including banks, can be denied access to the international payment systems, thereby harming the local financial system and economy.
4) Money laundering and terrorist financing attracts criminals to a financial system and allows them to operate freely and promote illegal activities.
5) Money laundering and financing terrorism place the economy and the security of the country at risk.
6) Currencies and interest rates can be distorted by money launderers’ investment practices.
7) Institutions that accept illegal funds cannot rely on those funds as a stable deposit base.
8) Money laundering may distort some sectors and create instability in markets.

**Answer 31**
1) At-risk reputations of a financial institution result in loss of public confidence
2) Legal and financial risks associated with defending against money laundering/financing terrorism charges and investigations, which can also lead to the seizure of correspondent bank accounts abroad
3) Regulatory risk associated with sanctions taken by the supervisory authorities, including the revocation of licenses
4) The termination of various banking facilities
5) Loan losses owing to fewer numbers of high-quality borrowers
6) Deposits placed in a bank by a money launderer are not stable sources of funding
7) Noncompliant institutions can be fined or have their license revoked
8) Institutions can become the property of criminals

Answer 32

The principal agencies that interact and cooperate with financial sector supervisors are generally at the domestic level (answers depend on country and the assigned authority of supervisor):

1) Financial intelligence units—by ensuring that financial institutions have proper control and monitoring systems in place to detect and report suspicious activities to the FIU. This ensures that the quality of reports sent to the FIU is high and avoids overburdening the analytical capacity of the FIU with inadequate reports.
2) Investigative and prosecution authorities—to provide technical and professional advice and support. Financial sector regulators are knowledgeable about the financial sector and its operations and can provide expert advice and testimony for prosecution of ML/FT cases.
3) Regulators often have access to overseas regulators on a formal (e.g., through memoranda of understanding) or informal basis, which is useful for regulators in the investigation of money laundering and financing of terrorism. There are, of course, limits and restrictions on cooperation and on the use of information provided by the regulator, particularly with regard to information subject to confidentiality provisions—e.g., client account information.

Answer 33

ML/FT risks vary across countries and sectors. Each area should assess the degree of risk facing the financial and business sectors and implement the appropriate control mechanisms. Please note that certain sectors are more vulnerable than others to certain stages of the money laundering/financing terrorism processes. Examples of high-risk areas, which could vary from country to country, are

1) banks and trusts;
2) money exchange and remittance businesses (e.g., casas de cambio);
3) real estate;
4) dealers in high-value items (e.g., cars, boats, precious metals and stones, etc.)
5) casinos;
6) high cash-volume businesses (e.g., horse racing, mass entertainment events);
7) other.
Answer 34a

Red flags include:

- Beginning and ending balances are the same. This suggests use of the account as “pass through” with debits equal to credits.
- Multiple large deposits (Jan. 5, 12, 13, 15, 20, 21) followed by single large withdrawals. This pattern could indicate structuring and needs to be compared with the customer profile to check for consistency with the expected use of the account.
- The cash deposits and wire transfers need not be considered suspicious, but they need to be examined for consistency with the client’s profile and expected use of the account.
- Checks were cashed for large amounts.

Answer 34b

This account should probably be reported internally for further analysis. It has too many red flags that require further internal analysis. However, the profile of the customer must be examined before filing a report.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

- Module 1: Effects on Economic Development and International Standards
- Module 2: Legal Requirements to Meet International Standards
- Module 3a: Regulatory and Institutional Requirements for AML/CFT
- Module 3b: Compliance Requirements for Financial Institutions
- Module 4: Building an Effective Financial Intelligence Unit
- Module 5: Domestic (Inter-Agency) and International Cooperation
- Module 6: Combating the Financing of Terrorism
- Module 7: Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
3b

Compliance Requirements for Financial Institutions

Workbook

THE WORLD BANK
3b Compliance Requirements for Financial Institutions

Workbook
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti-Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit
Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation
Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism
Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing
Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments
Module 3b was written by Bob Cooper, HSBC, and Dave Johnson, Barclays, both representing Wolfsberg Group. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by Emiko Todoroki and John McDowell, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Pierre-Laurent Chatain, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations, 2003,” and “Special Recommendations on Terrorist Financing, 2005.”
Module 3b considers Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) from the perspective of a bank or other financial institution and provides the necessary information for employees of such an institution who deal with a wide range of AML/CTF issues. It also provides input for compliance officers of financial institutions. The following is a summary of the module’s content.

1. **Understanding money laundering and terrorist financing**
   1.1 What are the differences between money laundering and terrorist financing?  
   1.2 How is money laundering done?  
   1.3 What is the impact of money laundering and terrorist financing?

2. **Understanding the international framework and controls**
   2.1 United Nations  
   2.2 Financial Action Task Force on Money Laundering (FATF)  
   2.3 Basel Committee on Banking Supervision  
   2.4 The Wolfsberg Group  
   2.5 Local laws and offenses

3. **Key elements of an AML/CFT policy**

4. **Key operational controls of an AML/CFT policy**

5. **Customer due diligence**
   5.1 Verifying the identity of the customer  
   5.2 Verifying the identity of the beneficial owners, directors, and signatories  
   5.3 Obtain and record information on the purpose and nature of the business relationship  
   5.4 Conduct ongoing due diligence on the business
6. Special cases: customer due diligence, risk-based approach  
   6.1 Private banking customers 30  
   6.2 Correspondent banking 31  
   6.3 Non-face-to-face customers 32  
   6.4 Politically exposed persons (PEPs) 33  
   6.5 Other customers who pose a higher risk 33  
   6.6 Intermediaries 34  

7. Monitoring complex, unusual, and large transactions and activities 37  

8. Reporting of suspicious transactions and activities 41  
   8.1 Why is reporting suspicions so important? 41  
   8.2 What you need to know 41  
   8.3 Personal responsibility 42  
   8.4 What information is required? 42  
   8.5 How to deal with the customer after reporting 43  

9. Special screening of customers and wire transfer transactions 45  
   9.1 Customers 45  
   9.2 Wire transfer transactions 46  

10. Record keeping 47  

11. Training and awareness 49  
   11.1 When should training be provided? 50  

12. Sections for compliance officers 51  
   12.1 Risk-based approach to AML controls 51  
   12.2 Risk management 52  
   12.3 External reporting of suspicious transactions and activity (STR/SAR) 53  
   12.4 Cooperation with the authorities 54  
   12.5 Compliance/legal function 55  
   12.6 Audit function 55
This module covers the following Recommendations of the Financial Action Task Force (FATF) on Money Laundering:

- Legal systems: Recommendations 1, 2, and 3
- Measures to be taken by financial institutions and non-financial businesses and professions: Recommendations 5–11, 13, 15, and Special Recommendation VII

The objectives of the module are to help you

- understand the differences between money laundering and terrorist financing;
- understand how and why criminals use banks and other financial institutions to create the appearance of legitimacy;
- know what your responsibilities are with regard to AML/CFT regulations;
- know what key elements of an AML/CFT policy every bank and financial institution should implement;
- know in detail the requirements of customer due diligence (CDD); and
- understand the importance of identifying and reporting suspicious transactions.

At the end of the module you will be able to answer the following questions:

- What is money laundering and terrorist financing and how do they work?
- What controls have been developed at an international level to discourage money laundering and the financing of terrorism?
- What key elements of an AML/CFT policy should every bank and financial institution have in place, irrespective of the local laws?
- What are the key elements of a CDD procedure?
- What are the risk factors that need to be considered when implementing a risk-based approach to AML controls?
- What are the components of a risk-management process?
- How do you identify suspicious transactions/activity?
- How do you report suspicious transactions/activity?
- Why are the monitoring and screening of customer transactions so important?
- What is the importance of record keeping?
- Why is it so important to provide AML training and awareness raising?
- What is the purpose of the audit function?
- Where can you find other sources of information?
1 Understanding money laundering and terrorist financing

How much do you know?
Select the correct answer. Answers will be given at the end of the module.

QUESTION 1. Who might want to launder money?
   a) Drug traffickers
   b) Persons undertaking wire payment fraud
   c) Terrorists
   d) All of the above

QUESTION 2. Money laundering is not a problem for banks because it does not lead to losses, as it does in the case of fraud.
   a) True       b) False

QUESTION 3. Money laundering does not put individual bank employees at risk.
   a) True       b) False

QUESTION 4. The ability to launder the proceeds of criminal activity through the world’s financial systems is vital to the success of criminal operations because:
   a) It is difficult for investigating authorities to prove that laundered money is linked to criminal activity; consequently, criminals can spend their money without attracting unwanted attention.
   b) It allows criminals to avoid paying taxes.
   c) It is safer than keeping cash under the bed.

QUESTION 5. Money is only laundered through banks.
   a) True       b) False
Money laundering is the process criminals use to hide, control, invest, and benefit from the proceeds of their criminal activities. Crimes committed for financial gain (drug trafficking, robbery, theft, blackmail) tend to produce cash. This can pose real problems for criminals because spending large amounts of cash arouses suspicion. Therefore, criminals attempt to create a legitimate background for their money.

Money laundering is also used by persons seeking to fund terrorism. Criminal activities are often the source of terrorists’ funds. It makes sense to hide the link between those who finance terrorism and those who commit terrorist acts.

1.1 **What are the differences between money laundering and terrorist financing?**

Although laundering criminal proceeds and financing terrorism may use similar methods, their objectives are completely different. Look at the two explanations given below:

**A. LAUNDERING CRIMINAL PROCEEDS**

Those who engage in criminal activities for financial benefit usually do so for personal gain—to acquire property, to travel, and so on.

**B. FINANCING OF TERRORISM**

In contrast, persons involved in terrorist activities seek political or social change through intimidation in the following ways:

- **Funding terrorists and terrorist organizations.** Funds for terrorists may originate from legal or illegal activity, which complicates the task of identifying suspicious transactions. Donations from legitimate companies and individuals make up a share of the funds that support terrorists and terrorist organizations. Cash from such crimes as drug trafficking, robbery, extortion, and blackmail may also find its way into terrorist organizations. Fundraising may involve the collection of relatively small amounts of cash that are difficult to detect and trace.

- **Financing of terrorist acts.** At this stage, financial assistance helps terrorists obtain arms and explosives and to meet expenses during their attempt to commit a terrorist act. Examples are the living expenses, first-class airline tickets, and flight-simulator training of the hijackers in the 9/11 terrorist attacks. Subsequent investigations have revealed that the amounts involved were not significant, underscoring the point that terrorist funding can be difficult to detect.
The use of nonprofit organizations as a cover or conduit for the funding of terrorist organizations has been highlighted as a major risk factor by FATF. In addition to providing legitimate funds, some nonprofit organizations fail to apply the strict financial controls of companies that seek to maximize profits. For additional information, see *Combating the Abuse of Nonprofit Organizations* issued by the FATF in October 2002.¹

### 1.2 How is money laundering done?

**Knowledge check**

**QUESTION 6.** Name the three main stages of a money laundering operation. Use the space below for your answer.

---

Let us now read about the stages in some detail.

**Placement**—This is the first stage in separating the illicit funds from their illegal source. Typically, this is the stage when the criminal’s cash enters the financial system, although simply moving the cash away from where the crime took place (perhaps physically transferring the cash from one country to another) is also regarded as part of the placement stage. Following are some examples of placement.

- Depositing cash into an account or into several accounts in different locations
- Paying cash for bank drafts, traveler’s checks, and other value instruments
- Purchasing items of value for cash (such as works of art, antiques, motor vehicles, and so on)
- Commingling criminal cash with legitimate cash in a business account
- Converting cash in one currency into another currency

**Layering**—Once the criminal’s cash is in the financial system, the next stage in the process is designed to hide/confuse the audit trail back to the original deposit and make it difficult to link the funds to criminal activity or to the perpetrator of a predicate offense. This may involve moving the money from one account to another, from one investment to another, or even from one country to another. Following are some examples of layering:

• Buying, then selling, an investment product
• Buying and then surrendering a single-premium insurance contract
• Wiring payments to and from various accounts (personal and corporate) in different jurisdictions
• Engaging in international trade transactions
• Making other types of payment where funds move from one account to another

Integration—This is the third and final stage that completes a money laundering operation. If the criminal has undertaken the previous stages correctly, the money now appears legitimate. The criminal can then freely use the funds for whatever purpose he or she chooses, with minimal risk of detection. This is regarded as the most difficult stage to recognize because the funds appear legitimate. Following are some examples of integration:

• Purchase of property (for personal use or investment)
• Purchase of other high-value items, for example, jewelry, antiques, works of art
• Purchase of legitimate businesses
• Purchase of investments for income
• Any purchase for personal use with a check, credit card, or other payment method

Knowledge check

QUESTION 7. What kinds of criminal activity might lead to money laundering? Provide your answers in the space below.

Question 8. Check the list of possible criminal activities that might be linked to money laundering or terrorist financing. Which one is considered to generate the greatest amount of criminal proceeds in your country?

a) Extortion and kidnapping
b) Blackmail
c) Drug trafficking
d) Robbery
e) Fraud
f) Illegal gambling
g) Smuggling of goods and persons
h) Tax evasion
i) Contributions and donations (terrorist financing)
j) Funds from legitimate business activities (terrorist financing)
QUESTION 9. How much money do you think is laundered each year, throughout the world? Choose the best estimate from the following:

a) US$10,000,000
b) US$100,000,000
c) US$1,000,000,000
d) US$10,000,000,000
e) US$500,000,000,000

HOW MUCH MONEY IS LAUNDERED EACH YEAR?

No one really knows the answer, but publicized figures vary between US$500 billion and US$1.5 trillion annually. To put this figure into context, Wal-Mart, the largest retail company in the world, reported annual net sales of US$345 billion in 2007. The amount of criminally derived funds entering legitimate financial systems each year is almost incalculable.

1.3 What is the impact of money laundering and terrorist financing?

Some of the impacts are listed below:

- Criminal money can have a devastating effect on the economy of an entire country by undermining the competitiveness of legitimate businesses.
- Acts of terrorism also have an impact on the local economy. For example, it was reported that the bombing in Bali, Indonesia, in October 2002 may have cost the local economy more than US$1 billion in lost tourism revenues. The terrorist attacks on New York and Washington, D.C., in September 2001 may have cost the U.S. economy many billions of dollars.
- We should also remember that there are victims to all the crimes from which the proceeds require money laundering: the drug addicts whose lives are ruined by addiction; the vast numbers of people who do not have clean water to drink or sufficient food to eat, while corrupt officials are living exotic lifestyles; and the thousands of people who have been killed or maimed by terrorist attacks around the world.

For more information on the impact of ML/FT on the macro economy, see Module 1.

**Undermining competitiveness: An example**

ABC, Ltd. is a building company financed almost wholly by illegal drug money. Because ABC is awash in cash, its bids for building contracts are often far below the prices of their competitors. This has the effect, over time, of forcing legitimate businesses out of the building industry in a given locale. Once ABC becomes the dominant supplier, it can raise its prices and continue to use the business to launder money.
Now that you have a better understanding of money laundering and its global scope, it will be easy to see why international cooperation is imperative for the successful detection and prevention of money laundering and terrorist financing. The growing integration of the world economy means that individual countries can be affected by faraway events. Developed and developing countries alike stand to benefit from consistency in the application of anti-money laundering controls.

One method of harmonization is a set of international standards that provide a framework of principles that countries are encouraged to adopt and build into their own local legal and regulatory structure. One of the main drivers of this harmonization process was the establishment of the FATF. FATF Recommendations 1, 2, and 3 deal with legal systems and the scope of the criminal offense of money laundering. For more information on FATF Recommendation 1, see Appendix B. For more information on FATF Recommendation 2, see Appendix C. For more information on FATF Recommendation 3, see Appendix D. Other important international organizations and bodies include the United Nations (UN), the World Bank, the International Monetary Fund (IMF), the Council of Europe, the Basel Committee on Banking Supervision, the International Association of Insurance Supervisors (IAIS), the International Organization of Securities Commissions (IOSCO), Interpol, the Egmont Group, the Wolfsberg Group, and other organizations and bodies. For more information on the role of different international and regional organizations and bodies, see Module 1.

2.1 United Nations

The United Nations has adopted several major conventions and protocols related to money laundering and terrorist financing. The UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988) was a precursor to the initial FATF Forty Recommendations (see below), published two years later. The Vienna Convention requires member countries to criminalize money laundering related to drug offenses.

The UN Convention against Transnational Organized Crime (the Palermo Convention, 2000) entered into force on September 29, 2003, and it was ratified by 137 countries. Together with its three protocols this convention provides an international framework for dealing with transnational organized crime,
including money laundering and the confiscation and seizure of the proceeds of organized crime.

The UN Convention against Corruption (the Merida Convention, 2003) was adopted on October 31, 2003, and entered into force on December 14, 2005. As of October 2007 it has been ratified/accessioned by 103 countries. The Convention, *inter alia*, requires countries to criminalize certain corruptive behavior and associated money laundering, as well as imposes an obligation to seize and confiscate funds derived from corruption offenses.

The International Convention for the Suppression of the Financing of Terrorism (the SFT Convention, 1999) requires ratifying states to criminalize terrorism, terrorist organizations, and terrorist acts. Under the convention, it is unlawful for any person to provide, or collect, funds with the intent or knowledge that the funds will be used for acts of terrorism. The convention came into force in 2002.

### 2.2 Financial Action Task Force on Money Laundering

In 1989, the G7 Summit established the FATF. Its mandate was to develop and promote an international response to combat money laundering. This led to the adoption in 1990 of a comprehensive set of anti-money laundering standards, known as the FATF Forty Recommendations. These recommendations cover the broad spectrum of anti-money laundering control—among them legal measures, international cooperation, and a broad range of controls related to financial institutions and other financial sector businesses. There are also eight FATF-style regional bodies (FSRBs) as of March 2009. The original FATF Forty Recommendations were revised in 1996 and 2003. Following the terrorist attacks on the United States in September 2001, Eight Special Recommendations on Terrorist Financing were drafted and published in October 2001. A ninth Special Recommendation was published in October 2004.

When combined with the Nine Special Recommendations, the FATF Forty Recommendations provide a comprehensive framework of measures for countering money laundering and terrorist financing. Most countries now have some level of anti-money laundering controls and have endorsed the FATF Recommendations.

The FATF not only sets standards to combat money laundering and terrorist financing, but it also implements rigorous review mechanisms that aim at ensuring the compliance of countries with the standards. The FATF has devel-

---

2 The FATF Forty Recommendations can be found at [http://www1.oecd.org/fatf/40Recs.htm](http://www1.oecd.org/fatf/40Recs.htm). A list of FATF member countries can be found at [http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html](http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html).

3 The different regional groupings can be found at [http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html#ObserverBodies_and_Organisations](http://www.fatf-gafi.org/document/52/0,2340,en_32250379_32237295_34027188_1_1_1_1,00.html#ObserverBodies_and_Organisations).

4 The FATF Nine Special Recommendations can be found at [http://www1.oecd.org/fatf/SrecdTF_ en.htm](http://www1.oecd.org/fatf/SrecdTF_ en.htm).
oped, together with the IMF and World Bank, a common methodology to assess AML/CFT regimes. This methodology has been adopted by each of the FSRBs and, thus, is used as the universal assessment tool for all jurisdictions. It also plays an important role as a forum for sharing information on money laundering techniques and typologies, as well as reaching out to the public and governments and other parties affected by FATF’s standards: financial institutions and certain designated nonfinancial businesses and professions (DNFBPs).

2.3 Basel Committee on Banking Supervision

Another internationally recognized source of guidance on money laundering is the Basel Committee on Banking Supervision.5 “Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering” was issued in 1988. It stipulated basic ethical principles and encouraged banks to put in place effective procedures to:

- identify customers and understand their business;
- decline suspicious transactions; and
- cooperate with law enforcement agencies.

Two other Basel Committee publications—“Core Principles for Effective Banking Supervision,” published in 1997 and “Core Principles Methodology,” published in 1999—were added to the international framework of anti-money laundering controls.

In October 2001, the Basel Committee published “Customer Due Diligence for Banks,” which provided in-depth guidance on the CDD process. The document covers the following key areas:

- the importance of know-your-customer (KYC) standards for supervisors and banks;
- essential elements of KYC standards;
- the role of supervisors; and
- implementation of KYC standards in a cross-border context.

The elements of the KYC process were further broken down into the following:

- customer acceptance policy,
- customer identification,
- ongoing monitoring of accounts and transactions, and
- risk management.

“Customer Due Diligence for Banks” is recommended reading for banks seeking more detailed information and guidance on this very important aspect of anti-money laundering control.6

5 The home page for the Basel Committee can be found at http://www.bis.org/.
6 “Customer Due Diligence for Banks” can be found at http://www.bis.org/publ/bcbs85.htm.
2.4 The Wolfsberg Group

In October 2000, a number of international private banks (the Wolfsberg Group) agreed on a set of global anti-money laundering guidelines to govern private banking business. Revised in May 2002, these guidelines are regarded as important global guidance for sound business in international private banking. These informative publications by the Wolfsberg Group include the following:

- a statement on the suppression of the financing of terrorism;
- anti-money laundering principles for correspondent banking;
- a statement on monitoring, screening, and searching;
- anti-money laundering principles on private banking (revised version);
- frequently asked questions about beneficial ownership;
- frequently asked questions about politically exposed persons; and
- frequently asked questions about intermediaries.

2.5 Local laws and offenses

In this course, it is not possible to cover in detail the anti-money laundering legislation of every jurisdiction. Local laws have been influenced by the FATF Recommendations and Basel principles mentioned previously, and by other sources—among them the three money laundering directives of the European Union (EU), and the UN, and the Council of Europe Conventions.

However, it is possible to highlight the key aspects that should be included in national legislation. It will then be your responsibility to determine other legal and regulatory requirements to be applied in your jurisdiction.

In the early days of anti-money laundering legislation, criminal activity was often restricted to drug-related offenses. Over the years, the trend has become for legislation to encompass “all crimes,” as in the second and third money laundering directive of the EU, as well as in the 2005 Council of Europe Warsaw Convention on Money Laundering and Financing of Terrorism.

What is a predicate offense?

The FATF has recommended that the following approach be adopted when determining which crimes should be captured by local AML legislation: FATF Recommendation 1 requires countries to apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses. Predicate offenses may be described by reference to all offenses, or a threshold linked either to a category of serious offenses or to the penalty of imprisonment applicable to the predicate offense, or to a list of predicate offenses, or a combination of these approaches. For more information on FATF Recommendation 1 see the Appendix B. It is also discussed in Module 2.
FATF Recommendation 1 refers to the scope of the criminal offense of money laundering. Under the UN Conventions (Vienna Convention, Palermo Convention, and Convention against Corruption) the following three categories of activity constitute the criminal offense of money laundering:

- Conversion or transfer of property
- Concealment or disguise of property
- Acquisition, possession, or use of property

Countries should also criminalize participation in, association with, or conspiracy to commit, attempt to commit and aiding, abetting, facilitating, and counseling the commission of any of the offenses established in accordance with three categories above, unless this is not allowed in accordance with the fundamental legal principles of the country.

For more information on categories of activity making up the criminal offense of money laundering, see Module 2.

In addition, the following illegal activities should also be covered by money laundering legislation:

- failure to report suspicions of money laundering, or to report transactions over a specific threshold; and
- informing, or “tipping off” the subject of a report or investigation that a report has been filed or an investigation launched.

Penalties arising under these and other offenses will vary from one jurisdiction to another. However, it is common for penalties for the above offenses to include a fine, imprisonment, or both. Personal responsibility will be taken into account, along with the legal consequences for the employer. To understand what that means, consider the following scenario.

**Analysis of a scenario**

Read the following hypothetical scenario highlighting personal responsibility and various other AML/CFT issues and then identify the risks to you and your employer. Write your response in the following space. Some suggestions are provided in the subsequent box.

You are the relationship manager for your bank’s corporate accounts. In opening an account for a client (ABC Ltd.) you complete the documentation process required by your bank, but you neglect to confirm details of the beneficial owner because at the time it seemed unimportant. The account operates as you might expect for the first three months. Subsequently, a number of transactions are referred to you because they seem out of line with the company’s stated business activity. These include large wire payments from third parties based in
offshore locations, with the funds being moved swiftly to unrelated third parties in Western Europe. When you ask the account signatory about these transactions, he confirms they are unusual when compared to the previous activity, but he assures you there is nothing to worry about. You take no further action.

Without details about ABC’s beneficial owner, you have no way of knowing if it has been set up for a politically exposed person (PEP) or for a known terrorist group. The former may require greater CDD and an understanding of the source of any funds received. The latter could represent a serious risk to you and your organization, with legal and regulatory repercussions.

Your lack of concern about the unusual activity is dangerous to you and your organization. If the funds prove to be linked to criminal activity, your organization may face penalties or sanctions. You and your bank could be criminally prosecuted for assisting a money laundering operation or failing to report suspicious activity.

Regulatory authorities may impose guidance or rules based on the law. Offenses would occur if an institution were deemed not to have met its obligations under the law or regulations. The penalties from breaches could vary from a formal warning to large fines or penalties, such as the imprisonment of senior management.

**Knowledge check**

**QUESTION 10.** What is the greatest risk to an organization involved in a major, publicized money laundering case?

a) Threat of fine or penalty

b) Loss of clients

c) Damage to reputation

d) Loss of profits
WHY IS DAMAGE TO REPUTATION SO IMPORTANT?

The penalties mentioned previously can all be serious. Multimillion dollar fines have been imposed around the world, but the biggest risk to major financial institutions is damage to reputation. No one will ever know how much business is lost to an organization as a result of publicized involvement (perhaps inadvertent) in a major money laundering case. The short-term effect can often be measured in the fall of a company’s quoted share price, a potential cost to shareholders of millions of dollars.

The following are some examples of penalties that have been imposed on financial institutions:

- Financial Supervisory Authority (FSA) in United Kingdom fines Bank of Ireland £375,000 (September 2004)\(^7\)
- Financial Crimes Enforcement Network (FinCEN) in USA fines Riggs Bank US$25,000,000 (May 2004)\(^8\)
- FSA in United Kingdom Fines Bank of Scotland £1,250,000 (January 2004)\(^9\)
- FSA in United Kingdom fines ABBEY £2,320,000 (December 2003)\(^10\)

\(^8\) http://www.finncen.gov/riggsassessment3.pdf.
Whatever their complexity and scope of operations, financial institutions should be committed to achieving a money laundering deterrence policy that establishes minimum standards and principles of control. Such a commitment provides a clear statement of intent to regulators and law enforcement. In cases where a financial institution has operations in more than one jurisdiction, a global policy should be applied to all business operations. The AML/CFT policy provides an opportunity for senior management to instill a culture of good practice throughout the bank or financial institution.

Knowledge check

**QUESTION 11.** What are the key operational controls a bank or financial institution should introduce to deter money laundering or the financing of terrorism? Consider each of the following cases and write your answers in the space provided.

- A marketing plan to ensure maximum product sales are achieved
- A procedure to ensure that all customers are identified
- An information technology policy ensuring appropriate controls on all computers and communications equipment
- A policy on diversity and equal opportunity
- A policy maintaining customer records and transaction details
- A policy requiring clients to provide additional information about their business so that the financial institution can gauge its likely level of activity
AML/CTF policy usually includes

- a high-level summary of key controls;
- objectives of the policy (some examples include to comply with all legal requirements and to protect the reputation of the institution);
- the scope of the policy (a statement confirming that the AML/CFT policy applies to all areas of the business, including on a global basis);
- waivers and exceptions—procedures for obtaining dispensations from any aspects of the policy should be carefully controlled; and
- operational controls.
Listed below are the key operational controls.

- Statement of responsibility for compliance with AML/CFT policy
- CDD
  - customer identification/verification
  - additional KYC information
  - high-risk customers
  - non-face-to-face business (if applicable)
  - correspondent banking (if applicable)
  - handling of politically exposed persons
- Monitoring for suspicious activity
- Identification of suspicious transactions/activity
- Reporting of suspicious activity
- Cooperation with the authorities
- Recordkeeping
- Screening of transactions and customers
- Training and awareness
- Adoption of risk-management practices and use of a risk-based approach

**Knowledge check**

**Question 12.** Which of the following people in your institution will be responsible for AML/CFT?

a) Senior management  
b) Cashiers  
c) New-accounts staff  
d) Payments staff  
e) Internal audit  
f) Legal and compliance  
g) Training
Responsibilities

An institution’s AML/CFT policy should include a statement that sets out the responsibilities of each of the major categories of employees.

- Senior management: Responsible for ensuring that the various business units within the institution comply with the AML/CFT policy and local law. Responsible for taking appropriate action to resolve issues/failings identified by internal audit or compliance.
- Customer service and other relevant employees: Responsible for following and applying the procedures developed locally to ensure compliance with the AML/CFT policy.
- Internal audit: Responsible for checking whether business units comply with the institution’s internal procedures and, in turn, with the AML/CFT policy. Failings are to be reported to senior management or the board of directors for action, depending upon corporate governance principles of your country.
- Legal and compliance: Responsible for explaining the local legal and regulatory requirements to senior management and providing other advice and guidance on anti-money laundering controls as necessary. May also conduct monitoring or reviews to establish compliance with AML/CFT policy.
- Money laundering compliance officer/reporting officer: Financial institutions are required to appoint a senior management official to be responsible for the implementation of effective AML controls. Often, the money laundering compliance officer/reporting officer is responsible for the process of reporting suspicions to the authorities.
- Training: Responsible for developing/delivering the right level of AML/CTF training and awareness required by the business.

Penalties

Penalties for failing to comply with AML/CFT policies and procedures should be set out in the employees’ terms of employment. In particular, in jurisdictions where employees have a legal obligation to report suspicious transactions/activities, an institution may make failures to report a disciplinary offense, even if there is no action taken by law enforcement for the failure to report.

Customer due diligence

CDD includes the process of identifying, verifying, and recording the identity of prospective customers, as well as additional information about customers’ background, business, and likely level of activity at the institution. It is a major factor in any financial institution’s overall AML control process. The AML policy of the organization should contain a clear statement of the circumstances under which CDD is required. For more information on FATF Recommendation 5, see Appendix E. CDD issues are also discussed extensively in Module 3a.
Knowledge check

**QUESTION 13.** In which of the following situations do you think it would be appropriate for a bank or other financial institution to undertake CDD?

a) When establishing a business relationship that includes the opening of a bank account to allow for receipt and payment of third-party funds.

b) When making a large, single, one-off transaction (such as a sale of traveler’s checks or exchange of foreign currency).

c) When suspicions of money laundering or terrorist financing are raised.

d) All of them.

Let us now see what the FATF requirements are in this area. FATF Recommendation 5 states that CDD should be undertaken when

- establishing a business relationship,
- undertaking occasional (or one-off) transactions over a designated threshold,
- suspecting money laundering or terrorist financing, and
- doubting the veracity or adequacy of details of customer identification previously obtained.

**Monitoring for suspicious activity**

Monitoring of transactions/account activity can be done using a risk-based approach. In certain low-risk business functions, manual monitoring may be appropriate. In higher-risk and higher-volume businesses, it may be necessary to introduce an automated monitoring system to protect the bank. This may be particularly appropriate if customers use many different locations and channels, such as telephone, Internet, and branch banking, to conduct business, as no one person would see the full picture.

**Identification of suspicious transactions/activity**

Financial institutions should ensure that all relevant business functions apply appropriate scrutiny and monitoring of transactions, account activity, and customers to identify unusual or suspicious activity. Staff will need information on the types of activity to watch. These are known as red flags. Further information on red flags is provided in later sections in the module.

International standards require the reporting of suspicious activity, and any financial institution’s AML policy should refer to this reporting obligation of its employees. Even in jurisdictions where there is no requirement to report suspicions, it would be prudent for an institution to have procedures for internal reporting of suspicious activity to a senior person. In this way, an assessment of the risk of continuing to conduct business for any particular customer may be undertaken. Staff will also need to know how to deal with a customer who has
previously undertaken suspicious transactions. Further information is provided later in the module.

**Reporting requirements**

Reporting requirements vary from jurisdiction to jurisdiction. Clearly, you must be aware of, and understand, reporting requirements in your own jurisdiction. There are three main variations of the requirement to report transactions and account activity to the authorities:

- **Cash transaction reporting**—Introduced first in the United States, this mandates the reporting of cash transactions in excess of US$10,000 in the United States. Other jurisdictions also introduced cash transaction reporting requirements, for example, Australia, Canada, India, Slovenia, Serbia, and the Philippines. FATF Recommendation 19 requires countries to only consider the feasibility of implementing a cash transaction reporting system. It leaves, however, the threshold for reporting up to individual countries.

- **Suspicion reporting, subjective test**—This is the most common format for the reporting of suspicious transactions and account or other business activity; it requires employees of relevant financial sectors or businesses to report their suspicions without undue delay. Under the requirement, any employee of a financial institution who becomes suspicious during the course of normal business activities (for example, a cashier accepting a large cash deposit or a clerk processing a large wire payment request) has an obligation to follow internal reporting procedures. Employees who fail to report suspicion under these circumstances are open to prosecution; however, the authorities must be able to prove that the transaction or activity was suspicious.

- **Suspicion reporting, objective test**—This alternative approach to suspicion reporting places the onus on the employee in relevant financial sectors to report circumstances where there are reasonable grounds for suspicion. An employee who does not file a report when there are reasonable grounds to be suspicious is at risk of prosecution by the authorities. The authorities need not prove that the transaction or activity was suspicious, only that there were reasonable grounds for suspicion.

**Cooperation with the authorities**

The institution’s AML policy should also include a general statement of cooperation with local anti-money laundering authorities. However, due regard must be given to the institution’s duty of confidentiality to its customers. In this regard, requests for copies of account statements and other customer information must comply with a country’s laws. (In the event that local law is inconsistent with international standards, competent authorities should consider changing local law, including seeking legislative changes, if necessary.) The authorities may ask a financial institution to maintain a suspect account or relationship to gather further information. Every consideration should be given to the authorities’ request—within the bounds of commercial prudence.
Record keeping
The AML policy should specify how long records will be retained. The minimum length of record keeping required by the FATF Recommendation 10 is five years (or longer if requested by a competent authority, according to the methodology) after either completion of the transaction or termination of the account relationship. The records concerned will include

- customer identification and additional KYC details;
- transaction details;
- business correspondence;
- any other information that would be necessary to trace and identify the beneficiaries of accounts or property, and which could serve as evidence for the prosecution of criminal activity; and
- copies of any suspicion reports that have been filed.

Customer identification details should be retained for the prescribed period after the relationship with the customer ceases. Transaction details need to be retained for the prescribed period from the date of the transaction. FATF Recommendation 10 sets out record-keeping requirements. For more information on FATF Recommendation 10, see Appendix F.

Screening customers and transactions
To comply with sanctions and lists of known or suspected terrorists issued by the UN, each financial institution should consult with a competent authority within its jurisdiction to establish a list of high-risk individuals.

Screening customers
Financial institutions must screen new customer applications as well as their existing customer base. New customer applications need to be screened not only against lists of known or suspected terrorists, but also to identify potential PEPs.

Screening transactions
Financial institutions around the world are expected to be diligent when processing payments (inbound or outbound) on behalf of their customers. A check should be made against lists of known or suspected terrorists as well as other lists issued by the UN. For smaller institutions, a manual check of payments may be all that is required, but larger financial institutions will require an automated solution to identify suspect payments.
Training

The importance of a comprehensive AML/CFT training and awareness program cannot be overstated. Employees in different business functions need to understand how the institution’s policy, procedures, and controls affect them in their day-to-day activities. They also need to know about any specific money laundering risks in their particular area and to be aware of their legal obligations. In some jurisdictions, failure on the part of the institution to provide appropriate training provides the employee with a defense against any charge of failing to report. At the same time, it exposes the institution to additional legal risks. FATF Recommendation 15 refers to programs that financial institutions should develop, including training programs for AML/CFT. For more on FATF Recommendation 15, see Appendix G.

Risk management and risk-based approaches

The institution’s AML/CFT policy should explain how inherent risks will be managed.

Both the FATF and the Basel Committee advocate a risk-based approach to anti-money laundering controls. In jurisdictions where such approaches are either required or permitted, the institution should set out in its AML/CFT policy how the risk-based approach can be implemented throughout the business. This can range from the very basic (for example, additional controls for particular high-risk customers, such as PEPs) to more detailed procedures for business activities of higher risk, such as private banking and correspondent banking (where the Wolfsberg Group has published recommended minimum standards of control), and even complex systems for assessing the risk posed by every customer—linked to a transaction-monitoring system that highlights transactions based on the risk assessment. FATF Recommendation 5 also includes reference to introducing controls on a “risk-sensitive basis.” For more information on FATF Recommendation 5, see Appendix E.
Customer due diligence

Regulators around the world have recognized the importance of ensuring that financial institutions have appropriate procedures in place to know their customers. Verifying the identity of customers, beneficial owners, and other relevant parties to an account, and having sufficient information about those customers, are the cornerstone of any institution’s anti-money laundering controls. FATF Recommendation 5 refers to the CDD measures that financial institutions should take to prevent money laundering and terrorist financing. Some of the key elements of the process relevant to particular types of accounts are:

a) Verification requirements for personal accounts:

- Identity of customer
- Date of birth
- Contact details (address, telephone)
- Employment details
- Likely level of activity (salary, plus any other anticipated payments)
- Why the customer wants the account
- What products and services the customer is interested in

b) Requirements for nonpersonal accounts (private limited company):

- Verifying that the company exists (copy of certificate of incorporation or other evidence that the company has been legally incorporated)
- Verifying the identity of signatories/directors
- Verifying the identify of major shareholders/beneficial owners/major investors
- Understanding the type of business conducted
- Contact details (address, telephone, fax)
- Major customers
- Major suppliers
- Likely level of activity and format (cash, checks, wires)
- Copy of business plan
- Copy of annual audited accounts from previous year
- A determination of whether the client is regulated and, if so, by what entity
- A determination of whether the client is required to observe AML/CFT controls
The above is an example of CDD requirements for a private limited company. For other types of business (public limited companies, trusts, partnerships, sole traders, and agents or intermediaries), other information may be required. In general terms, an institution should never establish a business relationship until all relevant parties have been subjected to verification of identity, and an appropriate level of KYC information has been obtained.

Knowledge check

ABC, Ltd., a building company, is seeking a formal banking relationship with your institution. The directors are Mr. Smith, Mr. Jones, and Mr. Simpson. All three have been subjected to the identity-verification procedure. You have obtained all necessary documentation and information concerning ABC, Ltd. and its business activities. The major shareholders are Mr. Smith, Mr. Jones, and DEF, Ltd.

QUESTION 14. Do you need to perform further due diligence?

a) True  
b) False

QUESTION 15. DEF, Ltd. has Mr. Jones, Mr. Smith, and Mr. Simpson as its directors. However, all of the shares in DEF, Ltd. are owned by GHK, Ltd. Do you need to undertaken further due diligence?

a) True  
b) False

QUESTION 16. GHK, Ltd. is controlled by Mr. Smith, Mr. Jones, and Mr. Simpson as directors, but all the shares are owned by Mr. Burns. Do you need to undertake further due diligence?

a) True  
b) False

Knowledge check

XYZ, Ltd. is a computer company seeking a banking relationship with your institution. The directors are Mr. Smithers, Mr. Hutz, and Mrs. Lovejoy. However, 95 percent of the shares are owned by Mrs. Lovejoy. Again you have all the necessary documentation for the company and all the directors have been identified.

QUESTION 17. Do you need to undertake any further due diligence?

a) True  
b) False
5.1 Verifying the identity of the customer

Depending on whether your customer is a private individual or a business, the process for verifying the identity of relevant parties to an account or other relationship can become very complicated. For nonpersonal relationships, it is important that all persons who are in a position to exercise control or influence over the business should be subject to verification. This will include signatories, directors, and major shareholders. Depending on the product or service being requested, a risk-based approach can be applied to this verification process.

A financial institution should perform enhanced due diligence for higher-risk categories of customers, business relationships, and transactions. Examples of such higher-risk categories include

- nonresidents;
- private banking;
- legal persons or arrangements, such as trusts or other personal asset holding vehicles; and
- companies that have nominee shareholders or bearer form shares.

The types of enhanced due diligence measures for high-risk categories could include those set out in FATF Recommendation 6. For more information on Recommendation 6, please see Appendix I. See also Section 6 of this Module.

A) Personal customers

The identity of any individual should be verified by reference to an original document that is difficult to alter, amend, or forge. A valid passport is considered to be one of the most reliable documents, but a combination of other documents may convince the institution that they know the person with whom they are dealing. File copies of the passport should be made so as to retain access to the following information:

- Date of issue
- Place of issue
- Number
- Name of holder
- Country

Other identity verification documentation

Driver’s license, birth certificate, employer identity card, national insurance/health card, national identity card, credit cards, and other cards issued by reputable financial institutions. Please remember that it is the institution’s responsibility to comply with local requirements when deciding which documents will be acceptable.
Prospective customers who do not have any of the recognized identification documents, especially if the lack of such documents is not consistent with their background or business activities (for example, a frequent overseas traveler who can produce no passport), should be a matter of great concern for a bank. Identification and verification should be provided before opening an account or transacting any business for such an individual. In the event that a customer cannot present the required identification, internal policy should specify what staff should do. Generally, staff should decline access to the account and any transactions until adequate identification can be provided.

B) Nonpersonal Customers

It is important to obtain sufficient documentation to prove or establish that the business exists. For limited company relationships this would normally be achieved by obtaining a copy of the certificate of incorporation or a copy of an extract of an official register showing that the company name has been properly registered.

To help protect the organization against fraud as well as money laundering, it is also important to establish that those persons who represent themselves, or act on behalf of the company, are properly authorized to do so. This will include obtaining some form of evidence as to the names of the appointed company secretary, and directors. Other examples of nonpersonal customers and the suggested verification documents/process are the following:

- **Trust arrangement**: verify by obtaining a copy of the trust deed
- **Partnership**: verify by obtaining a copy of the partnership agreement
- **Public limited company**: verify by confirming the listing on a recognized or approved exchange
- **Financial institution**: verify by obtaining a copy of banking license, or check with home country central bank
- **Charities**: verify by confirming that the charity is registered and listed with appropriate authority

All documents obtained, should be accurately recorded so the bank will have this information for law enforcement and supervisory purposes, as well as any future internal compliance audits.

Business descriptions that include phrases like import/export, general trading, investments, business services, and so on, need further investigation to make sure the bank understands exactly what type of business is involved and the type of transactions that will be presented.
5.2 Verifying the identity of the beneficial owners, directors, and signatories

Let us try to understand the ownership and control structure of the customer’s accounts.

Who are the “beneficial owners”?

According to the FATF definition, a “beneficial owner” refers to the natural person who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

This would mean, for example, any person who owns a significant proportion of shares in the business (perhaps more than 20 percent) or is able to exercise control in other way, for example, as a result of a major investment of capital in the business. Where shares are held by other companies, the underlying owners of those companies need to be investigated.

Who are the “signatories”?

Signatories: A signatory to an account is able to exercise control or authority over funds passing through the account. If the account has many signatories, a risk-based approach should be adopted to determine the number of signatories whose identity must be verified to comply with the identity-verification requirement.

Who are the “directors”?

Directors: A director exercises control over the business—and thus over funds passing through the account. Consideration should be given to verifying the identity of one or more directors, depending on the circumstances. Detailed information about the directors and company secretaries can usually be confirmed by searching the records of the company registrar.

Companies that issue bearer shares represent a higher risk from an AML/CFT perspective. The true owners of the company will be almost impossible to confirm because ownership passes with the physical transfer of share certificates. Where shares are registered to other companies, the beneficial owner(s) of those companies need to be recorded.

When a financial institution is not able to identify and verify the beneficial owners of the companies, staff should decline access to the account and any transactions until adequate identification can be provided and such information is verified.
5.3 **Obtain and record information on the purpose and nature of the business relationship**

How is the account to be used (cash, wires, checks), and what is the likely level of activity?

> It is important to verify at the beginning of any business relationship the likely level of activity and the expected types of transaction. With this information, an institution can do two things. First, it can consider whether the information provided is realistic in terms of the business. Second, it gives the institution a benchmark against which it will be able to measure activity.

Where a new business customer advises that the initial activity through the account will be significant (greater than US$1 million, for example), the bank should understand the reasons behind this belief and be satisfied with the projected source of funds.

5.4 **Conduct ongoing due diligence on the business**

Ongoing due diligence will include reviewing transactions to ensure that they are consistent with the available information about the business, particularly in relation to sources of funds. Ongoing due diligence enables the institution to identify suspicious activity. Understanding the facts behind significant transactions adds to the overall knowledge about any particular customer.

Where a new business customer significantly exceeds the projected activity estimated when the relationship was established, the bank should understand the source of this increase and verify source(s) of the funds received.
While not directed at specific customers or products or services, the FATF has issued general guidance on the risk-based approach to AML/CFT to assist both authorities and the private sector to

- support the development of a common understanding of what the risk-based approach involves;
- outline the high-level principles involved in applying the risk-based approach; and
- indicate good public and private sector practice in the design and implementation of an effective risk-based approach.11

Some of the customers of financial institutions may carry a “higher risk” than others. The riskiness of customers may depend upon geographical location, customer type, or the product of service being offered to the customer. Some of these issues have been addressed in the “Risk-based approach to AML controls” section in the “Sections Identified for Compliance Officers.”

6.1 Private banking customers

What is private banking?

Private banking is a business activity that represents a higher risk of money laundering than many other financial activities. Dealings with wealthier clients will naturally lead to higher levels of funds being received (and paid out). The additional CDD for these types of customers should focus on the source of the wealth and the location of the funds to be brought into the banking relationship.

---

What are sources of wealth?

Understanding the source of wealth, particularly for high-net-worth clients, is an important element of the AML control process. This means obtaining (and in some circumstances verifying and validating) the background of the declared wealth of the individual concerned. Vague explanations (“family, property, business”) should be subject to further questioning until a full and satisfactory verification is obtained. For instance, if the sale of a business is given as an explanation, details relating to the name of the business, the date started, date sold, selling price, and buyer’s name should be requested.

What are sources of funds?

The source of funds refers to the location of the funds that are to be received into the account—both initially and in the future. These may include salary bonuses, other earned income, interest, and dividend payments. Where funds are to be received from an unrelated third party, further questions should be asked until the background to the transaction is fully understood.

6.2 Correspondent banking

Where a financial institution (correspondent bank) provides banking services to other banks (the respondent banks), this exposes the correspondent bank to additional money laundering risks, particularly where the respondent bank has no physical presence in the jurisdiction where the relationship is established. FATF Recommendation 7 refers to additional measures financial institutions should take for cross-border correspondent banking and similar relationships. For more information on FATF Recommendation 7, see Appendix H.

It is important that any financial institution offering correspondent banking services have its own CDD process in place to help mitigate the additional risks. You may need to examine that process or undertake routine checks to ensure that it is being followed. A correspondent bank might consider adopting a risk-based approach in its CDD process, based on where the respondent bank is registered or located. Listed below are some examples for banks based in a jurisdiction that:

- is known to have a strong AML/CFT regime—generally present a lower risk;
- does not participate in the FATF or a FSRB—generally present a medium risk; and
- does not cooperate with the FATF or a FSRB—generally present a higher risk.
Depending on where the respondent bank is located, the following aspects of due diligence need to be considered:

- respondent bank’s management and control;
- bank license;
- level of supervision and regulation in the home country;
- major activities and services provided to clients;
- location and organization;
- details of AML procedures and controls, including KYC procedures; and
- details of any third-party entities that will use the correspondent banking services (including other financial institutions)

High-risk situations

Requests for correspondent banking services received from an institution incorporated in a jurisdiction in which it has no physical presence (shell bank12), should be declined. Shell banks can be easily purchased by criminals and used for money laundering.

A correspondent bank also needs to realize that some respondent banks allow their accounts to be used by third parties to transact business on their own behalf. For example, in a “payable-through account” the respondent bank allows its customers to draw checks on the respondent bank’s account with a correspondent bank. In many such cases the respondent bank is offering checking services to its customers in a currency other than their local currency.

What is the main risk of this arrangement?

A “payable-through account” indicates that the correspondent bank is closely involved with the customers of its client, the respondent bank, without having any KYC information on those customers. There is a significant risk of money laundering under this type of arrangement.

6.3 Non-face-to-face customers

More and more financial institutions are providing financial services without a face-to-face meeting with the customer. In these situations, it is important that the level and detail of CDD should be at least as robust as that undertaken for customers who are interviewed personally by bank staff. Financial institutions should contact their respective supervisor for methods to achieve adequate

---

12 Shell bank means a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group.
CDD for such customers. As part of this effort, financial institutions should be aware of the various forms of electronic information services that are available, particularly when using them as a means of verifying identity.

6.4 Politically exposed persons (PEPs)

Who is a PEP?

According to the FATF, PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, such as heads of state or of government; senior politicians and party officials; senior executive, judicial, or military officials; and senior executives of state-owned corporations. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. This definition does not cover middle ranking or more junior individuals.

Recent years have seen some high-profile cases in which politically connected people, through their positions of power or influence, have benefited from the proceeds of corruption. As customers, PEPs should be subject to enhanced due diligence, which should include full details of funds and validation of their sources. It is also important to have a good understanding of the likely level of activity in the account and the form it will take (for example, cash, wire payments, checks). PEPs should also be subject to a more senior level of approval than would otherwise be required for standard customers. FATF Recommendation 6 discusses the enhanced due diligence that should be applied to PEPs. For more information on FATF Recommendation 6, see Appendix I.

6.5 Other customers who pose a higher risk

Financial institutions also need to be mindful of the increased risks of dealing with other types of customers and businesses that may be targeted by criminals with funds to launder—among them casinos, money service businesses, and dealers in precious metals/stones. There are also some types of business that represent higher risk simply by the very nature of their business activities, such as manufacturers and dealers in arms and other military equipment. Relationships with these types of businesses should be subject to approval at a more senior level than would normally be required.

These types of customers need to be subject to more regular reviews, particularly against the KYC information held by the institution and the activity in the account.

**Senior management approval**

Persons whose responsibilities include approving applications from customers of the types mentioned above will need to have a full appreciation of the potential risks associated with each type of customer. A financial institution can sustain
severe damage to its reputation if it is subsequently reported that the institution has provided financial services to a person facing charges of corruption or theft of public funds.

If a customer is reported in the local or international press as being involved, even indirectly, in potential corruption or bribery, it is important to review account activity even more carefully and frequently so the bank is satisfied that it is handling only legitimate transactions.

### 6.6 Intermediaries

There are many ways for customers to remain hidden from the banks and other financial institutions that are providing them products and services. Therefore, it is important to look beyond those who represent the client and verify the identity of the true beneficial owner. There can also be situations in which clients deal directly with a bank or other financial institution, but do not act on their own behalf. It is not easy to identify such situations, particularly if the client gives no indication of acting for another. This is why it is important to know whether a customer is acting on behalf of another; an affirmative declaration can be useful in this regard. FATF Recommendation 9 deals with relations between financial institutions and intermediaries or other third parties that are used to performing part of the CDD process on behalf of a financial institution. For more information on FATF Recommendation 9, see Appendix J.

A bank may find itself dealing with intermediaries for underlying clients under a variety of circumstances. Consider the following scenarios:

- The intermediary approaches the bank on behalf of a third party and introduces the customer to the bank. The bank then deals directly with the customer in the future, and the intermediary withdraws from the scene. The bank has a responsibility to exercise due diligence with respect to its customer, but not the intermediary. In some instances, intermediaries receive a fee for introducing the business to the bank.

- The intermediary continues to act on behalf of the customer. In these circumstances, both the intermediary and the underlying client are subject to appropriate CDD. The bank will need to consider the extent to which it may rely on due diligence undertaken by the intermediary to verify the underlying client. If the intermediary is based in a jurisdiction that has inadequate AML/CFT controls, the bank must assess the degree of reliability of the intermediary, and if appropriate, undertake additional CDD.

- The intermediary acts on behalf of several clients. Transactions for these clients are made through a client account or similar arrangement. In such circumstances, the intermediary is the client and so must be subject to due diligence. Additionally, depending on the regulatory status of the intermediary, the bank may need to undertake CDD on each underlying client. Examples are fund managers, independent financial advisers, and lawyers.
Let us consider a few examples.

**Analysis of scenarios**

**Scenario 1**
ABC, Ltd. is a professional firm of intermediaries who conduct business on behalf of multiple clients. There is no AML/CFT legislation in the jurisdiction in which ABC, Ltd. operates. Separate accounts have been established for customers, Mr. Smith, Mrs. Jones, Mr. Johnson, Mrs. Adams, Mr. Collins, and Mr. Jackson. The clients have signed a power of attorney to enable ABC, Ltd. to make transactions on their behalf.

**QUESTION 18.** Select the entities that require customer identification. Then check your answer.

a) ABC, Ltd. only
b) The signatories, directors, and beneficial owners of ABC, Ltd.
c) Smith, Jones, Johnson, Adams, Collins, and Jackson
d) All of the above

**Scenario 2**
ABC, Ltd. is a regulated financial intermediary and adviser. It requires client and office accounts to do business. ABC provides financial advice to underlying clients; related transactions are conducted through the client account. The jurisdiction in which ABC operates has robust AML/CFT laws and regulations. A new client, Mr. Addis, is seeking to invest US$500,000.

**QUESTION 19.** Select the entities that require customer identification and then check your answer.

a) ABC, Ltd. only
b) The signatories, directors, and beneficial owners of ABC, Ltd.
c) Mr. Addis only
d) All of the above
e) Only (a) and (b)
QUESTION 20. What other high-risk situations can you think of? Make a list and then compare your list to the answer provided at the end of the workbook.
AML/CFT legislation should require staff at financial institutions to report suspicious transactions and/or activities. This is a requirement of FATF Recommendation 13 (see Appendix N) and is discussed in section 8. This obligation must not be understated or underestimated.

Before this requirement can be accomplished, financial institutions must monitor accounts for unusual transactions or activities. Computer systems are now being used to flag suspicious activity, but these can be resource intensive, both in terms of cost and of the staff time required to review outputs. In cases where larger banks have installed electronic monitoring systems, the installation does not reduce or remove the obligation of employees to report their suspicions. Smaller financial institutions will still rely heavily on their employees to identify and report suspicious transactions/activity. FATF Recommendation 11 refers to complex, unusual, and large transactions, as well as transactions that have no apparent economic or lawful purpose. For more information on FATF Recommendation 11, see Appendix K.

### Analysis of scenarios

After monitoring accounts for unusual transactions or activities, consider whether the circumstances presented in the following scenarios are suspicious or not.

**Scenario 1**

Mr. Hibbard has maintained an account with your bank for the past five years. Your bank records show him to be an office worker.

**QUESTION 21.** Mr. Hibbard does not usually make large cash deposits to his account. Today, he wants to make a large deposit of cash in a single transaction. When questioned, he says that the funds are from the sale of his car.

a) Suspicious

b) Not suspicious
QUESTION 22. Mr. Hibbard deposits several small amounts of cash over a period of months. They add up to a significant amount.

a) Suspicious
b) Not suspicious

QUESTION 23. Mr. Hibbard requests that a large wire payment be sent to a third party in another jurisdiction. When questioned about the transaction he becomes angry, declaring that what he does with his money is his business. When you look at the account history, you see that the funds in question were credited to his account through a wire payment from another person in the same country as the payment he is now sending.

a) Suspicious
b) Not suspicious

QUESTION 24. Mr. Hibbard asks for investment advice, as he now has a large credit balance on his account. When checking the account you see the source of these funds appears to be a single check paid into his account the week before. The check came from his employer.

a) Suspicious
b) Not suspicious

Following are questions that could be asked when dealing with scenario 1:

- I notice that your account has been more active recently, Mr. Hibbard. Could you tell me more about the background of these transactions?
- I notice that you have received a large payment into your account recently. Can you tell me more about this?
- Can you tell why you need to make this payment, as I may be able to suggest a more effective way for you to do so?
- I notice that you have received a large payment from your employer; can you tell me more about this?

Scenario 2

XYZ, Ltd. has just opened a new account with your bank. All the necessary company documentation has been obtained, and the directors, signatories, and beneficial owners have been identified. The business activity has been given as import and export of mobile telephones.

Consider whether the circumstances presented in the following scenarios are suspicious or not.
QUESTION 25. You see from the company documentation that the company is registered in the British Virgin Islands.
   a) Suspicious
   b) Not suspicious

QUESTION 26. In the first month of operation, there are numerous wire payments into and out of the account. The totals are far in excess of the likely level of turnover indicated to the bank when the account was opened.
   a) Suspicious
   b) Not suspicious

QUESTION 27. There are payments that appear to be from other companies involved in the telecommunications business, as well as substantial amounts from individuals.
   a) Suspicious
   b) Not suspicious

QUESTION 28. The business has requested a letter of credit on a contract established with another mobile telephone company in a different jurisdiction.
   a) Suspicious
   b) Not suspicious

Causes for concern
The following are examples of situations that should give cause for concern in the absence of rational explanations from the customer.

Banking
- Large cash deposits
- A series of small cash deposits
- Cash payments to accounts of unrelated third parties
- Cash deposits received from unrelated third parties
- Deposits involving large numbers of traveler’s checks
- Deposits involving large numbers of money orders
- Regular deposits of checks drawn on casinos and other gaming establishments
- Significant increases in cash deposits (business customers)
- Payment and receipt of unrelated third-party funds transfers
- Payment and receipt of cross-border funds transfers
- Significant changes in account balance or transaction activity

—continued
Customer behavior

- Customer does not have appropriate identification documents.
- Transactions are out of line for customer's apparent means, business, or background.
- Customer appears nervous for no apparent reason.
- Customer advises no other banking facilities are used, when the age or experience of the customer would suggest this is unlikely.
- Customer shows no concern about interest, fees, and other charges.
- Customer appears overly concerned about secrecy of financial arrangements.

Investments

- Customer is prepared to invest without understanding key features of the product concerned.
- Customer appears unconcerned about risk.
- Customer seeks to redeem or cancel medium- to long-term investment shortly after making it.
- Customer is unconcerned about loss arising from cancellation or sale of investment.
- Customer seeks proceeds of investment to be paid to unknown third party.
- Customer cancels large, single-premium investment without reasonable explanation.
- Customer expresses preference for bearer investments without adequate explanation.

Insurance

- Policy holder overpays premium.
- Policy holder cancels single-premium policy.
- Policy holder makes a series of claims under a policy, with the total amount claimed remaining below the level of the premiums paid.
As discussed earlier in the module, reporting requirements vary from jurisdiction to jurisdiction. Most AML/CFT legislation includes a requirement that staff in the financial sector report suspicious transactions or activity. This obligation must not be understated.

Even in jurisdictions where there is no requirement to report suspicions, it is prudent for a bank to have procedures that require employees to report suspicious activity internally to a senior person. In this way, an assessment of the risk of continuing to conduct business with any particular customer can be made.

8.1 Why is reporting suspicions so important?
The importance of reporting your suspicions cannot be overstated:

- It is a legal requirement in many countries. Failure to do so could result in money penalties or criminal prosecutions of individuals.
- It helps protect the reputation of your bank.
- It helps to protect you from unfounded allegations of assisting criminals, including terrorists.
- It helps the authorities investigate money laundering, terrorist financing, and other crimes.

8.2 What you need to know
As a member of staff you will need to know about the following key requirements:

- Your personal responsibilities
- How to identify suspicious activity
- What information is required
- How to report
- How to deal with the customer after reporting

---

13 In this section we shall discuss the reporting requirements relevant to the operational staff of a financial institution. We have discussed the issues related to reporting of STR/SAR to the FIU in the “External reporting of suspicious transactions or activity (STR/SAR)” section of the module (identified for compliance officers).
8.3 Personal responsibility

Countries have different requirements related to the filing of suspicious transaction/activity reports (STRs/SARs). In all cases, however, the essential factor is that when an employee becomes suspicious of a customer, transaction, or series of transactions, a report must be submitted. Do not assume that someone else will submit a report because you may be held personally responsible if you were the one who processed the transaction or had other dealings with the customer that caused you (or should have caused you) to become suspicious. Some countries set a minimum threshold for the reporting of suspicious activity, although this is part of the international standards, which have no minimum.

8.4 What information is required?

Your bank should have a standard report form available to use to meet your personal responsibilities. It may be a paper or electronic form. If you do not know where to obtain the form, ask your line manager after you have completed this training module.

The form used in your bank should clearly set out the information required to enable you to submit a useful report. Other banks may have a looser approach. Whichever method is used in your organization, the “five Vs” will help you complete a STR/SAR with the correct details.

Who is the customer whose account or investment has raised your suspicions? You should include:

- details of their employment (or business activity);
- relationship with your business area; and
- date relationship was established.

What happened to make you suspicious?

- Describe the transactions, activity, or behavior that you think is suspicious.
- Note the type of payment involved (cash, wires, checks).

When did the suspicious activity occur?

- If a single transaction, what was the date?
- If a pattern of activity, when did it start?
- Describe the activity during the period in question—for example, 15 incoming wires, all from the same bank or remitter.
- Highlight when the activity was first identified.

Where did the suspicious activity take place?

- Identify the branch/department or other locations.
- Identify all the account numbers and types of account used.
- Identify other financial institutions involved as remitters or beneficiaries of funds.
Why do you think this activity is suspicious?

8.5 How to deal with the customer after reporting

Remember the following key points.

- Continue to deal with the customer in the usual manner.
- Do not alert the customer that you have reported your suspicion—to do so may constitute “tipping off,” an offense.
- Refer or report any future suspicious activity.
- Refer any legal orders received from the authorities.
- In some jurisdictions, it may be necessary to obtain consent before processing transactions that are regarded as suspicious—know your local law.
- If you have doubts or concerns, speak with your line manager or compliance officer.
- In some jurisdictions (for example in Switzerland) you may be required to freeze the account until the authorities have investigated. Your local money laundering reporting office will be able to provide you with further advice.
- Make sure you receive an acknowledgment of receipt of your report.

Exercise

Consider the following scenario:

Tavistick Trading, Ltd. is a customer of your bank. In addition to payments to recognized suppliers and from recognized customers, there are a number of wire payments from a single remitter (Celestial Enterprises, through a bank in Panama) with matching payments to a single beneficiary (Mountain Alliance Foundation, through a bank in Liechtenstein). You have the details of payments received and made over the last six months that total more than US$7 million.

**QUESTION 29.** Which of the following pieces of information would you include in your report?

a) Registered company of British Virgin Islands’ number 78809910
b) Registered address: The Plantation House, Sugar Mill Cove, Tortola, BVI
c) Date of incorporation January 31, YYYY
d) Business address: 123, Any Street, Your Town, and Country
e) Directors: J. Evans and E. Jones
f) Signatories: R. Smith and S. Rogers
g) Shares held by: J. Evans, R. Smith, and T. Baker
h) Identification details held for directors and signatories, but not for T. Baker
i) Nature of business activity: Wholesaler and retailer of toys for children aged 3–11
j) Main suppliers: Mattel, Lego, Disney, Triang
k) Main customers: major retail stores in London, New York, Paris
l) Projected activity when account opened three years ago was given as US$500,000
m) Last set of annual accounts held was dated 18 months ago
n) Copy of business plan provided when account was opened
o) Past six months of bank statements showing details of all account activity
p) Turnover in past six months: US$8,540,000
Following the events of September 11, one of the major impacts on the financial system was the issuance and distribution of lists of suspected terrorist names by various authorities around the world. In many jurisdictions around the world, it is an offense to provide financial services to anyone suspected of being involved in terrorist-related activity. Banks and other financial institutions need to consider how best they can protect their businesses by screening any high-risk customers and transactions.

9.1 Customers

FATF Special Recommendation III requires countries to freeze funds of terrorists, those who finance terrorism, and terrorist organizations. The purpose of this requirement is to prevent use of their banking and financial systems by terrorists or terrorist organizations. Countries differ in how they implement sanctions against specific individuals and entities. All UN member countries are required to adhere to the UN Security Council designation lists and relevant decrees either by specific laws or regulations or simply by circulating lists to institutions for possible action. For more information on FATF Special Recommendation III, see Appendix O.

In addition, some countries have adopted laws or regulations that allow them to designate individuals and entities (other than those on UN lists) as terrorists and to impose targeted sanctions against those individuals and entities.

Financial institutions should keep themselves well-informed of the sanctioning systems imposed by applicable laws and regulations and make sure that they keep up to date with the lists circulated or published by the competent authorities in their own jurisdiction. In this regard, banking authorities should give unambiguous instructions as to what a bank should do when it finds a client’s or potential client’s name/organization on a terrorist list. For example, because the goal is to freeze terrorist assets to prevent a terrorist act, if a person on a designated terrorist list seeks to open an account, it might be appropriate for the bank to open the account, but immediately freeze the funds deposited and report the incident to authorities. On the other hand, there should be a complete prohibition on execution of any outgoing transaction (i.e., transfer or withdrawal) by a designated terrorist or terrorist organization; but, again, the bank should immediately freeze the account and notify authorities. Finally,
banks should also have their own specific procedures in place for staff to follow in these circumstances, which are consistent with national laws, regulations, or relevant decrees.

9.2 Wire transfer transactions

FATF Special Recommendation VII contains specific requirements for wire transfers. Among these is a provision for countries to ensure that financial institutions (including money remitters) conduct enhanced security and monitoring for suspicious wire transfers that do not contain complete originator information (name, address, and account number).

For banks with a relatively small number of inward/outward wire transfers, this critical task could be performed manually. For medium-size and larger organizations, an automated name-matching system to compare remitter and beneficiary names and originator information on each wire transfer instruction may be necessary. For more information on FATF Special Recommendation VII, see Appendix L.
The importance of record keeping cannot be overemphasized. By maintaining appropriate records, banks and other financial institutions help provide an audit trail of funds, and thus assist the authorities in tracing any suspect funds back to their original criminal source. It is also important that any records held are easily retrievable without undue delay (refer to news item below). It is important that any records retained are complete, accurate, and easily retrieved in the event of any subsequent enquiry/investigation. FATF Recommendation 10 describes the record-keeping requirements of financial institutions. For more information on FATF Recommendation 10, see Appendix F.

News item
In the United Kingdom, the Bank of Scotland was fined £1.25m by the Financial Services Authority for its failure to maintain appropriate records. In this case the bank had identified its customers but had difficulty in producing the records when requested to do so.

Knowledge check
QUESTION 30. What is the international standard for retention of bank records related to transactions on behalf of their customers?
  a) At least 1 year
  b) At least 3 years
  c) At least 5 years
  d) At least 10 years
QUESTION 31. What information do you think would be covered by these requirements?

a) Customer identification details
b) Additional KYC information obtained during the lifetime of the relationship
c) Business correspondence
d) Any credit or debit transaction
e) Details of previous addresses
f) Details of internal suspicious transaction reports
g) Details of any external report
h) Details of marketing letters sent to the customer
The communication of the policy, procedures, and other controls to prevent money laundering and financing of terrorism, and training in how to apply those procedures, support all other AML/CFT strategies. Staff who are meeting with customers or handling transactions or instructions will be the bank’s strongest defense against money laundering and financing of terrorism—or its weakest link. Thus, the success of the bank’s AML/CFT strategy is supported by the effectiveness of its training and how well the obligations are communicated to employees. This is the foundation upon which the reputation of the institution can be protected or destroyed.

### Which staff should receive regular AML/CFT training?

- **Cashiers**—They are very important; they may spot suspicious deposits or withdrawals.
- **Account opening staff**—They are very important, as they are the first line of defense against any potential money laundering and financing of terrorism.
- **Staff dealing with foreign exchange**—Foreign-exchange staff are very important, as they may identify suspicious activity when handling currency transactions for the customer.
- **Investments staff**—Investment staff are very important because investments are often used by money launderers, typically in the layering stage.
- **Insurance staff**—Staff handling insurance products are very important because insurance contracts can be used by money launderers, typically as part of the layering stage.
- **Line management**—Line managers are very important, especially as sources of information and guidance for their subordinates.
- **Senior management**—Senior managers are very important if they are to understand the risks to themselves and to the reputation of the institution that might arise from even inadvertent involvement in a money laundering or a terrorist financing scheme.
- **Temporary/contract staff**—Temporary employees should have an understanding of the key issues and how they affect the business area in which they are working.
- **Money laundering reporting officer and support staff**—Even employees who process SARs and STRs need to be made aware of new schemes and tactics used by money launderers or those who finance terrorism. Such employees are often contacted for advice by others in the organization.

—continued
When should training be provided?

There are two main strategic approaches for AML/CFT training and awareness. First, new employees should receive basic training before they interact with the customers or handle transactions so that they do not expose the organization to increased risk. This training may need to be more detailed or specific depending on the business function in which the new entrant is employed.

Second, all relevant staff should receive refresher training on a regular basis. The timing of this training can vary from very frequent (monthly or quarterly specific reminders in high-risk areas) to a more generic content that is delivered on a regular basis (once every year or two years to all other staff). Again, this is an area where a risk-based approach can be adopted.

The content and timing of any AML/CFT training or awareness program is one area where a bank or other financial institution can adopt a risk-based approach. Those business areas considered at greatest threat from suspicious activity should receive more frequent training.

What kind of information should be covered in an AML/CFT training or awareness program?

- The law—specifically the personal responsibilities that arise under the law (including offenses and penalties)
- The policy and specific procedures of the bank to help prevent or deter money laundering and financing of terrorism, as applied to the individual and business area concerned
- Examples of suspicious activity (red flags and typologies)
- How and to whom to report suspicions
- How to deal with customers after reporting suspicious activity or transactions

- Staff employed in a domestic capacity (cleaning and catering)—It is unnecessary for these staff members. Because they will never deal with a customer or any transactions, they do not require any AML/CFT training.
- IT staff—If the IT staff does not deal directly or indirectly with customers or customer transactions, they need not be included in AML/CFT training or awareness programs.
- Compliance and audit staff—Although they may not have direct responsibility for dealing with customers or customer transactions, compliance and audit staff may become suspicious when performing their duties. Thus, they need to be aware of the broad range of AML/CFT controls, including how and to whom any suspicions should be reported.
12.1 Risk-based approach to AML controls

When considering the implementation of a risk-based approach to AML/CFT controls, banks and other financial institutions should consider the following risk elements and determine how each factor will be dealt with operationally (FATF Recommendation 5 includes a reference to controls introduced on a "risk-sensitive basis"):  

Geography

Since 2000, the FATF has published a list of non-cooperative countries and territories (NCCT). These are jurisdictions considered to represent a higher degree of risk from an AML/CFT perspective because they are deemed to have inadequate laws, regulations, and rules to deter those seeking to launder money (as of October 2006, no country remained on the list). Local regulations may require institutions to apply additional controls to business dealings with such jurisdictions—a good example of a risk-based approach. Banks and other financial institutions may also seek to identify other countries that may pose a special AML/CFT risk.

Customer type

It is now understood that certain types of customers will represent a higher degree of risk from an AML/CFT perspective and all institutions should apply higher standards of AML/CFT controls, including CDD, to these types of customers.

PEPs (for example, heads of state or senior politicians) occasionally use their position to benefit financially from corruption. Higher standards of CDD should be applied to such clients, irrespective of where in the business their relationship was established. Consideration should also be given to the nature of the customer’s business. Casinos, money service businesses, and dealers in military equipment represent a higher degree of risk than retailers of clothing or sports equipment, for example.

Product/service

Financial institutions shall consider which of their products or services represent a higher risk of potential abuse by criminals seeking to launder criminal funds.
For instance, products such as third-party wire payments, letters of credit, cash handling, and credit cards are all high risk. Other services that may also require additional care and attention could be large project finance deals (possible corruption) as well as private banking and correspondent banking, as mentioned above. FATF Recommendations 7 and 8 identified the following areas that present a higher degree of ML/FT risk:

- Payable-through accounts and correspondent banking, especially where respondent banks are from financial centers with weak supervision and where shell and parallel banking structures are permitted
- Products and services that permit customer or transactional anonymity and where there is no physical contact with clients

For more information on FATF Recommendation 7, see Appendix H. For more information on FATF Recommendation 8, see Appendix M.

12.2 Risk management

**Controls**

The institution’s AML/CFT policy should explain how inherent risks will be managed. This can be achieved in the following ways:

- Through monitoring by line management or a designated compliance team to check business units for compliance with the institution’s AML/CFT policy, as well as local legal and regulatory standards. To be fully effective, review plans or schedules should be established in advance.
- Through a reporting process that allows significant exceptions to be reported quickly and efficiently through the compliance hierarchy. Again, criteria for such reporting must be agreed upon and understood. Some possible examples:
  - A breach of any law, rule, or regulation
  - Disciplinary action by the local regulator
  - Damage to the company’s reputation
  - Breach of AML/CFT policy
  - Fine incurred
  - Monetary loss
  - Serious internal fraud
  - Breakdown of compliance controls
  - Other events deemed appropriate to report
- Through annual (or more frequent) certification by compliance officers that AML/CFT controls have been enforced and no exceptions identified
- Through inclusion in job descriptions of references to the application of AML/CFT policy and procedures
- Through appropriate segregation of duties
BENEFITS TO THE BUSINESS

Financial institutions benefit in several ways from the application of robust AML/CFT controls and risk-management systems. The benefits fall into the following categories:

Customer service

By applying strong identification and KYC controls, the business will be better able to understand its customers and their transactions. It will be better positioned to sell additional products and services to its customers in the future.

Protection from risk

A robust CDD process also provides protection to the business from the following risks (References from “Customer Due Diligence for Banks,” Basel Committee on Banking Supervision, October 2001):

- **Reputational risk.** Adverse publicity about a bank’s business practices and associations, which can arise when a bank becomes a vehicle for illegal activities by its customers, can cause a loss of confidence in the institution.
- **Operational risk.** Institutions can sustain direct or indirect losses from inadequate or failed internal procedures, often a result of failure to practice due diligence. One example might be a fraudulent account that obtains credit facilities.
- **Legal risk** is the risk of legal action, adverse judgments, or unenforceable contracts that can disrupt and adversely affect the operations of a bank. An example would be failure to observe mandatory CDD standards.

12.3 External reporting of suspicious transactions and activity (STR/SAR)

The business units of any financial institution should have procedures in place so that once suspicious transactions or activity is identified the following action is taken. FATF Recommendation 13 requires that financial institutions report suspicious transactions to their financial intelligence unit (FIU). For more information on FATF Recommendation 13, see Appendix N.

Whereas internal reporting includes the following aspects . . .

- Details of the suspicion are reported to a central point within the institution using a standard report format. Usually the person who receives these reports will be someone based within the compliance/security function, depending on the organizational structure. Let’s call this nominated officer the MLRO.
- The suspicion report should be subject to some form of validation by the MLRO. This process is important for the following reasons:
  - Not all suspicions reported by staff will be of the same standard, so further research may be required.
  - An independent review prevents the bank from making disclosure reports to the local authorities that are inappropriate.
External reporting should consider the following issues:

- The MLRO can make sure that only relevant information is disclosed to the local authorities within any suspicion report.
- The MLRO provides a single point of contact for the authorities with the bank.
- The MLRO can make a determination regarding requests for other information received from the authorities.

Some other aspects to be considered:

- the MLRO can consider the risks associated with continuing the relationship with the client and provide advice/guidance to the business management as appropriate; and
- in some jurisdictions where there is a suspicion regarding a transaction, consent may be required from the local authorities before the transaction can be processed.

**Cash transaction reporting (CTR)**

In some jurisdictions around the world, there is a requirement to report cash transactions over a preset threshold. Compliance with this obligation can often be achieved by using systems to identify and report such transactions.

### 12.4 Cooperation with the authorities

When dealing with suspicions of money laundering or terrorist financing, financial institutions will always need to consider where their duty of client confidentiality ends and their obligation to provide assistance to the authorities with their own criminal investigations begins. Generally, where a bank has a legal obligation to report suspicions, it is protected from any action by the customer for breach of confidentiality.

However, confidential information about any customer may only be provided to the authorities, without the consent of the customer, when there is a legal obligation to do so. Therefore, in general terms, any further information concerning a client who has previously been the subject of a suspicion report should only be advised to the authorities in accordance with national legislation.

On some occasions, the authorities may request that an account relationship that has previously been reported be allowed to continue in operation, to provide more financial intelligence as part of any investigation. Any such request received may need to be considered in the light of the possible increased reputation risk to which the bank would be exposed by continuing with such a relationship.
12.5 Compliance/legal function
The compliance function provides support to business line management in the following areas of AML/CFT controls:

- It interprets legal and regulatory requirements.
- It provides an independent evaluation of the bank’s own policies and procedures.
- It assists with the development and review of procedures required for compliance with local legal and regulatory requirements, as well as with the policy of the bank.
- It provides advice and guidance to the business on day-to-day issues that may arise with respect to potentially suspicious transactions and other matters relating to AML/CFT controls.
- It monitors compliance with key AML/CFT procedures and controls.
- By means of exception reporting, it provides alerts to senior management on major failures in the application of AML/CFT policy.

12.6 Audit function
An organization’s internal audit function needs sufficient resources and should enjoy an appropriate degree of independence within the organization. Specifically, internal auditors (or external auditors, where appropriate) should be able to

- confirm the overall integrity and effectiveness of the management systems, controls, and AML/CFT technical compliance;
- focus on risk and include appropriate sample tests with emphasis on higher-risk areas, products, customers, and services;
- consider the completeness of customer identification and KYC information gathered at the account opening stage;
- assess the employees’ knowledge and understanding of the AML/CFT controls applicable in any business area;
- assess the adequacy, accuracy, and completeness of any training programs delivered;
- assess the adequacy of the bank’s process for identifying and reporting suspicious activity;
- recommend corrective action for any deficiencies identified (perhaps in conjunction with compliance) and carry out follow-up reviews; and
- promptly communicate their findings to the board/senior management as appropriate.
Check your understanding

Select the correct answer. Detailed explanations will be given at the end of the module.

**QUESTION 32.** Who might want to launder money?
   a) Drug traffickers
   b) Persons undertaking wire payment fraud
   c) Terrorists
   d) All of the above

**QUESTION 33.** Money laundering is not a problem for banks because it does not lead to losses, as it does in the case of fraud.
   a) True    b) False

**QUESTION 34.** Money laundering does not put individual bank employees at risk.
   a) True    b) False

**QUESTION 35.** Money is only laundered through banks.
   a) True    b) False

**QUESTION 36.** Which of the following statements is true?
   a) Money laundering does not harm anyone.
   b) Money laundering occurs only through banks.
   c) The receipt and payment of high-value funds is a major topic in the fight against money laundering.
   d) Money laundering relates only to cash.

**QUESTION 37.** Which of these statements is true?
   a) Money laundering activity can damage a bank’s reputation.
   b) Money laundering is good for the bank because it supplies additional cash to the system.
   c) Employees need to be worried about large cash deposits only when considering suspicious transactions.
   d) Money laundering is something only the bank, but not you as an individual, must worry about.
**QUESTION 38.** Which of these is a definition of money laundering?

a) Money laundering is the process by which banks move cash around for their customers.

b) Money laundering is a process designed to hide the origin of criminal funds.

c) Money laundering is a process designed to prevent the confiscation of criminal funds by the authorities.

**QUESTION 39.** Which of these is a stage of the money laundering process?

a) Collaborating

b) Drying

c) Layering

d) Building

**QUESTION 40.** When opening an account for a new customer, what information must be obtained on every occasion?

a) Verification of identity

b) Assets held

c) Annual salary

d) Time at current address

**QUESTION 41.** Which of the following documents provides the best evidence of a new customer’s identity?

a) Passport or national identity card

b) Driver’s license

c) Birth certificate

d) A letter of introduction

**QUESTION 42.** A new private limited company has opened an account with your bank. Which of the following persons need to be identified?

a) Signatories

b) Directors

c) Shareholders (beneficial owners)

d) All of the above
**QUESTION 43.** While dealing with a customer, you become suspicious that he or she may be involved with the proceeds of a serious crime. Which of the following actions should you take?

a) Tell your line manager and submit a suspicious activity report.
b) Forget about it.
c) Tell the customer—he or she has a right to know about it.
d) Tell one of your colleagues.

**QUESTION 44.** You only have an obligation to report a suspicion if you actually performed the transaction for the customer.

a) True  

b) False

**QUESTION 45.** It is permissible to tell a customer that a suspicious transaction report has been submitted if he or she asks you.

a) True  

b) False

**QUESTION 46.** Unlike fraud, money laundering activity does not affect the bank’s profits.

a) True  

b) False
Appendix A: References

FATF Recommendations

• The Forty Recommendations (FATF, June 2003)
  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
• Special Recommendations on Terrorist Financing (FATF, October 2004)

Useful Web sites

• Financial Action Task Force on Money Laundering (FATF)
  http://www.fatf-gafi.org/pages/0,2966,en_32250379_32235720_1_1_1_1_1_1,00.html
• Basel Committee on Banking Supervision (BCBS)
  http://www.bis.org/bcbs/index.htm
• Transparency International
  http://www.transparency.org/index.html
• Wolfsberg Group
  http://www.wolfsberg-principles.com/index.html

Reference Documents

• FATF Annual Reports (FATF)
  http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32237245_1_32247548_1_1_1,00.html
• NCCT Annual Reports (FATF)
  http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32235720_1_32247550_1_1_1,00.html
• Typologies Reports (FATF)
  http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32235720_1_32247552_1_1_1,00.html
• Customer Due Diligence for Banks (BCBS, October 2001)
  http://www.bis.org/publ/bcbs85.pdf
• Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering (BCBS, December 1988)
  http://www.bis.org/publ/bcbsc137.pdf
• Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (BCBS, April 2002)
  http://www.bis.org/publ/bcbs89.pdf
• Banking secrecy and international cooperation in banking supervision (BCBS, August 1981)  
  http://www.bis.org/publ/bcbs00f.pdf  
• Joint Forum (Initiatives by the BCBS, IAIS, and IOSCO to combat money laundering and the financing of terrorism, June 2003)  
• Wolfsberg Statement on Monitoring Screening and Searching (Wolfsberg Group, September 2003)  
  http://www.wolfsberg-principles.com/monitoring.html  
• Wolfsberg AML Principles for Correspondent Banking (Wolfsberg Group, November 2002)  
  http://www.wolfsberg-principles.com/corresp-banking.html  
• Wolfsberg Statement on the Suppression of the Financing of Terrorism (Wolfsberg Group, January 2002)  
  http://www.wolfsberg-principles.com/financing-terrorism.html  
• Wolfsberg AML Principles on Private Banking, Revised Version (Wolfsberg Group, May 2002)  
  http://www.wolfsberg-principles.com/privat-banking.html  
• Wolfsberg FAQs on Beneficial Ownership (Wolfsberg Group)  
  http://www.wolfsberg-principles.com/faq-ownership.html  
• Wolfsberg FAQs on Politically Exposed Persons (Wolfsberg Group)  
• Wolfsberg FAQs on Intermediaries (Wolfsberg Group)  
  http://www.wolfsberg-principles.com/faq-intermediaries.html  
• Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD, November 1997) [see “Country Reports”]  
  http://www.oecd.org/document/21/0,2340,en_2649_34859_2017813_1_1_1,00.html#text  
• Global Corruption Report (Transparency International)  
  http://www.globalcorruptionreport.org/  
• Corruption Perception Index (Transparency International)  
  http://www.transparency.org/surveys/index.html#cpi  
• Report on Correspondent Banking: A Gateway for Money Laundering (Minority Staff of the Permanent Subcommittee on Investigations, United States Senate, February 2001) [300 pages]  
• Private Banking and Money Laundering—A Case Study of Opportunities and Vulnerabilities (S. Hrg. 106-428, Hearings Before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, November 1999) [1,128 pages]  

Countries should apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses. Predicate offenses may be described by reference to all offenses, or to a threshold linked either to a category of serious offenses or to the penalty of imprisonment applicable to the predicate offense (threshold approach), or to a list of predicate offenses, or a combination of these approaches.

Where countries apply a threshold approach, predicate offenses should at a minimum comprise all offenses that fall within the category of serious offenses under their national law or should include offenses which are punishable by a maximum penalty of more than one year’s imprisonment or for those countries that have a minimum threshold for offenses in their legal system, predicate offenses should comprise all offenses, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offenses within each of the designated categories of offenses.\textsuperscript{14}

Predicate offenses for money laundering should extend to conduct that occurred in another country, which constitutes an offense in that country, and which would have constituted a predicate offense had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offense had it occurred domestically.

Countries may provide that the offense of money laundering does not apply to persons who committed the predicate offense, where this is required by fundamental principles of their domestic law.

\textsuperscript{14} See the definition of “designated categories of offenses” in the Glossary.
Countries should ensure that:

a) The intent and knowledge required to prove the offence of money laundering is consistent with the standards set forth in the Vienna and Palermo Conventions, including the concept that such mental state may be inferred from objective factual circumstances.

b) Criminal liability, and, where that is not possible, civil or administrative liability, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which such forms of liability are available. Legal persons should be subject to effective, proportionate and dissuasive sanctions. Such measures should be without prejudice to the criminal liability of individuals.
Countries should adopt measures similar to those set forth in the Vienna and Palermo Conventions, including legislative measures, to enable their competent authorities to confiscate property laundered, proceeds from money laundering or predicate offences, instrumentalities used in or intended for use in the commission of these offences, or property of corresponding value, without prejudicing the rights of bona fide third parties.

Such measures should include the authority to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the State’s ability to recover property that is subject to confiscation; and (d) take any appropriate investigative measures.

Countries may consider adopting measures that allow such proceeds or instrumentalities to be confiscated without requiring a criminal conviction, or which require an offender to demonstrate the lawful origin of the property alleged to be liable to confiscation, to the extent that such a requirement is consistent with the principles of their domestic law.
Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.

Financial institutions should undertake customer due diligence measures, including identifying and verifying the identity of their customers, when:

- establishing business relations;
- carrying out occasional transactions: (i) above the applicable designated threshold; or (ii) that are wire transfers in the circumstances covered by the interpretative note to Special Recommendation VII;
- there is a suspicion of money laundering or terrorist financing; or
- the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The customer due diligence (CDD) measures to be taken are as follows:

a) Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.\(^\text{15}\)

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer.

c) Obtaining information on the purpose and intended nature of the business relationship.

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 institution’s knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

Financial institutions should apply each of the CDD measures under (a) to (d) above, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship or transaction.

\(^\text{15}\) Reliable, independent source documents, data or information will hereafter be referred to as “identification data.”
The measures that are taken should be consistent with any guidelines issued by competent authorities. For higher risk categories, financial institutions should perform enhanced due diligence. In certain circumstances, where there are low risks, countries may decide that financial institutions can apply reduced or simplified measures.

Financial institutions should verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit financial institutions to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering risks are effectively managed and where this is essential not to interrupt the normal conduct of business.

Where the financial institution is unable to comply with paragraphs (a) to (c) above, it should not open the account, commence business relations or perform the transaction, or it should terminate the business relationship; and should consider making a suspicious transactions report in relation to the customer.

These requirements should apply to all new customers, though financial institutions should also apply this Recommendation to existing customers on the basis of materiality and risk and should conduct due diligence on such existing relationships at appropriate times.
Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic or international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority.

**Interpretative Note to Recommendations 10 and 11**

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself, the premium payment and the benefits.
Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.
b) An ongoing employee training programme.
c) An audit function to test the system.

Interpretative Note to Recommendation 15
The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.
Financial institutions should, in relation to cross-border correspondent banking and other similar relationships, in addition to performing normal due diligence measures:

a) Gather sufficient information about a respondent institution to understand fully the nature of the respondent’s business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a money laundering or terrorist financing investigation or regulatory action.

b) Assess the respondent institution’s anti-money laundering and terrorist financing controls.

c) Obtain approval from senior management before establishing new correspondent relationships.

d) Document the respective responsibilities of each institution.

e) With respect to “payable-through accounts,” be satisfied that the respondent bank has verified the identity of and performed on-going due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer identification data upon request to the correspondent bank.

Appendix H:
FATF Recommendation 7
Financial institutions should, in relation to politically exposed persons, in addition to performing normal due diligence measures:

a) Have appropriate risk management systems to determine whether the customer is a politically exposed person.
b) Obtain senior management approval for establishing business relationships with such customers.
c) Take reasonable measures to establish the source of wealth and source of funds.
d) Conduct enhanced ongoing monitoring of the business relationship.

**Interpretative Note to Recommendation 6**

Countries are encouraged to extend the requirements of Recommendation 6 to individuals who hold prominent public functions in their own country.
Countries may permit financial institutions to rely on intermediaries or other third parties to perform elements (a)–(c) of the CDD process or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer identification and verification remains with the financial institution relying on the third party.

The criteria that should be met are as follows:

a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)–(c) of the CDD process. Financial institutions should 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.

b) The financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10.

It is left to each country to determine in which countries the third party that meets the conditions can be based, having regard to information available on countries that do not or do not adequately apply the FATF Recommendations.
Financial institutions should pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors.

**Interpretative Note to Recommendations 10 and 11**

In relation to insurance business, the word “transactions” should be understood to refer to the insurance product itself; the premium payment and the benefits.
Appendix L: 
FATF Special Recommendation VII

VII. Wire transfers

Countries should take measures to require 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 that do not contain complete originator information (name, address and account number).
Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. In particular, financial institutions should have policies and procedures in place to address any specific risks associated with non-face-to-face business relationships or transactions.
If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

**Interpretative Note to Recommendation 13**

The reference to criminal activity in Recommendation 13 refers to:

a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or
b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.
III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.
Answers
Module 3b Answers

Answer 1
d)

Answer 2
False

Answer 3
False

Answer 4
a)

Answer 5
False

Answer 6
Placement—Placement is the first stage of money laundering.
Layering—Layering is the second stage of money laundering.
Integration—Integration is the third stage of money laundering.

Answer 7
Almost any kind of criminal activity that generates significant amounts of funds is likely to lead to money laundering in some form.

Answer 8
c) Drug trafficking is believed to generate most criminal proceeds in most countries; however, the circumstances of individual country will dictate the correct answer.

Answer 9
e) The estimate most often quoted is US$500,000,000,000.

Answer 10
c) All of the penalties mentioned can be serious. Multimillion dollar fines have been imposed around the world, but the biggest risk to major financial institutions is damage to reputation. No one will ever know how much business is lost to an organization as a result of publicized involvement (perhaps inadvertent) in a major money laundering case. The short-term consequences can often be measured in the fall of a company’s quoted share price, a potential cost to shareholders of millions of dollars.
Answer 11
- A marketing plan to ensure maximum product sales are achieved
  - Not quite. While it is expedient for financial institutions to maximize the sale of products and services to new and existing customers, this approach will not prevent money laundering or the financing of terrorism.

- A procedure to ensure that all customers are identified
  - Yes. This is a critical element of any AML/CFT policy. Close attention must be given to its implementation.

- An IT policy ensuring appropriate controls on all computers and communications equipment
  - No. While it is important that systems used by financial institutions are protected from attack (malicious or accidental), this does not directly deter money laundering or the financing of terrorism.

- A policy on diversity and equal opportunity
  - No.

- A policy maintaining customer records and transaction details
  - Yes. Records maintained by a financial institution help the authorities trace suspect funds back to their original source.

- A policy requiring clients to provide additional information about their business so that the financial institution can gauge its likely level of activity
  - Yes. This is a key element of any KYC policy.

Answer 12
All of them have varying responsibilities for dealing with AML/CFT, and training should reflect this. The challenge is to decide who needs to be trained in which aspects of AML/CFT. Employees who deal directly with customers will need to face a more intense and detailed program than will other employees, who may only need to have a general level of awareness. Remember, your institution is only as strong as its weakest link.

Answer 13
d) In many jurisdictions CDD must be completed when a single one-off transaction exceeds a specified threshold. Within the European Economic Area a threshold of EUR 15,000 has been set.

Answer 14
Yes. Because DEF, Ltd. is a major shareholder, you need to know who is behind the company.

Answer 15
Yes. Because GHK, Ltd. is the main beneficial owner, you need to understand who owns and controls the company.
**Answer 16**
Yes. You should establish the identity of Mr. Burns.

**Answer 17**
No, because the directors and major shareholder have been identified.

**Answer 18**
d)

**Answer 19**
e)

**Answer 20**
The following are examples of some other high-risk scenarios:

- Money service businesses that operate in jurisdictions without regulation and are not subject to any local AML/CFT controls
- Unregulated businesses involving gaming/gambling activities, including Internet gambling
- Offshore trusts, special-purpose vehicles, and international businesses established in locations where there is no or inadequate AML/CFT legislation and regulation
- Private or public companies not subject to regulatory disclosure requirements that are constituted in full or in part with bearer shares
- Customers with complex account relationships across multiple jurisdictions and where high-value and high-frequency transactional activity cannot easily be monitored
- Dealers in high-value goods
- Cash-based businesses
- Lawyers and accountants
- Dealers in precious metals and stones

Each of the above examples will represent a slightly different risk. You may be able to think of many others.

**Answer 21**
Not suspicious, unless the amount deposited exceeds the amount one might reasonably obtain from the sale of a motor vehicle, or unless the large deposits continue.

**Answer 22**
Suspicious, unless you are able to speak to Mr. Hibbard and ascertain a legitimate reason for the activity. As an office worker, he would not normally be receiving numerous cash credits to his account. The deposits are broken down
into smaller sums that can be credited to the account without raising concern. This method is often used by persons who have large amounts of cash that they need to get into the financial system.

Answer 23
Suspicious. This does seem odd. Why would someone send Mr. Hibbard a payment only for him to send the funds back to the same country in a short period of time? Unless more information can be obtained, this appears to be part of a layering operation to confuse the audit trail leading to the original source of the funds.

Answer 24
Not suspicious. Although this might appear suspicious at first, it is important to understand the source of the funds and the reasons why they were received. It is likely that in these circumstances Mr. Hibbard may have retired or received a bonus. The key is to know more about Mr. Hibbard’s circumstances.

Although you must be careful that Mr. Hibbard is not stealing the funds from his employers, it is unlikely that he would come to the bank seeking investment advice if he were. More likely he would want to move the funds on or even withdraw them in cash.

Answer 25
Not suspicious. As in other jurisdictions, companies registered in the British Virgin Islands can be used for legitimate business as well as a front for potential money laundering. That the company is registered there is not itself grounds for suspicion.

Answer 26
Suspicious. This should be cause for concern. Why did the company not know about such a substantial increase in activity at the time the account was opened? Any legitimate business would be the subject of negotiation and contracts. For the increased activity to occur so quickly must be regarded as suspicious.

Answer 27
Suspicious. Why would private individuals be sending large amounts to the company? It is possible that the company is being used as a front for money laundering, that is, to commingle criminal funds with legitimate funds generated by business activities.

Answer 28
Not suspicious. Although letters of credit can be abused by money launderers, they also are used by legitimate businesses around the world to provide an element of protection when conducting business with other third parties. Therefore, this request, on its own should not be regarded as suspicious.
Answer 29
(a)–(l) Yes
(m)–(n) No, not required as part of a SAR
(o) No, not required as part of a SAR, although the competent authorities may subsequently request this information.
(p) Yes

Answer 30
(c) FATF Recommendation 10 states that all necessary records should be maintained for at least five years.

Answer 31
(a)–(c) Yes, to be retained for at least five years from the date the relationship with the client ends.
(d) Yes, to be retained for at least five years from the date of the transaction.
(e) No, this information is not usually required.
(f) Yes, these are very important as they can constitute clear evidence that a report was submitted, providing a defense against charges of failure to report.
(g) Yes, also very important as evidence that a report was made to the authorities.
(h) No, this information is not required.

Answer 32
(d) Any form of criminal activity that generates some form of financial proceeds may need to use a money laundering process to disguise the origin of the funds. Persons seeking to finance terrorist-related activity may also use the money laundering process to disguise the origin of the funds collected and payments made for the purchase of arms/explosives.

Answer 33
False. When a bank becomes involved in a money laundering scheme, wittingly or unwittingly, it will lose money in the following ways: through fines and penalties imposed by regulators, through fines arising from criminal prosecution, and through profit losses arising from a damaged reputation.

Answer 34
False. A growing number of countries throughout the world have developed anti-money laundering laws and regulations that place a personal responsibility on individuals who work in the financial sector. Employees of banks and other financial institutions may face disciplinary action or even criminal prosecution for dereliction of duty if they neglect to report suspicious activity.
Answer 35
False. Money laundering occurs throughout the financial sector and in many other parts of society as well. Goods and services purchased with criminal money are usually considered part of the money laundering process because the purchases allow cash to enter the financial system with legitimate appearance.

Answer 36
c) People commit crimes and then launder the funds to make them appear legal. Money laundering can occur through almost any business. Cash is often involved, typically in the first stage of a laundering operation.

Answer 37
a) Any transaction could be part of a money laundering operation. In many jurisdictions employees of financial institutions have personal legal obligations related to controlling money laundering.

Answer 38
b)

Answer 39
c)

Answer 40
a) The other information may be useful but it is not essential.

Answer 41
a) A driver’s license may be used in some countries as a proof of identification. In many countries, the issuance of birth certificates is not controlled. Thus a birth certificate should not be relied upon as evidence of identity. It is risky to rely on a letter of introduction.

Answer 42
d) All parties should be identified.

Answer 43
a) You cannot forget about it because you may be under a personal legal obligation to report your suspicion. Telling the customer might mean you are committing the offense of “tipping-off.” You might wish to discuss the circumstances with a more experienced colleague, but if you are suspicious, you still must submit a report.
Answer 44
False. You have an obligation to report any suspicion you may have at the earliest opportunity, regardless of whether you were directly involved in the transaction.

Answer 45
False. Under no circumstances must you tell a customer, or any other third party, that a suspicious transaction report has been submitted.

Answer 46
False. By damaging the reputation of the bank, profits can be significantly affected.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

Module 1: Effects on Economic Development and International Standards
Module 2: Legal Requirements to Meet International Standards
Module 3a: Regulatory and Institutional Requirements for AML/CFT
**Module 3b: Compliance Requirements for Financial Institutions**
Module 4: Building an Effective Financial Intelligence Unit
Module 5: Domestic (Inter-Agency) and International Cooperation
Module 6: Combating the Financing of Terrorism
Module 7: Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Building an Effective Financial Intelligence Unit

Workbook
Building an Effective Financial Intelligence Unit

Workbook

THE WORLD BANK
Washington, D.C.
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti-Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

Module 4 was written by Martin Comley, the World Bank. The draft was reviewed by Bess Johnson Michael, the World Bank, and Matthew Byrne and Louise Schultz, AUSTRAC. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by Emiko Todoroki and John McDowell, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo and Paul Allan Schott, the World Bank. Key sources for this workbook include: Financial Action Task Force on Money Laundering, “The Forty Recommendations, 2003”; and “Special Recommendations on Terrorist Financing, 2005”; and Paul Allan Schott, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second Edition, the World Bank, 2004.
Module 4 will examine the financial intelligence unit (FIU) and its role in the national anti-money laundering and combating the financing of terrorism (AML/CFT) regime. This module addresses the following issues:

1. Basic Concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regime
   1.1 Where strategically does the FIU fit into AML/CFT regime? 4
   1.2 Where legislatively does the FIU fit into AML/CFT regime? 6
   1.3 So, what is an FIU? 7
   1.4 Why a “national center”? 7
   1.5 Information gathering—and more 9
   1.6 What are the FIU’s functions? 9

2. Building FIU functionality
   2.1 Receipt 11
   2.2 Analysis 24
   2.3 Dissemination 32
   2.4 Other FIU functions 33

3. Coordination and cooperation at the policy and operational levels 38
   3.1 Domestic 38
   3.2 International 40
   3.3 Cooperation and access to financial intelligence 42
   3.4 The Egmont Group 48

4. Skills, integrity, and security of FIU personnel 49
   4.1 What skills do FIU personnel need? 49
   4.2 Where will you find the initial personnel for your FIU? 49
   4.3 What issues do “mixed” staff bring with them? 50
   4.4 Integrity 50
   4.5 Security 51

5. What type of FIU will you have? 53

6. Summary 55
This module covers issues in the following FATF Recommendations:
Overall, the FATF Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing (FATF 40 + 9) should be considered relevant in this module. Principally, however, we will look at Recommendation 26. But, we will also explore, in lesser detail, issues covered by the following recommendations as they affect either the FIU or the reporting of suspicious transactions: Recommendations 25, 30, 31, and 40 (Recommendations 13, 16, and 19, as well as Special Recommendations IV and IX are referenced in Knowledge Checks).

At the end of the module you will be able to
• discuss where the FIU fits into your country’s AML/CFT strategy;
• explain what an FIU is;
• describe the functions of an FIU;
• discuss the importance of interagency and international cooperation;
• describe the Egmont Group;
• understand how the FIU should be staffed;
• describe which FIU model is most appropriate for your country;
• assess whether your country’s FIU is effective enough to meet its responsibilities; and
• look at the challenges that FIUs face.
1

How much do you know?

**QUESTION 1.** Every relevant governmental authority should have its own FIU in its organization to independently fight against money laundering and terrorist financing.

a) True   b) False

**QUESTION 2.** Financial institutions should develop their own form of suspicious transaction reports (STRs) as part of their internal control and risk management.

a) True   b) False

**QUESTION 3.** Core functions of an financial intelligence unit (FIU) are analysis, dissemination, and investigation.

a) True   b) False

**QUESTION 4.** Suspicion transaction reports (STRs) are the only type of report an FIU could receive.

a) True   b) False

**QUESTION 5.** An FIU should be placed in the Central Bank as a national center for financial intelligence.

a) True   b) False

What systems and controls are necessary for an efficient AML/CFT regime? Guidance can be found in the FATF Forty Recommendations on Money Laundering, the FATF Nine Special Recommendations on Terrorist Financing, and “Methodology for Assessing Compliance with the FATF Forty Recommendations and the FATF Nine Special Recommendations,” (a joint program of the FATF, the World Bank, and the International Monetary Fund [IMF]), as well as in the various United Nations Conventions and United Nations Security Council (UNSC) Resolutions dealing with money laundering and the financing
of terrorism. Another useful reference document is “Financial Intelligence Units: An Overview,” from the World Bank and the IMF. Several other international and regional organizations/bodies, such as the Egmont Group and the Council of Europe, adopted conventions and other documents relevant for combating money laundering and terrorist financing. We will draw on these documents throughout this module. Reference to and familiarity with them is important in understanding how to build an effective FIU. For further information about the methodology for assessing compliance with the FATF 40 + 9, please refer to Module 1.

1.1 Where strategically does the FIU fit into an AML/CFT regime?

Tracking money launderers, terrorist financiers, and their funds requires a range of knowledge and skills covering not only laws, regulations, investigations, and analysis, but also banking, finance, accounting, and related economic activities. The required knowledge and skills may not be found in a single agency in countries developing AML/CFT regimes. It is likely, however, that some or all of the skills can be found in various official bodies.

Knowledge check

QUESTION 6. Give examples of official bodies in your country that have some or all of the skills mentioned above.

Financial investigations, which are critical in the fight against money laundering and terrorist financing, require access to financial information. Access to such information usually comes in one of three ways:

- In response to law enforcement/judicial investigations, in which specific material, such as financial information, is sought from individuals or legal entities. (These issues are covered by module 7.)
- Through systems and controls applied to a country’s financial institutions and designated non-financial businesses and professions (DNFBPs). Those systems require suspicious transaction reports (STRs) and other reports as designated by law to be generated and passed on to an official body (usually the FIU) for analysis and further action. In some countries, these reporting requirements go beyond specific transactions and involve suspicious activity reports (SARs). The terms are used interchangeably in these modules. For ease of reference, this module refers to such bodies as “reporting entities.”
• From foreign authorities, such as FIUs and law enforcement agencies (LEAs), which, based on their own STRs or criminal investigations, may share their findings with domestic FIUs and LEAs. In some jurisdictions, this is the main source of information and their financial investigations are usually triggered by foreign requests for cooperation or mutual legal assistance.

Knowledge check

QUESTION 7. Give some examples of types of reporting entities:

a) Financial Institutions (FIs)

b) Designated Non-financial Businesses and Professions (DNFBPs)

To be effective, a national AML/CFT regime must be described in a strategic plan that is the product of interdepartmental cooperation. It cannot be the work of a single ministry or agency.

QUESTION 8. Which ministries/agencies would typically be involved in such a group?

So far, we have mentioned the need for knowledge and skill in law, regulation, finance, and so on. We have mentioned LEAs, FIs, and DNFBPs. But we have not looked at the FIU. Why? Because it is important to realize the FIU does not stand alone; it must be seen as an integral part of an overall AML/CFT regime.
1.2 Where legislatively does the FIU fit into an AML/CFT regime?

The FIU is often the link between a nation’s criminal law enforcement authorities and its administrative regulatory bodies. The FIU may or may not have specific criminal or administrative functions assigned to it. Close integration of the criminal and administrative components tends to make AML/CFT regimes more efficient.

While not explicit in the FATF 40 + 9 Recommendations (or in the Egmont definition of an FIU), it is widely interpreted that the FIU should stand on a firm legislative basis, provided either by stand-alone legislation or by other legislation such as the anti-money laundering and/or countering financing of terrorism law. The following sections outlines matters that should be taken into consideration by the legislative drafter.
1.3 So, what is an FIU?

We find part of the answer in FATF Recommendation 26, which says:

“Countries should establish an FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis, and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.”

The UN Convention against Organized Crime (the Palermo Convention) in article 7, the United Nations Convention against Corruption in article 14, and the Egmont Group of Financial Intelligence Units in its “Statement of Purpose” provide a similar definition. The Egmont Group will be discussed later in this module. For more information on FATF Recommendation 26, see Appendix B.

1.4 Why a “national center”?

The answer to this is really a matter of prudent management of the national AML/CFT regime. Since the late 1980s, AML has grown from the simple reporting of drug-related funds to a system now covering a wider range of criminality—including the financing of terrorism. The range of financial institutions and DNFBPs that are required to maintain AML/CFT systems and controls also has grown.
**Knowledge check**

**QUESTION 9.** List some crimes that should be included as the predicate offenses for money laundering.

Further details on predicate offenses are given in Appendix C, as well as in Module 2.

We have seen that the FIU shares functions and processes—criminal and administrative—with other bodies. But it also has certain functions that are unique to it alone. Let us now look at some other simple examples of why the FIU should be a national center.

- Consider an individual who uses a bank that is close to his residence but happens to be in another administrative district. Imagine that the bank’s head office is located in a third district. In the absence of a national center, in which district would a report be made?
- Not all financial institutions and DNFBPs have their offices (or head offices) in the same towns/districts. Should each office report to a different branch of the FIU? If reports involve the same individuals but go to different centers, how will they be tied together?
- Should the different business areas of financial institutions and DNFBPs report to different centers? For example, if a financial institution undertakes several types of financial operations, should the banking division report to one office and the stockbroker another?
- Criminals are generally not involved in single forms of criminality. A drug trafficker may also be involved in fraud. In such a case, should the report be made to a police drug squad or the police fraud squad? And if the fraud is funding terrorism, who gets the report?
- The role of the FIUs in international cooperation shall also be taken into account—for example, to whom shall a foreign FIU send its request for the exchange of information if there are several branches of the FIU?

The previous examples are meant to be illustrative of practical problems that might occur in the absence of a central, national FIU. As we work through the module, you will encounter other examples of the importance of the FIU’s national scope. For the sake of the effectiveness of the AML/CFT regime, it is important that legally mandated reporting should be as simple and efficient as possible. Financial institutions and DNFBPs are required to identify STRs; they
should not have to worry about where to send the STR. The best solution is to designate a single national center to receive reports: the FIU.

1.5 Information gathering—and more
To meet international requirements (and as a matter of efficient management of the AML/CFT process), the FIU must be a national center for collection of STRs and related information. But acting as a national collection point for STRs is not its only function!

Knowledge check

**QUESTION 10.** Drawing on the definition contained in FATF Recommendation 26 (see section 1.3), write the three core functions of an FIU in the schematic below.

**QUESTION 11.** Without referring back in the module, list four of the bodies with which the FIU is most likely to interact.

1.6 What are the FIU’s functions?
To answer this question, we must look beyond FATF Recommendation 26. Because the FIU must interact across many parts of the AML/CFT regime, we must consult other Recommendations to determine the full scope of its responsibilities.

“Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (FATF)” is divided into 206 “essential
criteria” and 34 “additional elements” derived from the FATF 40 + 9 Recommendations. Those essential criteria and additional elements contain 37 explicit references to the FIU and STRs. And some criteria and elements that do not contain an explicit reference may nevertheless bear on the FIU or the STR process.

The important thing to remember is that Recommendation 26 is not the only source of guidance concerning the FIU’s functions or its scope of operations.

Knowledge check

**QUESTION 12.** Who should use “Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (FATF)” in reviewing the effectiveness of an AML/CFT regime?

Earlier we looked at the FIU as being, first, a national center for STRs and other information. We noted three functions associated with the STR process that are recognized as core functions of the FIU: receipt, analysis, and dissemination. We also mentioned that these three functions were not the totality of a FIU involvement in a country’s AML/CFT regime. What else is the FIU expected to do?

- Provide feedback on reported cases to financial institutions and DNFBPs.
- Produce sanitized cases from STRs and other material.
- Issue guidelines regarding the reporting requirements (FIU or another appropriate body).
- Publish periodic reports.
- Publish statistics.
- Contribute to and publish typologies and trends in money laundering and terrorist financing.
- Coordinate and cooperate, at the policy and operational levels, among:
  - policy makers;
  - law enforcement;
  - supervisors; and
  - other competent authorities.
- Engage in international cooperation.
- Provide training. While not explicitly mentioned in FATF or Egmont documentation, it often falls to the FIU to train personnel from financial institutions, DNFBPs, and LEAs, (as well as its own staff).
In the previous sections, we have briefly observed how the FIU and STR process fit into the AML/CFT regime.

For the rest of this module, you will assume the role of a project leader appointed by the National AML/CFT Committee to make recommendations concerning the establishment of the FIU and its day-to-day operations. Your twin goals are to serve your country and to meet internationally recognized standards.

The National AML/CFT Committee is counting on you for recommendations on how to structure your country’s new FIU. Start by looking at the FIU and how it will act as the national center for receipt of STRs and other reports, and for analysis and dissemination of information derived from those reports.

**Knowledge check**

**QUESTION 13.** Do you think each function—receipt, analysis, dissemination—can be “built” in isolation from the others? Select either yes or no, but give a brief explanation for your answer in the following space.

a) Yes  

b) No

2.1 **Receipt**

2.1.1 **FROM WHOM, OF WHAT, AND IN WHAT FORM?**

To deal with this, you first need to break the heading down into component parts. Let us do that by asking you a couple of questions.
Knowledge check

**QUESTION 14.** Which individuals and bodies (reporting entities) should be required to file STRs?


**QUESTION 15.** Are STRs the only type of report an FIU could receive? After providing your answer, give a brief explanation for your answer in the following space.

a) Yes  


b) No

Let us now discuss the issues.

**The STR—what’s in a name?**

Taking into consideration the range of entities from which you will be receiving reports and the diverse nature of their business products, you need to consider whether STR is the best term to define the reporting process. Must a transaction occur before a report can be made? Aren’t you looking for suspicious activity, whether or not a transaction occurs? You will find that the term “suspicious activity report” (SAR), now in common use, reflects the wider nature of reporting. Terminology can be important, as there is a tendency in some institutions to make literal interpretations.

**The content of the STR form**

Because the STR form will be a mainstay of your reporting process, give careful consideration to the design and content of the form. The data captured here will set parameters for the design of the FIU database. Remember, you cannot analyze what you do not capture. If your analysis is weak, this will have an adverse effect on your judgments about dissemination and the quality of what you do disseminate. The design and content of the STR form should be discussed with other stakeholders.
**Exercise**

Let us start by creating the format for an STR/SAR. Please use the following “Generic Reporting Form.” List fields that you consider as important to be included in the form.

**Details of Disclosing Organization (Reporting Entity)**

This category in the first sheet should provide information related to the reporting entity. Write the types of information you think you need in the appropriate category provided on the following form. If more information should be requested, add column.

**Person Subject of Disclosure**

This category in the first sheet should provide information related to a person who is the subject of the disclosure. Write the types of information you think you need for identifying the person in the category on the form. If more information should be requested, add column.

**Company Subject of Disclosure**

If a legal person\(^1\) or a legal arrangement\(^2\) is the subject of the disclosure, reporting entities may use this category, instead of “Person Subject of Disclosure” in the first sheet. Write the information you think you need for identifying the legal person in the category on the form. If more information should be requested, add column.

**Financial Summary Overview**

This category in the second sheet is customized specifically for reporting entities’ use and should provide information related to the reporting entity and the type of the report. Write the types of information you think you need in this category on the form. If more information should be requested, add column.

**Financial Summary Details**

This category in the second sheet should provide information related to financial transactions. Write the types of information you think you need for analyzing transactions in this category on the form. If more information should be requested, add column.

---

\(^1\) “Legal persons” refers to bodies corporate, foundations, anstalt, partnerships, associations, or any similar bodies that can establish a permanent customer relationship with a financial institution or otherwise own property. Source: Glossary for the FATF 40 Recommendations.

\(^2\) “Legal arrangements” refers to express trusts or other similar legal arrangements. Source: Glossary for the FATF 40 Recommendations.
**Associated Person**

This category in the third sheet is a repetition of the section “Person Subject of Disclosure.” There are cases in which the information of a person associated with a person or company subject of disclosure would be useful for analyzing the case; in these, this form is used.

**Associated Company**

This category in the third sheet is also a repetition of the section “Company subject of Disclosure.” There are cases in which the information of a company associated with a person or company that is the subject of the disclosure would be useful for analyzing the case. In such circumstances, this form would be used.

**Reason for Suspicion**

This category in the fourth sheet is for providing the reason why you raise suspicion. When you are in charge of analyzing the above reports, you may want to understand the significance of why this behavior was suspicious in the view point of the reporter. There is no specific or particular way of filling up this sheet.  

---

3 In some countries special lists of indicators for suspicious transactions have been adopted and reporting entities may just refer to the relevant indicator whether by number or describing it.
### Generic Reporting Form

**Reporting Form: Page 1**

<table>
<thead>
<tr>
<th>Details of Disclosing Organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Organization*:</td>
</tr>
<tr>
<td>Branch or Outlet:</td>
</tr>
<tr>
<td>Business area of Branch Outlet:</td>
</tr>
<tr>
<td>Your Disclosure Ref:</td>
</tr>
<tr>
<td>Date disclosure sent to FIU:</td>
</tr>
<tr>
<td>Has the subject been disclosed on before; if so give previous FIU Ref:</td>
</tr>
</tbody>
</table>

*If this is the first report you have made, complete a separate form to register your appointed compliance/money laundering officer.*

<table>
<thead>
<tr>
<th>Person subject of disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
<tr>
<td>Given Names(s):</td>
</tr>
<tr>
<td>Gender:</td>
</tr>
<tr>
<td>Date of Birth:</td>
</tr>
<tr>
<td>ID Document details:</td>
</tr>
<tr>
<td>Address No. &amp; Street:</td>
</tr>
<tr>
<td>City or Town:</td>
</tr>
<tr>
<td>Region:</td>
</tr>
<tr>
<td>Post or Zip Code:</td>
</tr>
<tr>
<td>Country:</td>
</tr>
<tr>
<td>Employer:</td>
</tr>
<tr>
<td>Occupation:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OR Company subject of disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name:</td>
</tr>
<tr>
<td>Company No:</td>
</tr>
<tr>
<td>Tax Number:</td>
</tr>
<tr>
<td>Type of Business:</td>
</tr>
<tr>
<td>Country of Reg:</td>
</tr>
<tr>
<td>1. Registered Office Address No. &amp; Street:</td>
</tr>
<tr>
<td>City or Town:</td>
</tr>
<tr>
<td>Region:</td>
</tr>
<tr>
<td>Post or Zip Code:</td>
</tr>
<tr>
<td>Country:</td>
</tr>
<tr>
<td>2. Trading Address No. &amp; Street:</td>
</tr>
<tr>
<td>City or Town:</td>
</tr>
<tr>
<td>Region:</td>
</tr>
<tr>
<td>Post or Zip Code:</td>
</tr>
<tr>
<td>Country:</td>
</tr>
</tbody>
</table>

Other Information not in fields above:
Generic Reporting Form

Reporting Form: Page 2

Financial Summary Overview:

<table>
<thead>
<tr>
<th>Institution Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlet/Branch:</td>
<td></td>
</tr>
<tr>
<td>Date Opened:</td>
<td>Date if Closed:</td>
</tr>
<tr>
<td>Customer’s Turnover:</td>
<td>Turnover time period:</td>
</tr>
<tr>
<td>Customer A/C or Ref No:</td>
<td></td>
</tr>
<tr>
<td>Balance held:</td>
<td>Date of Balance:</td>
</tr>
</tbody>
</table>

Financial Summary Details:

* Date: | Credit or Debit: |
| Value: | Currency: |
| Cash: Yes or No: | If no: type of financial instrument: |
| Counterparty Name: |  |
| Counterparty Institution: | If bank, bank code: |

* Date: | Credit or Debit: |
| Value: | Currency: |
| Cash: Yes or No: | If no: type of financial instrument: |
| Counterparty Name: |  |
| Counterparty Institution: | If bank, bank code: |

* Date: | Credit or Debit: |
| Value: | Currency: |
| Cash: Yes or No: | If no: type of financial instrument: |
| Counterparty Name: |  |
| Counterparty Institution: | If bank, bank code: |

* Date: | Credit or Debit: |
| Value: | Currency: |
| Cash: Yes or No: | If no: type of financial instrument: |
| Counterparty Name: |  |
| Counterparty Institution: | If bank, bank code: |

USE ADDITIONAL SHEETS IF THERE ARE FURTHER DETAILS TO BE SHOWN.
And complete the following: Financial Summary SHEET No: of .
(Example: Sheet 2 of 2. This would include the first sheet plus one extra.)
**Generic Reporting Form**

Reporting Form: Page 3

**ASSOCIATED Person (with subject of disclosure):**

<table>
<thead>
<tr>
<th>Family name:</th>
<th>Title:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Given Names(s):</td>
<td>Gender:</td>
</tr>
<tr>
<td>Date of Birth:</td>
<td></td>
</tr>
<tr>
<td>ID Document details:</td>
<td></td>
</tr>
<tr>
<td>Address No. &amp; Street:</td>
<td></td>
</tr>
<tr>
<td>City or Town:</td>
<td></td>
</tr>
<tr>
<td>Region:</td>
<td></td>
</tr>
<tr>
<td>Post or Zip Code:</td>
<td></td>
</tr>
<tr>
<td>Country:</td>
<td></td>
</tr>
<tr>
<td>Employer:</td>
<td></td>
</tr>
<tr>
<td>Occupation:</td>
<td></td>
</tr>
</tbody>
</table>

**OR ASSOCIATED Company (with subject of disclosure):**

| Company Name: | |
| Company No: | |
| Tax Number: | |
| Type of Business: | |
| Country of Reg: | |
| 1. Registered Office: | |
| Address No. & Street: | |
| City or Town: | |
| Region: | |
| Post or Zip Code: | |
| Country: | |
| 2. Trading Address: | |
| No. & Street: | |
| City or Town: | |
| Region: | |
| Post or Zip Code: | |
| Country: | |

**Other Information not in fields above:**

---

**USE ADDITIONAL COPIES OF THIS SHEET IF THERE ARE OTHER ASSOCIATED PEOPLE OR COMPANIES**

Complete the following if additional associated person or company sheets are used:

**ASSOCIATE SHEET No: of .**

(Example: Sheet 2 of 2. This would include this sheet plus one extra.)
Generic Reporting Form

Reporting Form: Page 4

Reason for suspicion

Use additional sheets if there are further details to be shown.
Analysis

Some of the important fields have been identified in the following templates. Let us discuss some of the issues related to the important fields in a reporting form.

<table>
<thead>
<tr>
<th>Generic Reporting Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Details of Disclosing organization:</td>
</tr>
<tr>
<td>Name of Organization*</td>
</tr>
<tr>
<td>Branch or Outlet</td>
</tr>
<tr>
<td>Business area of Branch Outlet</td>
</tr>
<tr>
<td>Your Disclosure Ref</td>
</tr>
<tr>
<td>Date disclosure sent to FIU</td>
</tr>
<tr>
<td>Has the subject been disclosed on a previous report?</td>
</tr>
</tbody>
</table>

1. Name of Organization*
2. Branch or Outlet
3. Business area of Branch Outlet
4. Your Disclosure Ref
5. Date disclosure sent to FIU
6. Has the subject been disclosed on a previous report?

*If this is the first report you have made complete a separate form to registering your appointed compliance / money laundering officer.

<table>
<thead>
<tr>
<th>Person subject of disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family name(s)</td>
</tr>
<tr>
<td>Title</td>
</tr>
<tr>
<td>Given Names(s)</td>
</tr>
<tr>
<td>Gender</td>
</tr>
<tr>
<td>Date of Birth</td>
</tr>
<tr>
<td>ID Document details</td>
</tr>
<tr>
<td>Address No. &amp; Street</td>
</tr>
<tr>
<td>City or Town</td>
</tr>
<tr>
<td>Region</td>
</tr>
<tr>
<td>Post or Zip Code</td>
</tr>
<tr>
<td>Country</td>
</tr>
<tr>
<td>Employer</td>
</tr>
<tr>
<td>Occupation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OR Company subject of disclosure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
</tr>
<tr>
<td>Company No</td>
</tr>
<tr>
<td>Tax Number</td>
</tr>
<tr>
<td>Type of Business</td>
</tr>
<tr>
<td>Country of Reg</td>
</tr>
<tr>
<td>1. Registered Office</td>
</tr>
<tr>
<td>Address No. &amp; Street</td>
</tr>
<tr>
<td>City or Town</td>
</tr>
<tr>
<td>Region</td>
</tr>
<tr>
<td>Post or Zip Code</td>
</tr>
<tr>
<td>Country</td>
</tr>
<tr>
<td>2. Trading Address</td>
</tr>
<tr>
<td>Address No. &amp; Street</td>
</tr>
<tr>
<td>City or Town</td>
</tr>
<tr>
<td>Region</td>
</tr>
<tr>
<td>Post or Zip Code</td>
</tr>
<tr>
<td>Country</td>
</tr>
</tbody>
</table>

| Other Information not in fields above |

Some of the issues that need to be considered on this sheet are:

1) Details of disclosing organization:
   - Information on the individual making the report may not be necessary and may infuse confidence in the financial sector because they will know that there will be no personal risk in making these reports. However, if the institution is making the reporting for the first time, it may need to register itself with the FIU.
   - Business area (such as retail banking, private banking, and so on) may be important to identify trend analysis and typologies, indicating the areas that have significant risks in money laundering and financing of terrorism (ML/FT).
- Date of disclosure to the FIU may be compared with the transaction date, the date the report reached the FIU to determine the efficiency of compliance at the financial institution, and other reasons of delay/disparity.
- Date of disclosure may be used by the FIU to monitor its own progress with the report.
- It does not matter if the underlying information was false as long as the financial institution did its customer due diligence (CDD). The fact that the information is false may indicate initiation of action.

2) Person subject of disclosure:
- Simple information such as name, title (which will indicate gender that may not be understood for foreign names), and date of birth can make the data unambiguous and be very helpful in the analysis of the reports.
- Name of employer can be significant because certain employment fields may have higher risk of ML/FT than others.

3) Company subject of disclosure:
- Once again, some business types may have a higher risk of ML/FT than others.

4) Other information:
- A field that encourages reporting entities to provide additional information that may not be captured in other fields.
5) Financial summary overview:
   - This is the snapshot of the account (account opening date, account closing date, if relevant) or any other business relationship that may indicate the priority of the investigation.
   - The snapshot of the account turnover may indicate the importance of the report, too.

6) Financial summary details:
   - As indicated above, the date of transaction in relation to the date of report and in relation to the date of receipt within the FIU can provide important inputs to the FIU.
   - Counterparty information can help FIUs to make comparative analysis with similar counterparties.
   - Once again, reporting entities should be encouraged to provide more reports.
7) Additional sheet:
- As indicated, information should not be omitted. If there is more information to be filled, use other sheets with appropriate numbering.

8) Information on associated persons:
- It is important to know the associated parties, such as the names of all the directors/signatories, and so on, to enable the FIUs to learn if the associated parties have been linked in other reports.

9) Reason for suspicion:
- The narrative section will allow reporting institutions to explain why they thought it suspicious behavior. It also helps the FIU understand the details of the transaction that were given in the previous sheets. You have seen this form as the last “Generic Reporting Form” in the exercise.

**Conclusions**

STR is an important form that gives information on what has been asked. The design of this form has to do with your analysis and the design of your database. It is important to hold dialogue with relevant stakeholders on the contents of
the STR form because information you are trying to capture is relevant to you and to the other stakeholders.

Here are some citations to examples of forms used in other countries:

- Lebanon: http://www.sic.gov.lb/downloads/STRe.doc
- United Kingdom: http://www.ncis.gov.uk/disclosure.asp

**Content of other types of reports**

You may choose to collect other reports, in addition to the STR. Consider how those reports will be collected and analyzed. You may wish to consider adapting the STR to achieve this. See Appendix D for a discussion on this issue. The form can be adapted, by changing field titles, to enable reporting across different financial institutions and DNFBPs. The more standardized the underlying data, the quicker and easier input, manipulation, and analysis of the data will be. A cosmetic change of field name does not affect the underlying data process. For example, “Credit” for a bank becomes “Drop” in a casino and “Deposit” in a property purchase.

**Receipt in what form?**

Having decided what type of reports your FIU will receive and the data to be collected in that report, you must now consider how you will receive the report.

**Knowledge check**

**QUESTION 16.** List different ways for receiving STRs and other information at the FIU. Consider the advantages and disadvantages of each method of receipt.

---

**Guidance**

FATF Recommendation 25 calls on the FIU or another competent authority to provide financial institutions and other reporting parties with guidance regarding the manner of reporting, including the specification of reporting forms, and the procedures to be followed when making a report. For more information on Recommendation 25, see Appendix E.
2.2 Analysis

Analysis is one part of a process called the “intelligence cycle,” which also encapsulates the overall STR process.

The stages in the intelligence cycle are:

Direction: The AML/CFT reporting regime provides direction by specifying reporting requirements (STRs, currency reports, and so on).

Collection: Methods of collection may vary for different types of institutions and different types of reports.

Evaluation: Different types of information have different priorities. Accurate assignment of priority helps us make the most of information.

Analysis: Analysis is done to produce results for dissemination. The product of analysis may be an internal report or a report to law enforcement authority or any other competent authority.

Dissemination: When the customer (an LEA, for example) is satisfied, the intelligence cycle ends. Or it may begin anew—to collect missing data.

The intelligence cycle is often employed without being recognized as a formal process. For successful treatment of STRs and other reports, however, the process must be formalized through the adoption of standard operating procedures.
It is helpful to remember what we mean by analysis. A widely acknowledged definition is “the assembly of information from diverse sources to show pattern and meaning.” A key part of the success of the FIU’s analytical function, therefore, must be identifying, accessing, and using diverse sources.

Analysis takes two forms: tactical and strategic.

### 2.2.1 Tactical Analysis

Tactical analysis is generally associated with the collection of data—in this case STRs and other reports—and comparing those data with other data already held by the FIU and other information and intelligence available to the FIU from public or private sector sources or from their foreign counterparts. This form of analysis tends to be case specific (that is, pertaining to a particular subject or group) and seeks to prove or rule out its association with certain criminal behavior—money laundering, terrorist financing, or a predicate crime. The analyst forms hypotheses and inferences based on the evaluation and analysis of the data to assist the FIU and/or LEA in identifying activity patterns, new targets, relationships among the suspect and accomplices, investigative leads, criminal profiles, and so on.

### 2.2.2 Strategic Analysis

Strategic analysis is the process of developing knowledge (“strategic intelligence”) to be used in shaping the work of the FIU in the future. The main characteristic of strategic intelligence is that it is not related to individual cases, but rather to new issues and trends. The scope of any strategic analysis may be narrow or wide, as required; it may consist of the identification of evolving criminal patterns in a particular group or the provision of broad insights into emerging patterns of criminality at the national level to support the development of a strategic plan for the FIU.

Strategic intelligence is developed after all available information has been collected and analyzed. It requires a wider range of data and experience than tactical analysis does. The data come from reports provided by the reporting entities, the FIU’s own operational intelligence and tactical information, public sources, law enforcement, and other government agencies. The analyst may conclude from the data that, for example, an unusual pattern or volume of transactions is emerging in a certain reporting sector or region. Such findings may form the basis for further actions by the FIU, the law enforcement agencies, or regulatory/supervisory bodies. At a broader level, strategic intelligence may suggest the need to impose reporting and other obligations on new entities. Depending on the circumstances, strategic intelligence may be shared with other law enforcement agencies, the government agencies charged with the development or coordination of AML/CFT policy, as well as with the regulatory/supervisory bodies.

In the sections that follow, we will encounter various forms of tactical and strategic analysis.
2.2.3 Analyzing STRs and other information

Knowledge check

QUESTION 17. Taking for granted that new reports will be compared against existing reports held in the FIU, list other public sector or government agencies whose data and information would be useful for analysis purposes.

Where data from public/government sources are available in a format usable by the FIU, comparative analysis with STR information should be undertaken to enhance STRs. However, comparative analysis is not the only form of analysis. Other forms of information and intelligence should be sought to help structure the analytical process. Computers, while they speed processes considerably, should not be sole tool of analysis. Invest, too, in building staff members’ capacity for analysis.

Using experience gained in previous cases, FIU staff can perform initial or subsequent screenings of reports against known domestic and/or international typologies. Equally important are briefings from law enforcement and the security/intelligence services on their experience and current priorities. These additional processes can assist in identifying reports for dissemination at an early stage. Even if STR subjects are not already known to law enforcement, their patterns of behavior may resemble methods of operation known to be used by criminal or terrorist groups.

At the conclusion of the initial research process, all available data should be reassessed and a decision made whether the report, in its enhanced form, needs further research or is suitable for dissemination. Reassessment may involve further research within the FIU or the acquisition of further information from reporting entities or from other domestic and foreign agencies.
See below a discussion on the “FIU Analytical Process.”

**Simple STR (and other info) process/analysis**

Let’s build from our simple model...

1. Receipt
2. Analysis
3. Dissemination

**Analytical Screening/Database Analysis**

Receipt of STR & other reports

The first figure is the simple STR process that we already discussed. The second diagram explains the analytical screening/database analysis process built on the first simple model.
Analytical screening

This is the first stage of analysis, which can be quite important before the database actually takes command of the data. One may consider manual intervention at this stage. But to undertake this successfully, the FIU needs to be conversant with what the priority projects are for the FIU and its customer—and the customer in this case is the law enforcement agencies. The customer may also be the police or the FIU itself; it may be the tax authority (customs or revenue); or it may be the security department in terrorism.

For example, assume that an LEA is looking at a certain ethnic group, transmitting money in a certain way. Now, it may not be known whether there is a certain name involved and/or it may be known whether there is a specific geographical location or an address. The database itself will not be able to do comparative analysis and extract useful information unless it is a very complex database. So one of the ways of dealing with this is to ensure your staff is properly informed as to what are of higher priority to enable him or her to do the analytical screening.

Database analysis

The FIU may do a comparative analysis of not only what is within the database of STRs but also compare it against external sources of information. Once again, the outcome of this needs to be prioritized—determine what and whose that priority is.

The issue of prioritizing becomes more important as the system develops and grows, the FIU gets more and more reports, and the database results are higher. It is important for the FIU to populate its database with information that is more valuable.

2.2.4 FIU SUPPORT FOR LAW ENFORCEMENT OPERATIONS

The same analytical processes can be used by the FIU to support law enforcement operations. Where LEAs are investigating predicate crimes or money laundering itself (if the LEA is the competent body to investigate money laundering), the addition of STR information can be of tremendous assistance, whether or not an STR was the starting point for their investigation. Requests for assistance from an LEA must show that the agency has a bona fide and lawful reason for requesting FIU support and must contain sufficient information to enable the FIU to search its database. (Access to STR information and confidentiality will be discussed later in the module.) The FIU will then follow the same analytical processes as if the request had originated as an STR.
2.2.5 **Statistical Information and Its Analysis**

Gathering and presenting statistics are important tasks of any FIU. Statistical information, properly analyzed, can be a valuable tool to the FIU, investigators, and policy makers alike.

Let us discuss some of the issues related to statistical information and analysis by analyzing some charts and diagrams.

### Issues to consider

- What caused the movement in the number of STRs?
- Is the change because reporting entities have a better understanding of the reporting mechanisms, or is it because reporting entities want to report more in order to avoid regulatory scrutiny (a quality vs. quantity issue)?

It is important to understand the reasons for the change to determine the actions that may be required.
### What do these figures/changes mean?

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Banks</td>
<td>3,401</td>
<td>17</td>
<td>2,997</td>
<td>12</td>
<td>3,790</td>
<td>13</td>
<td>50</td>
</tr>
<tr>
<td>Bureaux</td>
<td>98</td>
<td>3</td>
<td>527</td>
<td>12</td>
<td>699</td>
<td>7</td>
<td>17</td>
</tr>
<tr>
<td>Mutual Societies</td>
<td>425</td>
<td>19</td>
<td>442</td>
<td>20</td>
<td>699</td>
<td>7</td>
<td>23</td>
</tr>
<tr>
<td>Money Tran</td>
<td>98</td>
<td>1</td>
<td>201</td>
<td>4</td>
<td>372</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>Insurance</td>
<td>406</td>
<td>7</td>
<td>379</td>
<td>7</td>
<td>222</td>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>High value</td>
<td>12</td>
<td>4</td>
<td>99</td>
<td>7</td>
<td>119</td>
<td>9</td>
<td>102</td>
</tr>
<tr>
<td>Casinos</td>
<td>1</td>
<td>1</td>
<td>71</td>
<td>1</td>
<td>85</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Lawyers</td>
<td>2</td>
<td>1</td>
<td>68</td>
<td>21</td>
<td>77</td>
<td>26</td>
<td>274</td>
</tr>
<tr>
<td>Mortgage Providers</td>
<td>58</td>
<td>5</td>
<td>142</td>
<td>10</td>
<td>64</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Asset Mgmt</td>
<td>21</td>
<td>1</td>
<td>44</td>
<td>1</td>
<td>50</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Accountant</td>
<td>7</td>
<td>2</td>
<td>78</td>
<td>5</td>
<td>40</td>
<td>4</td>
<td>359</td>
</tr>
<tr>
<td>Financial Advisors</td>
<td>17</td>
<td>1</td>
<td>21</td>
<td>2</td>
<td>29</td>
<td>2</td>
<td>421</td>
</tr>
<tr>
<td>Cheque Cashers</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Regulator(s)</td>
<td>37</td>
<td>3</td>
<td>24</td>
<td>3</td>
<td>9</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Motor Dealers</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
<td>7</td>
<td>7</td>
<td>1,378</td>
</tr>
<tr>
<td>Credit Union</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>326</td>
</tr>
<tr>
<td>Equities Markets</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Auction Houses</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>29</td>
</tr>
<tr>
<td>Other STR</td>
<td>122</td>
<td>x</td>
<td>145</td>
<td>x</td>
<td>117</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>STR Number by year</td>
<td>4,708</td>
<td>5,251</td>
<td>6,125</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The above two graphs show the shift in terms of discrete business sectors. The issues to consider here are:

- Why is the reporting in the banking sector going up although that in the insurance sector is static or in decline?
- Is regulation of the sectors responsible for the reporting pattern?
- Once again, the quality of reports will matter more than the actual number.

This diagram shows the geographical spread of reporting. The issues to consider are:

- This kind of analysis may allow the FIU to determine the spread between commercial centers and agriculture centers (all units will have comparable financial size).
- Why is there a disparity between the centers? Is it because of lack of training or the location of compliance offices or corruption within the institutions?

Once again, it is important for the FIU to understand these factors to determine the trends and patterns of suspicious activities.

Understand how important the reporting format for making these analyses is. Unless data fields require the reporting entities to provide the information on business sectors, geographical location, and so on, such analyses cannot be done.

The types of statistics that FIUs must gather and retain are examined in section 2.4.1.
2.2.6 Analysis of Feedback

Analysis of raw STRs should not be the end of the analytical process, particularly if one is looking for national or international trends and typologies. The FIU should provide feedback to LEAs, regulators, and security/intelligence services that contribute to FIU analyses to build a national perspective on money laundering and terrorist financing and on the strengths and weaknesses of the current AML/CFT regime. The result of the FIU’s domestic trend analysis should be fed to your FATF (or FSRB) representative and to the international community for inclusion in their typologies. (Feedback will be examined later in this module.) FATF and FSRB typologies will not be covered in this module, but you can learn more from the FATF and Asia/Pacific Group on Money Laundering Web sites.4

2.3 Dissemination

The third core function of an FIU is the dissemination of the information it has received and the sharing of the results of its analysis. The ability of an FIU to quickly share reliable financial intelligence and related information with domestic and foreign authorities is critical to the success of its mission. Because funds move quickly in and out of financial institutions and across national boundaries, an FIU must be able to provide, as rapidly as possible, its information to competent authorities for purposes of criminal law enforcement. An FIU’s ability to share valid information quickly affects not only the effectiveness of a country’s internal AML/CFT regime, but also its ability to cooperate internationally.

Knowledge check

QUESTION 18. Who are the consumers or users of the information your FIU disseminates? Please list.

QUESTION 19. Having identified the probable consumers of your disseminated products, you should now consider what each of those consumers may require. Does every consumer require the same type of product? Write a sentence or two justifying your choice.

________________________________________________________________________

________________________________________________________________________

QUESTION 20. List one or two specific requirements of each of the consumers of the FIU information.

________________________________________________________________________

________________________________________________________________________

2.4 Other FIU functions

Earlier we briefly looked at other functions an FIU might undertake. We will examine these in a little more depth.

2.4.1 Statistics

One of the other functions of an FIU is the compilation and production of statistical information. Statistical data can help you evaluate the overall efficiency of your AML/CFT regime.

Knowledge check

QUESTION 21. Having looked at various issues surrounding the FIU, what statistical information do you believe would help the FIU and others to measure the effectiveness of the AML/CFT regime?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
2.4.2 Feedback

A common problem in national AML/CFT regimes is poor feedback to interested parties. The FATF covers the need to provide feedback in Recommendation 25. Among the competent authorities obliged by the FATF to provide feedback, the FIU is the one with the most contact with reporting entities, where feedback is generally in high demand. The issues surrounding feedback resemble those surrounding receipt of information: feedback of what, from whom, and in what format? For more information on Recommendation 25, see Appendix E.

Knowledge check

QUESTION 22. An FIU should be able to provide several types of feedback. List some different forms. Compare them with the list in the answer.

As you learned in section 2.1, the STR form and other reporting instruments are an important source of feedback data. But they are not the only source.

How will you capture the feedback information described in the previous answer? It is very important that you consider these issues at this stage, as any recommendations you make regarding feedback and how to collect and disseminate it will affect the design and use of the FIU database.

Knowledge check

QUESTION 23. Write down your ideas on how to capture the above information from other competent authorities. After doing this, compare your answer with the comment provided.
QUESTION 24. Should feedback received by the FIU from other competent authorities be the same feedback you provide to reporting institutions? Write a sentence or two justifying your choice below before reviewing the answer.

2.4.3 Training

While training is not a core function of FIUs, it has, in one form or another, generally fallen to nearly every established FIU in the world. From your work in this module you will have gained an appreciation of the unique position the FIU has in the country’s AML/CFT regime. AML and CFT are dynamic subjects, as is the development of a country’s AML/CFT regime. One of the best tools available to manage those dynamics is training.

For discussion

In what areas do you think the FIU may be well placed to provide training? Exclude, for the moment, training of its own staff. Note your response in the following space before reviewing the comments.
Areas in which the FIU may provide training

As a repository of specialized, multidisciplinary expertise, the FIU may be well qualified to advise and train reporting entity and government agency personnel in many aspects of AML/CFT—including those listed below.

Roles in the AML/CFT framework

The FIU sits somewhere in the middle of the overall AML/CFT regime. Explaining its role and interaction with other agencies/departments, financial institutions, and DNFBPs can be of mutual benefit. The FIU will generally have experience in certain areas of analysis, financial systems, and specialist AML/CFT laws and regulations. Sharing this knowledge can improve other players’ ability to fight money laundering and terrorist financing. The greater the understanding, the better the cooperation you are likely to obtain from other players.

Reporting procedures

The quality of data can be improved by training financial institutions and DNFBPs to complete STRs and other reporting instruments. Reporting entities can benefit from guidance on preparation of forms and on problems encountered by the FIU due to improperly completed forms. Be sure to include good examples as well as bad.

Analysis and feedback

The presentation of analysis, statistics, trends, and typologies benefits all parties in the AML/CFT regime, as does feedback. Remember that different audiences need different levels of detail. Tailor your presentation to your audience. Depending on the skill set and availability of FIU staff, the FIU may consider training other competent authorities in analytical techniques.

Understanding financial information

The FIU often develops institutional experience in the interpretation of a range of financial products. Sharing that experience with LEAs and prosecutors can improve their use of the information produced by the FIU.

2.4.4 Regulation of AML/CFT Systems and Controls

Regulation of AML/CFT systems and controls is not a core function of an FIU, but it must be handled by a competent authority. The FATF expects the FIU (or another competent authority) to provide guidance on reporting requirements and to oversee and ensure compliance with required systems and controls in financial institutions and DNFBPs.

Ask yourself whether your FIU is the institution best placed to assume this function in your country. Does your staff have the necessary skills? Do they have the time? What implications will it have on the core functions of the unit? Would this work duplicate or overlap that of other agencies or departments?

You might also ask how skills of regulatory staff could be best used within the FIU. Such skills may be most effective if used to advise regulatory and supervisory bodies and act as liaison between the FIU and those bodies. Consult Modules 3a and 3b for a detailed treatment of regulatory and supervisory requirements.
2.4.5 INVESTIGATIVE/JUDICIAL INQUIRIES

Judicial investigations are not a core function of the FIU, as defined by the FATF or the Egmont Group. However, some FIUs do have this function.

As with regulatory systems and controls, you must consider whether your FIU is the institution best placed to assume these additional functions, in addition to its core functions (receipt, analysis, and dissemination). What specialized skills are necessary to undertake investigative/judicial inquiries? What additional staffing and resources would the FIU need? Would the FIU carry out surveillance and other investigative actions? Would FIU personnel prosecute at trials?

Again, should these skills and staff be part of the FIU as a core function? That is, should the FIU employ active investigators and prosecutors? Or would they be more effective if used to advise external investigative and judicial bodies in AML/CFT matters?

2.4.6 POSTPONING OF SUSPICIOUS TRANSACTIONS

In many countries the FIUs also have a power to postpone or suspend a transaction when there is a suspicion that a transaction is related to money laundering or terrorist financing. The objective of this unique measure is to give the FIU sufficient time to analyze the transaction, and if, after analysis, the conclusion is reached that the transaction is indeed related to ML/FT, the FIU shall transmit the file to the proper law enforcement or judicial authority that has the power to freeze the transaction for a longer period.

The maximum duration of such measure is determined by national law, and, in most cases, it is 72 hours. However, in some countries, for example, Luxemburg, South Africa, Ukraine, and Thailand, the maximum postponing period can be extended to five or more days.

The authority to postpone a suspicious transaction only makes sense when the disclosures of suspicious transactions are made before execution can occur. It is important that the entity reporting a suspicious transaction to the FIU indicates the time it needs to carry out the transaction.

As regards the international standards, the postponement of suspicious transactions is only regulated as a special measure by the 2005 Council of Europe Convention on laundering, search, seizure, and confiscation of the proceeds from crime, and on the financing of terrorism (the Warsaw Convention). Article 14 of the convention requires countries to adopt such legislative and other measures as may be necessary to postpone domestic suspicious transactions; Article 47 deals with the international cooperation among FIUs for postponement of suspicious transactions. Although 28 countries have already signed and 4 countries have ratified the convention, this treaty is not yet in force because of the missing minimum number of 6 required ratifications.
This section will focus on coordination and cooperation between the FIU and other competent authorities. Module 5 will discuss interagency and international cooperation.

### 3.1 Domestic

Money may change hands and move around the world at the speed of an electronic wire transfer. For that reason, law enforcement agencies and prosecutors that investigate money laundering and financing of terrorism must be able to count on a virtually immediate exchange of information. The FIU, therefore, needs to be able to coordinate and cooperate with other domestic authorities.

---

*This diagram is representative only; other sectors may be included.*
At a policy level, the FIU either should be represented at, or be in a position to fully brief, the high-level national AML/CFT policy committee. It also should be in a position to inform relevant government departments about AML/CFT, and to assist in the formulation of government policies that overlap or interact with AML/CFT requirements. A similar policy dialogue should occur with law enforcement and regulatory agencies active in relevant areas. Mutual expectations among the departments should be spelled out and formal protocols for cooperation, where necessary, adopted.

The FIU is well placed to assist in matters of domestic coordination among competent authorities. It may even take the lead in the fight against money laundering and terrorist financing in the country. It is important to note that the type of role being considered here is that of coordination and not of one such as policy development, which should remain with the appropriate competent body.

In our discussion of the analysis function, we noted the need for information and intelligence from other domestic agencies. We also considered the dissemination of different information to different bodies at different times, noting that dissemination covers a wide range of information, from a single STR to support for major law enforcement operations, right through to policy issues. We also discussed the need for the FIU to receive feedback from various bodies.

**Cooperation and access to financial intelligence**

The model is still being broken into three stages but with different headings. These headings are important to understand as they often determine how the data passed to each body can and will be handled:

- **Information**: is only a report of suspicious behavior not necessarily criminal behavior.
- **Intelligence**: Having gone through the intelligence process, it is something deemed actionable by the LEA. The FIU role** is generally not to gather material in a format usable for or in judicial proceedings.
- **Evidence**: Is turning the the product of “intelligence” into form and format usable in a judicial proceeding.

**Internationally, with some exceptions, the FIU does not usually undertake the investigative function itself.**
Domestic cooperation can be best achieved where mutual sharing of information between agencies and departments is legally authorized, where such cooperation is explicitly endorsed by the intergovernmental group overseeing AML/CFT, and where the nature and extent of cooperation is reported to and reviewed by that group. For the AML/CFT regime to achieve its maximum potential, these domestic relationships need to be clearly understood by all players. Where necessary, formal arrangements for cooperation should be established.

3.2 International

International cooperation is equally important to the FIU. Without international cooperation, an FIU is not able to fully exploit an STR that contains international counterparts, or to access information related to foreign nationals, addresses, and accounts mentioned in an STR or to which an STR might point. In addition to such operational imperatives, understanding and contributing to international trends and typologies depends on good international cooperation.

Information should be shared with competent foreign authorities through the most efficient means available and, where possible, be done directly and by means of secure communications.

As with domestic cooperation, appropriate legal gateways must allow for the sharing of FIU information and analysis with relevant international counter-
parts. While a free flow of information is to be encouraged, there must be an understanding of what is being exchanged, for what purpose, and how it will be protected from unauthorized use, as well as how it will be used by the recipient.

The key to such an understanding is knowledge of the difference among information, intelligence, and evidence. FIUs are normally involved only in the sharing of information and intelligence (“information” might be an original STR report, while “intelligence” is the result of the analysis done on the report by the FIU). The sharing and subsequent use of information and intelligence are subject to less exacting conditions than are documents and other material that could be produced as evidence.

FATF Recommendation 40 deals with international cooperation. See Appendix G for further details on Recommendation 40.

A diagram to illustrate the concept is given below.
3.3 Cooperation and access to financial intelligence

3.3.1 Domestic

Coordination and cooperation, as we have just discussed, are essential to the prevention and detection of money laundering and terrorist financing. Yet there are limits to the sharing of information. Remember that an STR is a report of suspicious behavior and not, in itself, an allegation of criminal behavior. It should be treated accordingly. Proper safeguards should be built into the system to ensure that recipients of the information have the need to know (not just a desire to know) and are bound by appropriate standards of confidentiality.

“"For discussion"

Read the examples of appropriate limits on access to financial intelligence. Comment on the examples provided.

Limits on access to financial intelligence

A public servant receives his monthly salary into his bank account each month and occasionally other very small payments; this has been the consistent pattern of his account and is considered normal by his bank. The public servant suddenly receives a substantial amount of funds into his account from a foreign jurisdiction—this amount is completely out of character, significantly large, and from a jurisdiction seemingly unconnected to the customer. When examined by the bank, the transaction is not consistent with the customer's occupation and not similar to any previous dealings/transactions the bank has ever seen. The bank rightly makes a report to the FIU. Without looking in detail at the analysis process at the moment, who should be able to access this report and why?

What if the genuine explanation was the following: Unbeknown to the bank, a close member of the customer's family, who has lived abroad for many years, had just died. The money earned by the close relative during her life was legitimate and all the taxes had been properly paid. After death, all the estate's affairs were fully in order (including tax) and the customer was to inherit a considerable portion of the funds. Does this alter your decision as to who should be able to have access to this report now?

What if the genuine explanation was this: Law enforcement (together with the public prosecutor, depending on the jurisdiction) was conducting a corruption investigation into payments being made by a large construction firm for that firm to secure contracts (above other construction firms) from the government to undertake projects. Knowing this, who should have access to this information now?

What if the analysis was inconclusive and a law enforcement officer called the FIU and said that he was conducting a corruption inquiry but in truth he was corrupt himself? His intention was to gain information on behalf of the opposition political party to use to embarrass, where possible, current public officials, for which he would receive
3.3.2 International

We have discussed domestic sharing and why some restrictions may have to be put in place to control the release of information. We also discussed the need for international sharing of information, focusing on cooperation between FIUs.

Knowledge check

QUESTION 25. When attempting to access information internationally, why use the FIU as the contact point?
One way to achieve international cooperation and to understand the circumstances and requirements of other FIUs (under their domestic law) is to come to an agreement or understanding, ideally in writing. Many FIUs establish memoranda of understanding (MOU) with their international counterpart FIUs to outline the terms and conditions of information exchange, as well as controls and restrictions on exchanged information. The Egmont Group has provided guidelines\(^5\) for the exchange of information between FIUs. Many FIUs use these guidelines as the basis for creating their own MOU but incorporate requirements particular to their domestic legislation or priorities. Ultimately, the understandings between any FIUs depend upon the laws and requirements of their respective counterparts.

### 3.3.3 Is a Formal Agreement or Understanding Necessary Between FIUs?

The answer depends mainly on the law in each country. Legal conditions on international exchanges of information vary widely throughout the world. Some FIUs are required by domestic legislation to establish MOU; whereas others are able to exchange information simultaneously or upon request. In some cases, FIUs lack the authority to establish understandings with their international counterparts.

In establishing your FIU’s policy on international information exchange, consider the following issues:

- Imagine that you want to transmit an urgent STR inquiry to another country, but your legislation requires a prior agreement with that country. Will the transmission have to wait until an agreement is signed? Conversely, what if the counterpart FIU has an urgent request from you, but prior agreement is required? What happens to the case in the meantime?
- What legal requirements are placed on your FIU? Many nations impose requirements on information security, use of exchanged information for intelligence only, reciprocity, establishment of agreements between nations, or prior authorization for exchanges by the head of the FIU, a minister, or another authority. Establishing international understandings needs to be in line with your domestic obligations.
- Ideally, your domestic legislation will permit the exchange of intelligence quickly and efficiently. The more restrictive your law on sharing, the less effective your overall AML/CFT regime will be.
- Confidentiality and sharing requirements should be drafted in a way that does not inhibit international cooperation among FIUs. The ideal case is where a FIU can undertake research for another FIU/counterpart body on a case-by-case basis without the need to revert to a formal agreement.

---

• If your FIU is not required to establish an MOU, consider how you will communicate with FIUs that do require an MOU. Does your FIU have the authority to enter into an MOU?
• Where exchanges are frequent between two FIUs that operate different systems, an agreement or understanding may well be a useful tool to monitor compliance and the effectiveness of the relationship. But, the agreement should be broad enough so as not to inhibit international cooperation between FIUs; and it should not be so restrictive that constant amendments are necessary as AML/CFT systems develop and change.
• If your FIU has an investigative or prosecutorial function, you may find that other FIUs are limited in their ability to share with you.
• Special conditions imposed by domestic law on the exchange of information should be acknowledged in any agreement or understanding. They should be drafted as broadly as possible, so as not to inhibit international cooperation among FIUs.

Where an agreement is found to be necessary, consider the Egmont Group’s guidelines for the exchange of information between FIUs.

Some of the above issues have been discussed with the following illustrations on international cooperation and access.

Cooperation and access to financial intelligence

You will recognize this from the beginning of this module.

For sharing purposes we need to break this down in a slightly different way...

You will recognize the above schematic from an earlier section. It is an illustration of the simple process dealing with receipt, analysis, and dissemination of information. Although we use those headings for simplicity, they have other implications, depending on how the FIU is designed to work and when and how the FIU interacts with law enforcement and the prosecutor. Information and intelligence is what the FIU’s business is all about.
The FIU has undertaken the analysis work; it has produced some of the report that is generally characterized as “intelligence,” to which law enforcement will react. Some FIUs have the authority to undertake the investigative part of the process. Other countries leave the investigative aspects to the LEAs. Based on this information, law enforcement obtains information and other material through mechanisms that are available to them in a form that can be used in and for judicial purposes. Intelligence generally is pointing out the direction law enforcement should take but not undertaking that function for them. But there is a clear division between intelligence and evidence gathering. The lines are dotted because they can move in different directions depending on the functionality given to the FIU and law enforcement. Simplistically, the division would sit here. You have decided what the FIU will do, what the law enforcement will do, and what function the prosecutor will take. It will often be prescribed to local law or to an administrative process. However, an FIU needs to cooperate and work with its counterparts to have maximum benefit in the international arena.
Look at the next chart in relation to this, and you find the line has become very skewed. Where do you draw the line? In your jurisdiction, where is the line? You know well about your jurisdiction because you defined it in the law. This may not be the case when you deal with your counterparts. It may be that your counterpart FIU is a law enforcement FIU and it undertakes the evidence part of the work. It may be that their prosecutors are in the office and are directly involved in judicial process. It may be that they undertake a traditional FIU function, which is only the analysis and intelligence process.

Issues that need to be considered:

- How will information be handled and by whom?
- Are you comfortable with it?
- Is it conversant with the laws of your country?
- Is it conversant with the general principles of human rights and freedom of information?
- How do these reconcile?

They can be reconciled. The important issue is to know what your counterparty does. You should not come into a situation where you cannot share with your counterparty. It is contrary to the good use of any STR process and to the international recommendations, but understanding how they are going to work with it can help you decide what and where and when to make this information available, or through what processes it should be made available.
3.4 The Egmont Group

Background to the Egmont Group of Financial Intelligence Units

In June 1995, government agencies and international organizations gathered at the Egmont-Arenberg Palace in Brussels to discuss ways to confront the global problem of money laundering. Out of this first meeting was born the Egmont Group, an international body whose members share common goals. The Egmont Group provides a forum for FIUs to improve mutual cooperation to detect and combat money laundering and, more recently, terrorist financing. This includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of the FIUs’ personnel, and fostering better communication among FIUs through application of technology.

Currently, the organizational structure of the Egmont Group is the following: the Secretariat with the headquarters in Toronto; the Egmont Committee, which serves as the consultation and coordination mechanism for the heads of FIUs; and five working groups—legal, training, information technology, outreach, and operational.

The Egmont Group’s primary focus is the FIU’s role in fighting money laundering and terrorist financing. As a result of the new Egmont Group definition of an FIU (see below), many countries have amended or are in a process of amending their domestic legislation to include combating of terrorist financing among the core functions of their FIUs.

The Egmont Group established the definition of an FIU in 1996, but amended the definition in 2004 to reflect the FIU’s role in combating terrorist financing. The definition of an FIU is now the following:

A central, national agency responsible for receiving (and, as permitted, requesting), analyzing, and disseminating to the competent authorities disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money laundering and terrorist financing.

4.1 What skills do FIU personnel need?

FATF Recommendation 30 addresses the importance of adequate financial, human, and technical resources provided to competent authority. Some of those skills and resources should have become apparent in this module. For further information on Recommendation 30, see Appendix H.

Knowledge check

Question 26. What knowledge or skills do you see as necessary for FIU personnel? (Exclude management skills for the time being.) After you provide your comments in the following space, review the answer provided.

4.2 Where will you find the initial personnel for your FIU?

You have various options available:

- Recruit permanent staff or secondments (temporary transfers) from other public sector agencies and departments.
- Recruit directly from universities or parts of the private sector.
- Recruit from reporting entities or other nongovernmental organizations (NGOs).
- Seek secondments from international organizations, FSRBs, and established FIUs in your region.

The international consensus is that the FIU staff should reflect a mixture of skills necessary to undertake the three core functions of receipt, analysis, and dissemination. If your FIU will assume the functions of regulation, supervision, investigation, or prosecution, you will need skills that could be found in other agencies (regulators, supervisors, investigators, and prosecutors). Will your FIU be able to recruit those skills while maintaining the core functions? Does this affect your decision making about what functions to place within the FIU?
4.3 What issues do “mixed” staff bring with them?

If the staff will be drawn from various agencies, will all become permanent employees of the FIU or will some staff be seconded by their employers? Some of the issues that need to be considered are:

- Who will be in charge? Which agency will lead? (See section 5)
- How will you integrate different rank and pay structures?
- How do pay and ranking fit into the new FIU structure?
- How do you prevent conflicts of interest with the parent organization?
- Who is responsible for disciplining seconded staff for their work within the FIU?
- What happens to the pensions of transferred staff?
- What happens when a seconded staff returns to the parent organization?
- How will seconded staff keep up with career prospects within their parent organization?
- How will you build expertise among personnel?
- How will training and knowledge transfer occur and be maintained, particularly where officers are seconded and return to their parent organization?

Knowledge check

**QUESTION 27.** Can you suggest ways to minimize the risks posed by the issues raised above? Write down your responses and then review the suggestions in the answer.

4.4 Integrity

Whatever your personnel arrangements, the integrity of the FIU and its personnel are paramount if the FIU is to work with, and be trusted by, reporting institutions and other government agencies. Consider adopting:

- a confidentiality requirement governing the staff’s work in the FIU. The provision should complement the information-sharing process discussed in section 3;
- a disciplinary code that covers all personnel (including secondees) while they are with the FIU. The code should also oblige personnel who have left the FIU’s employment to maintain the confidentiality of information to which they had access while at the FIU;
• integrity checks on all personnel, regardless of background. This should be done at the time of recruitment and regularly thereafter;
• compulsory declarations of assets of staff members. Consideration should also be given to material changes in circumstances of those staff and their immediate family.

This list is designed to focus your attention on the important issue of integrity. It is not exhaustive.

Matters of integrity should be formally addressed in legislation and/or through a formal administrative process. Whichever route is taken, integrity issues must be clearly understood by prospective employees before commencing employment. That understanding should be refreshed during their employment, whether directly or through secondment, with the FIU.

4.5 Security

So far we have discussed how powerful financial intelligence and STR information can be in fighting money laundering and terrorist financing. Unfortunately, it can be as equally powerful in the wrong hands or where it is subject to misuse by the FIU or other staff associated with the FIU process. For these reasons, as with integrity, there can be no compromise on physical security—that is, in access to buildings and to the records of the FIU, paper or electronic. Equally important is staff discretion in discussing STRs or associated files or processes of the FIU.

Information security must be balanced with the efficiency of FIU systems and processes. Computer (or manual) systems should be subject to restricted access, but not so restrictive as to inhibit overall efficiency. The systems should be subject to both periodic and random review by properly agreed, understood, and enforced management processes.

Physical access should be restricted to staff. Other considerations include:

• Should visitors be prohibited from certain parts of or all buildings?
• Should visitors be escorted?
• Should certain areas be off limits to (unescorted) visitors?
• What information should visitors be allowed to see, copy, or remove?

Employment agreements must give effect to the need for confidentiality, discretion, integrity, and physical security. Staff should understand that they (and their visitors) may be subject to random searches by security staff.
The FIU should be protected by a disaster-recovery plan supported by the necessary infrastructure. The plan should address the following issues, among others:

- What happens when the electricity fails? What backup services (lights, security equipment, IT facilities) are necessary as a matter of safety and for minimum operations to continue? How quickly must the backup be operational?
- How (and how often) will the FIU’s data be backed up? Daily, weekly, monthly? Where will the backups be stored? How quickly can it be recovered if needed? Should the main server be mirrored as part of your backup plan? Where will the redundant server be located?
- What if the building and infrastructure incur serious damage (flooding, fire, earthquake, terrorist activity) that renders them unusable for some time? Does the FIU have a backup location? How quickly must that location be operational?
People charged with setting up an FIU often assume that the FIU must conform to another country’s model or that a particular department or agency should “own” the FIU without taking into account the duties and functions of the new unit.

Before deciding how the new FIU will fit into the current AML/CFT regime, study the full picture: core functions (and means of accomplishing them), additional functions, required skills, staff strength, sources of recruits, and so on.

The FATF, or any other international organization/body, does not dictate a particular type of FIU. But FATF Recommendations 26 and 30 do make some key points:

- The FIU may be an independent governmental authority or depend upon one or more existing authorities. Whatever the choice it must have sufficient operational independence and autonomy to ensure that it is free from undue influence or interference.
- The FIU must be a unified national unit that commands its own:
  - structure;
  - funding;
  - staffing; and
  - technical resources.

For discussion

Taking into account what you have learned in this module, where would your FIU be best placed?
Most FIUs fall into one of four categories:

- Administrative agency model
- Law enforcement model
- Judicial/prosecutorial model
- Hybrid model

The four models mentioned above have their advantages and disadvantages:

- The administrative agency model is a centralized, independent, administrative authority that receives and processes information from the financial sector and DNFBPs and transmits disclosures to judicial or law enforcement authorities for investigation and prosecution. It functions as a buffer between the financial sector and DNFBPs on one side and law enforcement on the other side.
- The law enforcement model implements anti-money laundering measures along with other laws, supporting the efforts of multiple judicial or police authorities with concurrent or sometimes competing jurisdiction over money laundering and financing of terrorism.
- The judicial/prosecutorial model is established within the judicial branch of government. When the country’s investigative agencies receive reports of suspicious financial activity, the judicial powers can be brought into play—seizing funds, freezing accounts, conducting interrogations, detaining suspects, conducting searches, and so on.

The hybrid model serves as a disclosure intermediary and a link to both judicial and law enforcement authorities. It combines elements of at least two of the FIU models.

Many FIUs combine the administrative model with some law enforcement and prosecutorial functions. When choosing a model, it is important to consider the relationship between relevant authorities and reporting entities in the country, as well as other unique economic and cultural circumstances. None of the models may work in “pure” form in a given country.

Whatever type of FIU you establish, the answer is not to mirror another country’s FIU but to establish one that best reflects the culture, economy, and other distinctive features of your country.
Knowledge check

QUESTION 28. Taking into account all the issues discussed in this module, briefly explain where and which type of FIU you would recommend to your National AML/CFT Committee or to your country’s policy makers.

Summary

- You considered where an FIU fits strategically into a country’s AML/CFT program.
- You examined its core functionality—receipt, analysis, and dissemination—and discussed other functions it might undertake.
- You went on to explore cooperation and coordination at the domestic and international levels.
- You considered how to balance the right to privacy with legitimate access to sensitive financial information.
- You explored integrity and staffing skills and structures.
- You then looked at how other FIUs have been formed and some advantages and disadvantages of each approach.
- Finally, you considered what might be right for your country.

Check your understanding

QUESTION 29. Reporting by financial institutions and DNFBPs should be made as simple and efficient as possible.

a) True   b) False

QUESTION 30. There are four basic models of FIUs: administrative agency model, law enforcement model, financial supervisory model, and judicial/prosecutorial model.

a) True   b) False

QUESTION 31. If domestic legislation permits the exchange of information quickly and efficiently, the MOU is not necessary for the communication between FIUs.

a) True   b) False
QUESTION 32. Feedback to other competent authorities is very important to improve domestic cooperation, but feedback to financial institutions and DNFBPs is not.

a) True    b) False

QUESTION 33. When a country sets up an FIU, the country should study and analyze the function of FIUs abroad and then imitate the selected country’s model.

a) True    b) False
Appendix A: References

FATF Recommendations

- The Forty Recommendations (FATF, June 2003)
  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- Special Recommendations on Terrorist Financing (FATF, October 2004)

Useful Web sites

- Conventions Against Terrorism (UNODC)
- Crime Conventions and related Resolutions/Drug Control Treaties and related Resolutions/Resolutions and Decisions (UNODC)
- Egmont Group
  http://www.egmontgroup.org/
- Overview—Conventions against Terrorism (UNODC)

Reference Documents

- Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (FATF, February 2004)
- Typologies Report 2004-2005 (FATF)
  http://www.fatf-gafi.org/findDocument/0,2350,en_32250379_32237235_1_32247552_1_l_1,00.html
- Financial Intelligence Units: An Overview (IMF/World Bank, 2004)
Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

**Interpretative Note to Recommendation 26**

Where a country has created a FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIUs.
Appendix C: Scope of the criminal offense of money laundering

FATF Recommendation 1

Countries should apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences. Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences, or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches.

Where countries apply a threshold approach, predicate offences should at a minimum comprise all offences that fall within the category of serious offenses under their national law or should include offences punishable by a maximum penalty of more than one year’s imprisonment or for those countries that have a minimum threshold for offenses in their legal system, predicate offences should comprise all offences, which are punished by a minimum penalty of more than six months imprisonment.

Whichever approach is adopted, each country should at a minimum include a range of offenses within each of the designated categories of offences.

Predicate offences for money laundering should extend to conduct that occurred in another country, which constitutes an offence in that country, and which would have constituted a predicate offence had it occurred domestically. Countries may provide that the only prerequisite is that the conduct would have constituted a predicate offence had it occurred domestically.

Countries may provide that the offence of money laundering does not apply to persons who committed the predicate offence, where this is required by fundamental principles of their domestic law.

For more on the predicate offenses of money laundering and terrorist financing, see Module 2, section 2.3.
In addition to STRs, there are several types of reports that may be submitted to the FIU relating to currency transaction, cross-border, cash movement, and monitor instrument movements, and so on. An FIU has to consider how it is going to capture this data and incorporate these in its database.

### Appendix D: Other types of transaction reports

#### Generic Reporting Form

<table>
<thead>
<tr>
<th>Details of disclosing organization</th>
<th>STR</th>
<th>X-Border</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Branch or outlet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business area of Branch Outlet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Your Disclosure Ref</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date disclosure sent to FIU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the subject been disclosed on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>previous ref, if so give previous</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIU Ref</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*If this is the first report you have made complete a separate form to registering your appointed compliance / money laundering officer.*

#### Person subject of disclosure:

- **Family Name**: 
- **Given Names(s)**: 
- **Date of Birth**: 
- **ID Document details**: 
- **City or Town**: 
- **Region**: 
- **Post or Zip Code**: 
- **Country**: 
- **Employer**: 
- **Occupation**: 

#### OR Company subject of disclosure:

- **Company Name**: 
- **Company No**: 
- **Tax Number**: 
- **Type of Business**: 
- **Country of Reg**: 
- **1 Registered Office**: 
  - **Address No. & Street**: 
  - **City or Town**: 
  - **Region**: 
  - **Post or Zip Code**: 
  - **Country**: 
- **2 Trading Address**: 
  - **Address No. & Street**: 
  - **City or Town**: 
  - **Region**: 
  - **Post or Zip Code**: 
  - **Country**: 

**Other Information not in fields above**
Different countries have approached this by different means. Some use entirely different forms to do it. It’s more convenient at the customs port to have a different form to complete, for example. Other may want to consider adapting the same form, which makes data capture and data manipulation within the FIU much easier to deal with.

This may need to be discussed with the stakeholders to see what will be the most convenient way to capture the data and that is convenient not only to them but for the FIU as well to produce an end product that is valuable to others.
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.

**Interpretative Note to Recommendation 25**

When considering the feedback that should be provided, countries should have regard to the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.
Appendix F: Recommendation 31

Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate, co-ordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.
Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

**Interpretative Note to Recommendation 40**

1. For the purposes of this Recommendation:

   “Counterparts” refers to authorities that exercise similar responsibilities and functions.

   “Competent authority” refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.
2. Depending on the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organizations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions to obtain relevant information.
Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.
If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

**Interpretative Note to Recommendation 13**

The reference to criminal activity in Recommendation 13 refers to:

a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or

b) at a minimum those offences that would constitute a predicate offence as required by Recommendation 1.

Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state inter alia that their transactions relate to tax matters.
The requirements set out in Recommendations 13 to 15, and 21 apply to all designated non-financial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals, and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12 (d). Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12 (e).

d) Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Interpretative Note to Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration, or mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.
Interpretative Note to Recommendations 5, 12, and 16

The designated thresholds for transactions (under Recommendations 5 and 12) are as follows:

- Financial institutions (for occasional customers under Recommendation 5)—USD/EUR 15,000.
- Casinos, including internet casinos (under Recommendation 12)—USD/EUR 3000.
- For dealers in precious metals and dealers in precious stones when engaged in any cash transaction (under Recommendations 12 and 16)—USD/EUR 15,000.

Financial transactions above a designated threshold include situations where the transaction is carried out in a single operation or in several operations that appear to be linked.
Countries should consider the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerized data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

Interpretative Note to Recommendation 19

1) To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, countries could consider the feasibility of subjecting all cross-border transfers, above a given threshold, to verification, administrative monitoring, declaration, or record-keeping requirements.

2) If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, and so forth, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should cooperate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.
Answers
Module 4 Answers

Answer 1
False. The FIU should be a national central body for financial intelligence. It would be ineffective and confusing to have more than one FIU in a country. Reporting institutions should file STRs to one national center of financial intelligence, which is an FIU.

Answer 2
False. There should be uniform STR form(s) used by all the reporting institutions. Otherwise, the FIU cannot process the STR quickly nor analyze the information effectively.

Answer 3
False. Core functions of FIUs are receipt, analysis, and dissemination of information.

Answer 4
False. Under FATF guidelines, reporting requirements may well extend beyond STRs. You will need to consider other forms. Recommendation 13 deals with STRs, which are the mainstay of an AML/CFT reporting regime. But you must also consider Recommendation 19 and the interpretative notes regarding cross-border transactions and currency transactions above defined thresholds, reports of which may produce valuable information. If you are not familiar with FATF Recommendations 13, 16, and 19, or with their Interpretative Notes and the glossary, as well as with FATF Special Recommendations IV and IX, review them before continuing.

Answer 5
False. An FIU may be placed in government ministries/agencies other than just the Central Bank. Each country should decide where it should be best placed.

Answer 6
Some of these agencies might include police, public prosecutors, state security agencies, financial sector supervisors/regulators, tax officials, customs officials, and intelligence services.
Answer 7

Definition: from the glossary of the FATF Forty Recommendations

“Financial institutions” means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public
2. Lending
3. Financial leasing
4. The transfer of money or value
5. Issuing and managing means of payment (e.g., credit and debit cards, checks, traveler’s checks, money orders and bankers’ drafts, electronic money)
6. Financial guarantees and commitments
7. Trading in:
   a. money market instruments (checks, bills, CDs, derivatives, and so on);
   b. foreign exchange;
   c. exchange, interest rate, and index instruments;
   d. transferable securities;
   e. commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues
9. Individual and collective portfolio management
10. Safekeeping and administration of cash or liquid securities on behalf of other persons
11. Otherwise investing, administering, or managing funds or money on behalf of other persons
12. Underwriting and placement of life insurance and other investment related insurance. This applies both to insurance undertakings and to insurance intermediaries (agents and brokers)
13. Money and currency changing

“Designated non-financial businesses and professions” means:

a) Casinos (which also includes Internet casinos)
b) Real estate agents
c) Dealers in precious metals
d) Dealers in precious stones
e) Lawyers, notaries, other independent legal professionals, and accountants—this refers to sole practitioners, partners, or employed professionals within

---

6 This also captures private banking.
7 This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfeiting).
8 This does not extend to financial leasing arrangements in relation to consumer products.
9 This applies to financial activity in both the formal or informal sector, for example, alternative remittance activity. See the Interpretative Note to Special Recommendation 6. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation 7.
professional firms. It is not meant to refer to “internal” professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.

f) “Trust and Company Service Providers” refers to all persons or businesses that are not covered elsewhere under these recommendations, and which as a business, provide any of the following services to third parties:

- Acting as a formation agent of legal persons
- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- Providing a registered office, business address or accommodation, correspondence, or administrative address for a company, a partnership, or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

(Reporting requirements for financial institutions and DNFBPs are also covered in modules 3a and 3b.)

**Answer 8**
The participants in an interdepartmental AML/CFT planning group would typically be drawn from the following agencies. Others may be included as appropriate.

- Ministry of:
  - Justice
  - Finance
  - Interior/Home Affairs
  - Trade and Commerce (if this ministry has a licensing, registration, or supervisory function over financial institutions and DNFBPs)

- Investigative/intelligence/prosecutorial agencies:
  - Police
  - General prosecutor’s office
  - Customs
  - Other agencies or task forces (as they apply): drugs, anticorruption, tax, organized crime
  - Security services
  - Intelligence agencies
  - Financial intelligence unit (where formed or in formation)

- Central bank
- Supervisors/regulators of other financial institutions
- Supervisory authorities of DNFBPs
- Representatives of financial institutions and DNFBPs
Answer 9

Definition: from the glossary of the FATF 40 Recommendations

Each country should at a minimum include a range of offenses within each of the designated categories of offenses:

- Participation in an organized criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint, and hostage-taking
- Robbery or theft
- Smuggling
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

Answer 10

Answer 11

- The interdepartmental governmental group
- Legislators and the legal system
- Law enforcement agencies
- Prosecutors, judiciary
- Financial sector regulators and supervisors
- Financial sector
Answer 12
The most important user of this document is you. The methodology sets out a framework for AML/CFT that allows you internally to build and test the effectiveness of your own regime.

It will also be used by the following bodies to assess countries’ AML/CFT regimes: World Bank, IMF, the FATF, and FATF-style regional bodies.

Answer 13
No. The three functions interact, so it is misleading to look at them in isolation. What is done in one area may affect the others. Consider the process as a whole. Policies and practices for receipt of information will depend on how and what you want to analyze. If you do not capture it, how can you analyze it? Having analyzed it, you need to consider what, if any, output (dissemination) there will be. Will the output of your analysis be sufficient for other agencies to take action? What are those other agencies? Do their needs differ? Does the intended output have implications for the data you should be capturing?

Answer 14
Answer: Financial institutions and DNFBPs. For further details, refer to FATF Recommendations 13 and 16, together with the associated Interpretative Notes and the glossary entries for financial institutions and DNFBPs. See Appendix I for Recommendation 13 and Appendix J for Recommendation 16.

Answer 15
No. Under FATF guidelines, reporting requirements may well extend beyond STRs. You will need to consider other forms.

Recommendation 13 and Special Recommendation 4 deal with STRs, which are the mainstay of an AML/CFT reporting regime. But you must also consider Recommendation 19 and the Interpretative Notes regarding currency transaction reports which may produce valuable information for the FIU. If you are not familiar with Recommendations 13, 16, and 19, or with their Interpretative Notes and the glossary, as well as with Special Recommendations 4 and 9, review them before continuing. See Appendix K for Recommendation 19.

Answer 16
- Personal visit to the FIU
- By telephone to the FIU
- Paper report, by post
- Fax
- E-mail
- Internet (or other Web-based technology)
- Dedicated link between a particular reporting entity and the FIU (for high-volume reporters)
Some advantages and disadvantages of various methods:

- **Personal visits to the FIU**
  - Who will receive the reports?
  - Is it logistically feasible for a person to receive the reports? (The answer will depend upon the frequency of submission.)
  - What issues of security and access to information are posed?

- **By telephone to the FIU**
  - Convenient but open to ambiguity and conflict, unless conversations are recorded

- **Paper report, by post**
  - Slow to arrive and time-consuming to process
  - Post may be insecure

- **Fax**
  - Quicker than post
  - Data must be rekeyed, raising issues of accuracy

- **E-mail/Internet (or other Web-based technology)**
  - Preferred mode for low- and medium-frequency reporting
  - Unsuitable for high-frequency of reporting because information must be transcribed at FIU end

- **Dedicated link between a particular reporting entity and the FIU (for high-volume reporters)**
  - Most efficient for high-frequency reporting
  - Overhead for institutions is lower over time
  - A dedicated link does not imply that the FIU can look into the database of the reporting entity, but that data captured by the reporting entity may automatically populate the designated fields of the report(s).

Conclusion: You must consider the technology available to your FIU, the technology available to reporting entities, and the capacity of individuals who will file reports. Several reporting methods are likely to be necessary.

**Answer 17**

“The FIU should have access, directly or indirectly, on a timely basis to financial, administrative, and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.”

—FATF Recommendation 26

This following list of data sources is not meant to be inclusive or prescriptive. Certain records may not exist or may be in a format not readily usable in
initial analyses. Legal gateways may need to be opened before certain sources can be tapped.

- Criminal records
- Criminal intelligence
- Security service/intelligence agencies
- National identity documents
- Passport
- Driving documents
- Vehicle registration
- Land/property registration
- Company and other types of businesses registration
- Tax information (revenue and customs)
- Supervisory/regulatory bodies
- FIUs or other competent authorities in other countries

In addition to public sector and government databases, consider commercial and other open sources of data for comparison and enhancement of the STR. Possible sources include the Internet, news sources and updates, and commercial credit reference agencies.

**Answer 18**
The main consumers are likely to be:

- LEAs
- Regulators/Supervisors
- Other FIUs
- Policy makers
- Legislators
- The National AML/CFT Committee and government departments
- The FATF or your FSRB

**Answer 19**
No. It is most unlikely that all consumers will have the same needs. Their roles and responsibilities differ; so will their needs. Targeting the correct information, to the correct agency, at the correct time, and in the correct format is vitally important for the credibility and sustainability of any FIU.

**Answer 20**
LEAs will be primarily looking for (i) STR analysis to conduct operations, (ii) information in support of other operations that they may be conducting, and (iii) results of your trend work, strategic analysis, and typologies. In what format will your analyses be best presented to the LEAs, and should they see the original reports? Should you present a composite of the analyses? The answers will differ by jurisdiction and according to the needs of the LEA and its place in the
judicial process. The important thing is to discuss these issues with LEAs and prosecutors. There is little point in disseminating a product that cannot be used or is not helpful.

Regulators/supervisors will want to know who is reporting, who is not, and how good the reports are. Quality generally will count for more than quantity, although a quantity of zero is generally an indicator of poor compliance, as is the case where a single institution makes frequent reports that are found to be of little use. Regulators/supervisors also will benefit from trend, strategic, and typology work.

Other FIUs can help you in your analysis of STRs. You can alert them to potential issues in their jurisdiction.

Policy makers and legislators will benefit from general statistics, as well as trend, strategic, and typology work. They will use it to measure success and to target new or weak areas.

The National AML/CFT Committee needs performance indicators, as well as trend, strategic, and typology work. The FATF and FSRBs need trend, strategic, and typology work.

**Answer 21**

Most of the data described below are drawn from information already gathered by the FIU through its STR processes. Other data must be drawn from other agencies—such as LEAs, prosecutors, and courts.

a) Numbers of STRs, CTRs, and other reports:
   - Received—from whom
   - Disseminated—to whom
   
   How long did it take to process and/or analyze the reports?

b) Numbers of reports received from other bodies:
   - Law enforcement
   - Regulatory/Supervisory bodies
   - Foreign authorities
   - Through mutual legal assistance/extradition (including freezing, seizure, confiscation, and investigation of predicate offenses)

C) Disseminations resulting in:
   - Investigation (crimes, terrorism)
   - Prosecution
   - Conviction
   - Property frozen (number of cases and value)
   - Property seized (number of cases and value)
d) Property confiscated (number of cases and value)
   • Number of foreign requests processed
   • Number sent—to whom—number resulting in intelligence received
   • Number received—from whom—number resulting in an intelligence response
   • Whether requests were proactive or reactive
   • How long it took to process and to analyze the requests

e) Number of postponed/suspended transactions by the FIU:
   • Based on FIU’s own initiative
   • Based on a request from a foreign FIU

**Answer 22**

- The most readily available feedback should be taken from information that is readily available within the FIU: (i) the number of disclosures; (ii) appropriate breakdowns by sector and institution; (iii) an analysis of whether the information was accurate, timely, and in sufficient detail; (iv) how the information was used—for example, disseminated to other competent authorities (and which ones), stored for future use, not suitable for further action)
- The most common form of feedback sought relates to the actual use and relevance of STRs. That information is most commonly found in feedback obtained from other competent authorities to which the FIU forwarded its files for possible further action. Did forwarded information result in an arrest, investigation, prosecution, seizure, and confiscation? Did it initiate a case that would not have started without the STR information? Did it add value to an ongoing inquiry? If none of these, did it add value to information or intelligence already held on a subject but not actionable at present? If the information could not be used, what was the reason? How many cases are closed, completed, subject to ongoing inquiry? Some of this information may well be subject to domestic legal principles; however, these should not be so restrictive that they eliminate the ability to provide some form of meaningful feedback.
- Feedback from regulatory/supervisory bodies. How often were supervisory measures taken on a basis of an FIU initiative? Were there any sanctions applied against the reporting entities?
- Feedback that leads to publicizing of current money laundering or terrorist financing techniques, methods, and trends (typologies), often in the form of “sanitized” cases
- Feedback to institutions in the form of acknowledgments of receipt of reports
Answer 23
Careful consideration must be given to the feedback process. LEAs and other competent authorities that make use of your STR information (in whatever format) are often busy with their own statutory functions and have little time to complete additional paperwork—such as lengthy feedback reports to FIUs.

A balance must therefore be struck between the FIU’s need for legitimate feedback and the need of other bodies not to be bogged down by additional paperwork. One compromise is to use a simple matrix that captures the above information and provides space in which the LEA or other body can write a few sentences about the prominent features of a case that it has completed before returning the form to the FIU. Such a process should capture statistical data on STRs (through the matrix) and provide a simple narrative that the FIU can use to identify cases for use in trend analysis or as sanitized case studies.

Answer 24
No. It is important to differentiate among forms of feedback.

- The FIU requires for its tactical and strategic analysis a greater level of detail than that needed by reporting institutions.
- As noted earlier, legal constraints may prevent the FIU from relaying to reporting entities information received from competent authorities, at least in its original form.
- Providing detailed information to reporting institutions may compromise the work of other authorities. This does not mean that no information should be provided; just that it must be in a generic format and provided in such a manner that does not compromise ongoing or future operational work.

The above notes are not meant to be exhaustive or comprehensive, but merely to help you consider how to handle different forms of feedback.

Answer 25
Chiefly because the counterpart FIU will understand the nature of your business! As a result of work done by the FATF, FRSBs, and the Egmont Group (which we will discuss in this module), your international counterparts are undertaking work similar to yours, and following similar principles. Like you, they are likely to share only appropriate information and to have proper regard for privacy rights.
Answer 26
As in previous examples, the following list is not all-inclusive.

- Understanding the scope of predicate offenses for money laundering and terrorist financing
- Understanding typologies and techniques necessary to analyze, investigate, and prosecute those offenses
- Understanding techniques for tracing the proceeds of crime used to finance terrorism
- Understanding when, where, and how property can be seized, frozen, and confiscated
- Understanding principles of international cooperation
- Familiarity with techniques used by supervisors to ensure that financial institutions are complying with their obligations (audit and compliance assessment skills)
- Analytical skills
- Computer literacy
- Other information technology skills
- Understanding of law enforcement capabilities (for staff not from a law enforcement background)
- Understanding the instruments, products, and documents in use at financial institutions and DNFBPs
- Special training or certification for financial investigators in investigations of money laundering and terrorist financing and their predicate offenses

Except for the last point, these skills do not take into account functions generally seen as outside the scope of the FIU, such as regulation, criminal investigations, or prosecution.

Answer 27
The issues raised in the previous answer are readily surmountable if thought through at the design stage. The costs of failing to plan ahead include discontent among staff and fragmentation of staff loyalties, with some staff acting as “agents” for their parent service and not contributing to the mission of the FIU.

Therefore, before a staff is hired:

- Set aims and objectives for the FIU.
- Establish a formal staff structure to meet those aims, rather than designing positions to suit specific individuals.
- Draft job descriptions for each post, specifying how the post fulfills the FIU’s functions and where it fits in the hierarchy.
- Make clear that posts will be filled based on ability, not rank in a prior or parent organization.
Answer 28
Again, there is no right or wrong answer, as long as your rationale is sound and touches on some or all of the following points:

- FIU staff and skills
- Funding and independence
- Interaction with other agencies and access to their data
- Products to be disseminated, to whom, and for what uses (intelligence vs. evidence)
- Core and additional functions
- Domestic and international cooperation and access to foreign intelligence.

The foregoing list is not meant to be exhaustive, but rather to highlight some basic points that may affect the type of FIU you recommend.

Answer 29
True. For the overall effectiveness of the whole AML/CFT regime it is important that reporting by financial institutions and DNFBPs be made as simple and efficient as possible.

Answer 30
False. The four basic models of FIUs are administrative, law enforcement, judicial/prosecutorial, and hybrid model.

Answer 31
True. While some FIUs are required by domestic legislation to establish MOU, other FIUs are able to exchange information simply upon request or simultaneously.

Answer 32
False. FATF Recommendation 25 suggests that the competent authorities provide guidelines and feedback to financial institutions and DNFBPs. Regular publication of industry-specific information, or “guidelines” regarding trends in suspicious activities for a country or region, is particularly beneficial. The FIU should educate supervisory agencies on these patterns and trends to prevent the overreporting of low-quality information. Feedback is an important mechanism to help supervisory agencies and supervised entities understand when reported data are useful, and when they are not.

Answer 33
No. Whatever type of FIU the country establishes, the answer is not to mirror another country’s FIU, but to establish one that best reflects the culture, economy, and other prevailing conditions within the country.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The *Combating Money Laundering and the Financing of Terrorism* training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

- **Module 1**: Effects on Economic Development and International Standards
- **Module 2**: Legal Requirements to Meet International Standards
- **Module 3a**: Regulatory and Institutional Requirements for AML/CFT
- **Module 3b**: Compliance Requirements for Financial Institutions
- **Module 4**: Building an Effective Financial Intelligence Unit
- **Module 5**: Domestic (Inter-Agency) and International Cooperation
- **Module 6**: Combating the Financing of Terrorism
- **Module 7**: Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Domestic (Inter-Agency) and International Cooperation

Workbook
Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide

Domestic (Inter-Agency) and International Cooperation

Workbook

THE WORLD BANK
Washington, D.C.
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

The initial work was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 5 was further written and developed by Jean Pesme, the World Bank. The draft was reviewed by Cari Votava, the World Bank, and Linda Samuel, U.S. Department of Justice. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by John McDowell and Emiko Todoroki, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include Financial Action Task Force on Money Laundering, “The Forty Recommendations,” 2003, and “Special Recommendations on Terrorist Financing,” 2005; and Paul Allan Schott, Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, Second Edition, the World Bank, 2004.

Capacity Enhancement Program on Anti-Money Laundering and Combating the Financing of Terrorism

Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in anti-money laundering and combating the financing of terrorism (AML/CFT) activities. This module addresses the following issues:

1. Interagency Cooperation: Why is it central to AML/CFT? 3
   1.1 Multidisciplinary approach to AML/CFT 5
      1.1.1 The objectives 6
      1.1.2 The tools 7
      1.1.3 The main actors 8
      1.1.4 Building cooperation 12
   1.2 A memorandum of cooperation among AML/CFT agencies 15
   1.3 Ongoing dialogue between government agencies and industry 16
   1.4 National AML/CFT strategy 18
   1.5 Information exchange and sharing 19

2. International Cooperation: Why is it important? 23
   2.1 Building an efficient AML/CFT strategy 23
   2.2 Prerequisites for effective international cooperation 26
   2.3 Modalities and channels for international assistance 28

This module covers the following Financial Action Task Force (FATF) Recommendations:
- Domestic interagency processes: Recommendations 25, 31, and 32
- International Cooperation: Recommendations 35–37, 40, and Special Recommendation V

At the end of this module, you will be able to
- explain why domestic interagency cooperation and sharing of information are central to AML/CFT;
- describe what mechanisms and tools are useful in enhancing domestic interagency cooperation;

—continued
discuss how financial sector supervisory authorities and law enforcement should cooperate and exchange information;
explain why international cooperation, effective exchange of information, and mutual legal assistance are important to AML/CFT;
list best practices for effective international cooperation; and
give examples of how to enhance international cooperation.
1

Interagency Cooperation: Why is it central to AML/CFT?

How much do you know?

Let us start by looking at some practical examples where domestic coordination comes into play. Read the brief scenarios, and answer the questions that follow in the spaces provided.

**QUESTION 1.** Following the acquittal of a known money launderer in your country, a small police station in a remote village discovers evidence that may have supported a conviction. As a result, your Parliament has demanded a report on recommendations to minimize legal, political, and bureaucratic impediments to interagency cooperation. You decide to hold meetings with representatives from relevant agencies to better understand and identify the impediments to information sharing and domestic cooperation. What government agencies/institutions in your country would you want to contact?


**QUESTION 2.** Your minister of justice has received complaints from counterparts in neighboring countries about your country’s lack of cooperation and information sharing on money laundering (ML) and terrorist financing (FT) cases. The minister asks the financial intelligence unit (FIU) to draft a report identifying political, legal, regulatory, and bureaucratic impediments to international cooperation and legal assistance. What government agencies/institutions should top the list of those you need to contact? Where could you find the most useful information on impediments, other than government agencies?


**QUESTION 3.** The AML/CFT law in your country now requires that certain professionals and entities not subject to official supervision be obligated to
monitor and report suspicious transactions and certain cash transactions to the
FIU. The head of your FIU wants to organize meetings with representatives of
these professions, entities, and organizations to discuss what modes of compli-
ance would work best for them. Which professions and entities would you
recommend to meet?

QUESTION 4. You are an assessor serving on a World Bank/IMF evaluation mis-

tion in Xanadu. Can you list five statistical indicators/documents you could
request from Xanadu authorities to gain a preliminary understanding of domes-
tic coordination and international cooperation?

QUESTION 5. What financial (or banking) sector principle is the most common
impediment to information sharing, for domestic or international purposes?

QUESTION 6. You are responsible for AML/CFT issues at your country’s Ministry
of Finance and you are heading a national delegation to a plenary meeting of the
FATF-Style Regional Body (FSRB) in which your country participates, in Blich.
Because you are coming directly from a third country, there was not enough time
to organize an interagency coordination meeting before joining the plenary.

On the first day of the plenary meeting, colleagues from your delegation’s other
agencies have yet to arrive. The Ministry of Justice representative for Begunia,
a neighboring country, has proposed to meet you to discuss bilateral coopera-
tion on AML/CFT, particularly between the FIU and prosecution authorities.
He expresses interest in discussing specific, individual cases and, in particular, a
letter your country sent to Begunia’s justice minister addressing a highly visible
corruption case involving a bank branch, in your country, of a major financial
institution headquartered in Begunia.
You are unaware of the specific money laundering case; however, you recall that in an interagency discussion some time ago, the head of your banking supervisory agency complained that Begunia’s international cooperation appeared less than robust. He insisted that his views not be shared with the relevant national agencies in your country. Although your Ministry of Finance and banking supervisory colleagues will not arrive until the next morning, you agree to meet one-on-one that evening.

Several events or circumstances described above do not promote high-quality domestic and international cooperation. Note three such circumstances you noticed in the space provided below.

1.1 Multidisciplinary approach to AML/CFT

AML/CFT is a multifaceted endeavor. A multidisciplinary approach to AML/CFT should mobilize all relevant agencies. There is no “one-size-fits-all” description of agencies that should participate in AML/CFT activities: each country has unique institutional settings. In this context, a broad approach may be the most conducive to identifying the parties at stake. The focus should be on the design mechanisms best suited to each country for the easy assimilation of coordination schemes (systems). There will be further discussion on this later.

Domestic coordination should be built on two pillars: the public authorities and the private sector.
This module focuses on the institutional settings to be put in place to foster domestic coordination. Other modules in this course lay out the specific conditions to be met to ensure that exchanges of information are legally possible at the domestic level and operationally facilitated. However, the first condition is a strong political will to encourage domestic coordination and exchange of information among the various domestic players both at the policy and operational levels. It is necessary to ensure that the constituents see the benefits and bear the fruits of domestic coordination. In the final analysis, all of the constituent agencies benefit because the country benefits from a more productive AML/CFT regime and robust prosecutions.

**A cross-cutting approach**

The very rationale during the 1980s to adopt a cross-cutting approach to money laundering (focusing initially on drug trafficking) was precisely to use the money trail and to leverage all possible resources. The fight against corruption and bribery (as recently evidenced by the inclusion of corruption/bribery in the list of predicate offenses) is another good example of the benefits of this approach, as the detection of the corruption act itself is usually very difficult—although tracing the money trail can prove very useful (see, for instance, the Abacha case and Mobutu case).

Interagency cooperation is one of the most challenging aspects of implementing an effective AML/CFT regime arising from the following examples:

- The great diversity of predicate offenses (bribery, corruption, smuggling, customs offenses, etc.) requires experts from a variety of specialized agencies or supervisory authorities that do not traditionally communicate with each other.
- ML and TF are largely perceived as victimless crimes that are transactional in nature. Unlike more traditional crimes, and absent a proactive attitude by all agencies involved in the fight against ML/FT, hard evidence of ML/TF emerges late (i.e., assets are transferred). The most useful evidence consists primarily of financial records, which are often locked away in financial institutions (FIs), and protected by banking/financial secrecy principles and not readily accessible to law enforcement agencies.
- Prevention and detection depend on reporting of suspicious transactions by individuals who owe some duty of confidentiality to their clients; reporting is based on suspicions as opposed to hard evidence.

**1.1.1 The objectives**

**QUESTION 7.** Can you identify two main objectives of domestic coordination?
Domestic coordination does not take place in a given country out of the blue. It proceeds from a conscious process and from an organized mobilization of information sharing/coordination mechanisms. Based on the description above of the objectives and expected benefits of enhanced domestic coordination, please describe the tools you would use in your country and the key actors you deem necessary for successful domestic coordination on AML/CFT. Use the space below for your response.

1.1.2 The tools

It is important to embed in each country’s institutions the mechanisms to foster interagency coordination. The following have been found to be generally useful:

- Quick reporting lines to the political level, providing momentum, legitimacy, and guidance
- Ongoing review of the legal framework, in light of practical experience and challenges, which requires regular feedback for law enforcement, FIU, and regulators on implementation failures
- Constructive dialogue on an ongoing basis between proponents with different legitimate viewpoints (for instance, investigative bodies and supervisory authorities)
- Careful review of communication channels and gateways that are in place with the purpose of improving the effectiveness and efficiency of those communication channels and gateways
- Review of intelligence agencies’ information databases to understand all potential sources of information that are available to those involved with AML/CFT and determine whether reciprocal agreements should be utilized.

Integration and coordination

Although the primary objective of AML/CFT work is to prevent, detect, and prosecute those involved with ML and TF, many agencies involved in this work were originally created to pursue other primary objectives. Integrating the various and diverse agencies into an effective AML/CFT regime is one of the biggest challenges of effective implementation.

One traditional example in that respect is the need to coordinate between the FIU and the supervisory authorities so that supervisory inspections assess compliance with...
1.1.3 The main actors

Interagency cooperation can be an enormous challenge when AML/CFT frameworks are put in place and should, therefore, not be taken for granted. In some countries, there may be laws that separate law enforcement from intelligence functions. However, overly strict intelligence secrecy policies and procedures can seriously impede AML/CFT work.

There is certainly the need for good coordination and communication among various authorities involved. This means the need to share a unified approach and implement measures necessary to combat money laundering and terrorist financing. This also means the need for rapid exchange of information among the various authorities. It calls for a complete understanding and identification of the agencies that should be involved and how their work, expertise, and perspectives can add value to overall AML/CFT efforts. There is also a need for a mix of formal (perhaps a dedicated coordination body) and informal communications-dialogue, which can play a crucial role engendering trust among partners. The agencies involved in the multidisciplinary process must be tailored to each country’s circumstances. The following key agencies usually participate at the operational level:

- Ministry of Justice and Prosecutor General
- Home Affairs/Interior Ministry/investigative agencies/police
- Ministry of Finance
- Financial Intelligence Unit (FIU)
- Central Bank and other supervisors/ regulators of the financial sector
- Supervisory authorities in the designated non-financial businesses and professions (DNFBPs)
- Customs and tax authorities

suspicious transaction or activity reporting (STR/SAR) and cash transaction reporting (CTR) requirements, as well as effectively sanction incidents of noncompliance. As the FIU possesses the institutional expertise to understand suspicious patterns of activities (i.e., “red flags”) across sectors and industries, this information must be coordinated and shared with relevant supervisors and disseminated to reporting institutions so they can understand how to identify what might be suspicious. Coordination among supervisory agencies in the financial sector is also an important prerequisite to level the playing field and to address the specific challenges of financial conglomerates. Law enforcement officials, police, and prosecution authorities must also share information with the FIU and supervisory agencies so they are informed of trends and targeted risk-based priorities.
Below are certain selected countries. See who is involved in each country’s national AML/CFT effort.

### National AML/CFT efforts around the world

#### The United States
- Central Intelligence Agency (CIA)
- Department of Homeland Security
  - U.S. Customs and Border Protection
  - U.S. Immigration and Customs Enforcement (ICE)
  - Secret Service
- Department of Justice
  - Drug Enforcement Administration
  - Federal Bureau of Investigation (FBI)
  - Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF)
  - Prosecutors
- Department of Treasury
  - Office of the Comptroller of the Currency (OCC)
  - National Credit Union Administration (NCUA)
  - Financial Crimes Enforcement Network (FinCEN)
  - Internal Revenue Service
  - Office of Thrift Supervision (OTS)
  - Office of Foreign Assets Control
- Department of State
- Federal Reserve Board
- Federal Deposit Insurance Corporation
- U.S. Congress
- U.S. Postal Service

#### Brazil
- Brazilian Agency of Intelligence
- Central Bank of Brazil
- Federal Police Department
- General Attorney Office for the National Treasury
- Ministry of Foreign Affairs
- Secretariat of Federal Revenue
- Securities and Exchange Commission
- Superintendence of Private Insurance

#### Croatia
- Administrative Services of the State
- Anti–Money Laundering Department—Croatian’s (FIU)
- Customs
- Ministry of Finance
- Ministry of Interior
- Police Services
- Supervision of Foreign Transactions Department
- Tax Department
- National Bank

---

---
Belgium
- Administrative Services of the State
- Banking, Finance, and Insurance Commission
- Belgium Financial Intelligence Processing Unit (CTIF-CFI)
- Central Office for Seizure and Confiscation (COSC)
- Chamber of Representatives of Belgium
- Federal Public Service Finance
- Federal Public Service Justice
- Federal Police

Switzerland
- Money Laundering Report Office Switzerland (MROS)
- Federal Department of Justice and Police
- Federal Customs Administration
- Federal Office of Private Insurance
- Federal Finance Administration/Money Laundering Control Authority
- Swiss Federal Banking Commission
- Swiss National Bank

Australia
- AUSTRAC
- Anti-Corruption Commission (WA)
- Australian Crime Commission
- Australian Federal Police
- Australian Securities and Investments Commission
- Australian Security Intelligence Organisation
- Australian Taxation Office
- Australian Taxation Office
- Crime and Misconduct Commission (Queensland)
- Independent Commission Against Corruption (NSW)
- New South Wales Crime Commission (NSW)
- Police Integrity Commission (NSW)
- State and Territory Police Services
- State and Territory Revenue Authorities

Argentina
- Banco Central
- Comisión Nacional de Valores
- Ministerio de Economía
- Ministerio de Justicia
- Ministerio Público Fiscal
- Ministerio de Relaciones Exteriores
- Unidad de Información Financiera (UIF)
FATF Recommendation 31 stresses the need for enhanced interagency cooperation, and Recommendation 32 advises countries to institute a mechanism to review AML/CFT regimes. Regarding the latter recommendation, its objective goes well beyond the issue of domestic coordination, as it aims to measure the effectiveness of AML/CFT regimes. However, such a measure cannot take place outside an interagency process, and undertaking such an assessment of effectiveness should be used as an incentive for domestic coordination and exchange of information. See Appendix B for more information on FATF Recommendation 31. Also see Appendix C for more information on FATF Recommendation 32.

**Knowledge check**

**QUESTION 8.** What are the minimum standards set by the FATF Recommendations for domestic coordination and exchange of information?
QUESTION 9. Can you identify at least two tools the FIU can use to provide feedback on suspicious activity/transaction reports (SARs/STRs) to reporting institutions?

1.1.4 BUILDING COOPERATION

Once again, a one-size-fits-all approach or mechanism is inappropriate for AML/CFT frameworks. Issues to consider include the following:

- Countries may choose to organize an interagency coordination committee or council. It is important to clarify the mandate of such a body. The focus should be on the exchange of information; this may be done on either an individual case or policy issue basis, or both.
- It may prove useful for legal reasons, among others, to have the coordination committee focus on architectural issues, such as legal impediments.
- Information sharing on individual cases also can be left to a more restricted dedicated body or to bilateral relationships between relevant units. It is essential the “policy coordination committee” members have working gateways in place. A memorandum of cooperation among agencies responsible for AML/CFT can help to achieve more fluid and timely exchanges of information.
- Several countries have used interagency coordination mechanisms to develop a national AML/CFT strategy, which fosters political buy-in, bolsters interagency ownership, and improves monitoring of the overall AML/CFT framework efficiency.

**Interagency cooperation**

An interagency coordination committee or council should include representatives from the various agencies involved in AML/CFT to ensure an effective and efficient AML/CFT system. Depending on each country’s institutional experience and culture, its required level of formalization will have to be assessed on a case-by-case basis. Operational coordination usually takes place on a more bilateral basis, depending on the legal framework for domestic exchange of information.

The committee or council should meet regularly and can usefully build on the work of more technical subcommittees. A chair should be appointed and may be rotated periodically or one agency designated to take the lead in the coordination efforts, depending upon the preferred or standard procedure for other interagency committees.
**For discussion**

Let us consider AML/CFT implementation in your country. Do you have knowledge of (or does there exist) a clear statement of the national AML/CFT policy objectives at the political level in your country? Does this document (decree, law, or other form) designate a particular body/institution responsible for achieving these objectives? Does the statement delineate how progress is to be measured, how often, and by whom (i.e., are annual or other periodic reports required)? Have resources (financial and other) been allocated/designated for reaching these goals? If a policy statement along these lines does not yet exist, do you think one would help minimize the barriers to domestic interagency coordination?

Let us see some country cases.

**Brazil**

The Council for Financial Activities Control (COAF), under the jurisdiction of the Ministry of Finance, was created for the purpose of issuing regulations, applying administrative sanctions, receiving pertinent information, and examining and identifying suspicious occurrences of the illicit activities defined in this law. COAF also coordinates and suggests systems of cooperation and exchange of information to enable rapid and efficient responses in the struggle against concealment or disguise of proceeds of criminal activities and terrorist financing funds, such as assets, rights, and valuables. It consists of the following parts:
**Lebanon**

A national committee coordinates AML policies in Lebanon. The committee is chaired by one of the vice governors of the Bank of Lebanon who is nominated by the governor and includes the following members:

- SIC (Special Investigation Commission-Lebanon’s FIU) secretary
- Representative of the prosecutor’s office
- Banking Control Commission member
- Customs representative
- Representative of Lebanese Internal Security Forces

**Cyprus**

To achieve the highest level of coordination among various agencies, the Republic of Cyprus recognized the need to create a special body that would facilitate interagency cooperation for a unified approach and implement the measures necessary to combat terrorism. This has now been achieved with a decision of the Council of Ministers to set up a Coordinating Body against Terrorism. This body is chaired by the deputy attorney general and is composed of representatives of the police, the Customs Department, members of the Law Office of the Republic, the Ministry of Justice and Public Order, the Unit for Combating Money Laundering (MOKAS), and the CIA.
For discussion

The number of agencies involved in the national AML/CFT effort may come as a surprise. Please think about the following questions:

- Can you identify how many key agencies in your country are involved in AML/CFT?
- What are the existing mechanisms for coordination? Are they AML/CFT-related or more general?
- Do your current interagency settings and authorities allow for critical assessment (building on implementation experience) of the overall AML/CFT framework and conflict-resolution mechanisms?

1.2 A memorandum of cooperation among AML/CFT agencies

**QUESTION 10.** Which agency would you see as the best candidate to develop a network memorandum of cooperation?

National agencies may enter into formal, mutual agreements to further collaboration and the exchange of information on AML/CFT. Interagency agreements integrate the procedures of different agencies and encourage day-to-day communication with other agencies. Agreements of this nature are useful to the FIU, which builds on multidisciplinary experience. The location of an FIU in the AML/CFT infrastructural setting can be a contentious issue; controversy can be alleviated at the outset by insisting on the multidisciplinary features of the FIU and creating a set of responsibilities for the related agencies. In that respect, staff exchanges bring in a variety of experiences and contribute to mutual understandings. Let us look at some country cases.

**Mutual agreements**

*Bulgaria*

In 2002, one cooperation agreement was reached between the Bureau of Financial Intelligence (BFI) and the National Audit Office and another between the BFI and the Agency for State Internal Financial Control. In 2003, another agreement was reached between the BFI and the Insurance Supervision Authority. The existence of such
agreements confirms the willingness of the institutions involved to cooperate and puts in place the mechanisms to facilitate that cooperation.

**Georgia**

A memorandum of cooperation was signed among the Financial Monitoring Service of the National Bank of Georgia, Georgian Bankers Association, Georgian Economists Association, and the National Committee of the International Chamber of Commerce, to promote the enforcement of the country’s AML regime. The parties that signed the agreement believe it will enhance financial monitoring practices in the country.

### 1.3 Ongoing dialogue between government agencies and industry

Working with the finance industry is essential for enforcement strategies on money laundering and terrorist financing—from both the regulatory and the information-sharing perspectives. Regulators and/or interagency committees or councils should organize regular meetings with representatives of the finance industry.

And as the scope of professions covered by the AML/CFT framework increases, appropriate channels of communication and dialogue on AML/CFT issues must open up with those covered professions (for example, lawyers, accountants, notaries). This is all the more important because many of these professions are supervised by independent associations rather than government supervisory bodies and thus oversight and supervision are not as formal and developed as they are for the finance industry.

**Why is this dialogue important?**

The main purpose of this dialogue is to increase cooperation between regulators and those entities that are regulated. Such two-way communication is generally very useful for supervisory officials and policy makers, allowing them to better understand the implementation challenges faced by those required to comply. This is particularly true in an area like AML/CFT because it is often unfamiliar territory for many of those subject to compliance obligations.

It is important that regulators avoid imposing unnecessary burdens on regulated entities and individuals. The key to the success of their efforts is ensuring that regulatory obligations and procedures are clear, workable, effective, and efficient (i.e., user friendly). Similarly, consultation with regulated entities and industry representatives is instrumental; it is particularly useful for affected entities to provide feedback on draft regulations before finalization. Continual dialogue also helps to foster the commitment of the industry over time and to avoid misinterpretations and misunderstandings.
Several tools are needed for dialogue, such as:

- **Legislation**: Agencies must be legislatively authorized to undertake AML/CFT work (or not prohibited from it).
- **Resources**: Agencies must have the resources (or allocated additional resources) to contribute to AML/CFT work.
- **Coordination**: The specific responsibilities of each agency should be clearly defined and delegated so that each agency understands how its expertise adds value to the national AML/CFT effort and accepts its role.
- **Cooperation and communication**: Regular meetings should be arranged between agencies for continued dialogue to encourage the airing of different viewpoints and opinions. In the long run, the teamwork and creative problem solving that should emerge should also trigger constructive and creative solutions.

Supervisory agencies responsible for compliance matters—including AML/CFT compliance obligations—should support the entities they supervise by providing information necessary for identifying suspicious transactions or behaviors (called “red flags”). Regular publication of industry-specific information, or “guidelines,” regarding trends in suspicious activities for a country or region, is particularly beneficial. The FIU should educate supervisory agencies on these patterns and trends to prevent the overreporting of low-quality information. Feedback is an important mechanism to help supervisory agencies and supervised entities understand when reported data are useful and when they are not.

FATF Recommendation 25 emphasizes the need for feedback from all competent authorities (i.e., beyond the FIU) to all covered financial institutions and designated non-financial businesses and professionals (DNFBPs) under the AML/CFT framework. See Appendix D for more information on FATF Recommendation 25.

---

**What kind of feedback is useful to the industry?**

While feedback should include all aspects of compliance, it should specifically focus on SARs/STRs (refer to FATF Recommendation 25). Some countries (e.g., Slovenia) allow for feedback on individual STRs between the FIU and the reporting institution. The FIU or other competent authority should complement such feedback with regular information on overall AML/CFT trends. For this purpose, cases are often sanitized to keep them confidential and to focus more on patterns and trends.

Feedback on prosecutions highlights and reinforces the benefits of industry collaboration.
EXAMPLES OF FEEDBACK

**The United States**
The U.S. financial intelligence unit (FinCEN) works in close collaboration with the Bank Secrecy Act Advisory Group (BSAAG), which provides a forum for frank exchanges of views and promotes cooperation and understanding between law enforcement agencies and the financial community. The group’s members represent the financial services industry, including both big and small banks, as well as the representatives of the securities industry, casinos, and money services businesses (check cashers, money transmitters, and issuers of traveler’s checks). State and federal law enforcement agencies and financial institution supervisors are part of the group.

**France**
France’s Monetary and Financial Code was amended in 2001 to create a liaison committee for the fight against money laundering and terrorist financing. All agencies involved in the fight and all professions required to report are represented on this committee, which is cochaired by the FIU and the Ministry of Justice, with the Treasury Department providing the secretariat. The liaison committee meets twice a year at the principals’ level after the meetings of technical subcommittees. Subgroups are set up to deal with issues requiring in-depth technical dialogue and analysis. The liaison committee is an important source of feedback to the industry on STRs and prosecution activity, and for identifying, at the political level, the main challenges in the AML/CFT effort.

**Bulgaria**
Bulgaria’s BFI values its good relationship with the commercial banks. BFI representatives attend seminars organized by commercial banks, where AML measures and other practical aspects of cooperation between the two sectors are discussed. Feedback on reports submitted to the BFI by commercial banks is another point of discussion. The BFI also has a good relationship with the Association of Commercial Banks. In the past, the BFI proposed amendments to the Law on Measures against Laundering Money.

**Interpol**
Interpol recommends closer cooperation between law enforcement agencies and banking and financial institutions. Such cooperation is useful, for example, in the development of guidelines and in the investigation of international fraud and financial crimes.

### 1.4 National AML/CFT strategy
A comprehensive national AML/CFT strategy creates a collective vision for combating ML/FT at the national level. The strategy should guide national AML/CFT coordination efforts. A national strategy can prove instrumental in implementing FATF Recommendations that give more weight to risk analysis, where such a strategy is tailored to cope with major risks and threats. To this end, the following complementary objectives can be pursued by a country:

- Define strategic objectives.
- Foster coordination, define specific responsibilities, and delineate guidelines and procedures.
• Align resources and tools with strategic objectives.
• Define the method and timing to measure effectiveness.

See Appendix E for further information on a national strategy. The strategy should be dynamic so that it undergoes regular review and revision. It should evolve over time to counter changing typologies of money launderers and terrorist financiers, as well as changing circumstances in the country, including changes in the institutional structures.

National strategies can serve as a very efficient mechanism to raise public awareness on the importance of AML/CFT and begin a dialogue about common concerns, such as privacy. Other points to talk about are goals, key priorities, and agencies charged with action plans.

It is critical for countries to hear all the relevant voices in the development of a national AML/CFT strategy. Law enforcement and financial regulatory authorities must work in partnership with covered financial institutions and DNFBPs to counter the criminal sector in an effective manner.

1.5 Information exchange and sharing

It is absolutely critical for information sharing and exchange among agencies in a country, both domestically and internationally, that each agency clearly understand the legal and theoretical constraints that restrict information sharing. Once understood, efforts should be undertaken to remove unnecessary barriers. Officials and policy makers should understand very clearly the costs of not sharing information and benefits of information sharing. Money laundering and terrorist financing transactions, in many of the important cases, tend to cross borders of several countries (jurisdictions). Additionally, the speed at which electronic transfers can be made ensures that criminals can easily put their assets out of reach of authorities, if evidence of the transaction activities cannot be appropriately shared on a timely basis. Therefore, unnecessary constraints or bureaucratic procedures, required as a condition for information sharing, can render the best AML/CFT system ineffective.

The exchange of intelligence information between national authorities is central to the prevention, investigation, and prosecution of money laundering and terrorist financing. The horizontal AML/CFT approach builds on SARs or STRs, creating, at the national level, a web of information exchanges. To facilitate a secure, but rapid, exchange of sensitive information, it is useful to consider developing a secure database that can be shared by all relevant authorities. Various authorities should be able to add financial intelligence information to the database.

Regulatory authorities, the FIU, and law enforcement must, together, ensure that information gateways and exchanges are secured, swift, and reciprocal. When setting up a new AML/CFT framework or improving an existing one, it is of paramount importance to make it clear that confidential information gathered through SAR/STR mechanisms will remain confidential, and that any abuse
or misuse will be punished. This is the key to assuring banks and other financial entities—and ultimately clients—that there is no unauthorized use of data received from SARs/STRs. The following chart illustrates key channels of interagency communication used by the main actors in a typical AML/CFT system. Again, there is no “one-size-fits-all” approach, and each network will have to be tailored to each country’s circumstances.

**Examples of information exchange**

**The United States**

Together with a federal court decision in November 2002, the USA Patriot Act (“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, USA PATRIOT ACT of 2001”) has broken down what had been called “the wall” that legally separated law enforcement and intelligence functions. The idea was to improve coordination and information sharing between the law enforcement community and intelligence agencies. Since the attacks of September 11, the cultural and operational wall between the FBI and CIA has also been broken down, with the two agencies becoming better integrated at every level of operation.

**Australia**

The Australian Transaction Reports and Analysis Centre (AUSTRAC) provides the Australian Taxation Office (ATO) and specified law enforcement, security, and revenue agencies with both general and specific access to information collected from financial transactions reports. Under memoranda of understanding (MOU), partner agencies have controlled online access to the data and, where appropriate, may extract parts of the data holdings. This allows foreign partners to add AUSTRAC’s financial intelligence to
Knowledge check

QUESTION 11. Is it mandatory to define a national AML/CFT strategy?

QUESTION 12. Can you write about two benefits of developing an AML/CFT national strategy?

QUESTION 13. Why is it necessary for the banking sector supervisor to consult with the FIU when defining its on-site inspection program? What information should he or she get from the FIU?

QUESTION 14. What information gathered during on-site inspections could be of interest to the FIU?

QUESTION 15. Can you name three government agencies or institutions that are important parts of an effective AML/CFT framework?
You are a member of the World Bank/IMF assessing the AML/CFT system (and its effectiveness) in Xanadu. During the discussions with the authorities, the following issues are raised.

**QUESTION 16A.** Your advice is sought on the best institutional setting for an FIU. Please select one proposal among the following.

The best institutional setting for the FIU is:

a) Within the Central Bank  

b) No one-size-fits-all answer; several features can contribute to efficient domestic coordination: memoranda of understanding, staff exchanges, annual reports  

c) Within the Ministry of Justice  

d) To report directly to the prime minister  

e) Within the prosecutor’s office  

f) Within the police

**QUESTION 16B.** The authorities have proposed the following agencies to participate in your meetings: the Central Bank, Customs, and the Ministry of Finance. You have been asked to offer your suggestions. Select the most appropriate response from the following:

a) Agree to this program.  

b) Request additional meetings with the FIU.  

c) Request additional meetings with the FIU and the Ministry of Justice.  

d) Request additional meetings with the FIU, the Ministry of Justice, the police, and the prosecutor’s office.  

e) Request additional meetings with the FIU, the Ministry of Justice, the police, the prosecutor’s office, the judiciary, and the supervisors.

**QUESTION 17.** Prepare a quick list of the bodies, agencies, and so on, that report individual or policy-based information on AML/CFT issues to the FIU in your country. Can you identify any gaps in the previous presentation (“Interagency exchange of information” in section 1.5)? Do you think these gaps result from insufficient coordination among relevant agencies/bodies or are legal impediments hindering the flow of information to the FIU?
2.1 Building an efficient AML/CFT strategy

ML/FT are global problems that not only threaten security but also compromise the stability, integrity, transparency, and efficiency of financial systems and undermine economic prosperity. The rapid exchange of information and effective international cooperation among the various agencies throughout the world are prerequisites for success.

Money launderers and terrorist financiers use the openness of the international financial system and free movement of capital throughout the world to achieve their goals. Although openness increases associated risks and calls for their management and mitigation, even “closed” economies with restricted international capital flow are not immune to abuse by money launderers and terrorist financiers. Most of the closed economies rely on capital controls that are not designed to address AML/CFT.

International cooperation will not be limited to cross-border problems stemming from the free movement of capital. Prosecution/law enforcement is a high priority because gathering evidence to support AML/CFT cases requires more and more mutual legal assistance. A comprehensive approach to international cooperation is vital; “silo” approaches are necessary but not sufficient.

Here again, this module focuses on the international instruments and tools used to bring about international cooperation, while the other modules in the course present sector-by-sector conditions and incentives. The primary thrust of the course is that a horizontal approach must complement vertical efforts. For the most part, international cooperation is constrained by the following obstacles:

- Lack of political will
- Legal barriers
- Lower priority to informational requests received from outside the country
- Concerns related to national security and intelligence information
- Concerns on the use of data retrieved through intercepts and surveillance
- Concerns regarding how information might be used in another country, in particular if its integrity and confidentiality might be put at risk
- High costs
More international cooperation is needed at different stages, some of which are discussed below:

**Stage 1: Enforcement of Prevention and Detection Requirements**

The cross-border nature of financial flows and the development of financial conglomerates with large international networks make it increasingly necessary for supervisors and regulators to adopt an international approach when assessing the implementation of AML/CFT obligations. This is a very strong trend in banking sector supervision, where supervisors are working to increase their coordination and cooperation in the supervision of banks operating in several countries. This does not mean that internationally exposed institutions are at greater risk of being abused by money launderers or terrorist financiers, but it does mean that, in a risk-based approach, enhancing international coordination and cooperation among supervisors is a key tool for AML/CFT.

**Stage 2: Financial Intelligence Gathering**

If transactions have international aspects, FIUs need to exchange information with their foreign counterparts to be able to analyze suspicious activity reports and other financial disclosures. FIU participation in the Egmont Group fosters their international networks. Such participation can be buttressed by developing a set of memoranda of understanding with foreign FIUs, if required by domestic law to share information.

**Stage 3: Investigation**

The same can be said for the investigative stage for the police and/or other law enforcement bodies to successfully investigate money laundering cases. The quick exchange of information with their foreign counterparts, without undue obstacles or delay, is increasingly becoming a key feature of any FIU, law enforcement, or police authority.

In addition, keeping in mind that money launderers and those who finance terrorism are always looking for safe havens with lax, ineffective, or corrupt AML/CFT regimes, or those with limited capabilities for international cooperation, countries will find that having a proper international cooperation framework in place helps them to prevent, detect, and prosecute money laundering and financing of terrorism in their own domestic financial system.

Several international bodies, and, of course Interpol, foster international cooperation at the investigative stage. They have placed AML/CFT very high on their agendas.

**Stage 4: Prosecution**

Central to AML/CFT prosecution, mutual legal assistance is usually associated with specific and more formalized forms of international cooperation, including ensuring that evidence collected abroad is acceptable.
Experience has shown that these objectives can and must be reconciled, provided, first, that the specifics of mutual legal assistance are acknowledged; second, that they are not abused to undermine international cooperation (in particular by imposing undue restrictions); and, finally, that countries are clear on the gateways, requirements, and conditions for mutual legal assistance.

STAGE 5: MUTUAL LEGAL ASSISTANCE

FATF Recommendations 36 and 37 also emphasize the importance of mutual legal assistance. For more information about mutual legal assistance, please refer to section 3.1 (Mutual legal assistance) in Module 2. See Appendix F for more information on FATF Recommendations 36. See also Appendix G for more information on FATF Recommendation 37.

FATF Recommendation 40 encourages countries to provide the widest possible range of international cooperation. See Appendix H for more information on Recommendation 40.

Knowledge check

Read the following hypothetical scenario for the following three questions:

You are a member of the World Bank/IMF mission assessing the AML/CFT regime in Xanadu.

QUESTION 18. You want to gain a quick understanding of the degree of international cooperation by the FIU. Cite three indicators and quantitative measurement tools on which you should request information from the authorities.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

QUESTION 19. You also want to check the quality of domestic coordination when addressing the challenges of international cooperation. Please list three quantitative and measurable indicators you should get information on, from the authorities, to improve your understanding of the situation of the country.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
QUESTION 20. Secrecy provisions (in particular, banking secrecy) can present significant impediments to international cooperation. Do you know what the fiscal excuse is, and how it can negatively affect international cooperation?

2.2 Prerequisites for effective international cooperation

For discussion

What do you think are some prerequisites or legal (legislative) steps countries should take in order to ensure that there are adequate legal channels for effective international cooperation? Record your thoughts in the space below, and then find your answers in the following sections.

For countries to use the existing channels of international cooperation, they need to meet at least the following three prerequisites:

1) Ratification and implementation the international conventions
2) Compliance with the FATF Recommendations and other sector-specific international standards
3) Building comprehensive and efficient domestic capacity

RATIFICATION AND IMPLEMENTATION OF THE INTERNATIONAL CONVENTIONS

International conventions are intended to establish some international standards for laws, regulations, and procedures for international exchange of information and mutual legal assistance. Countries should sign and ratify relevant conventions—and implement them fully in their domestic laws. FATF Recommendation 35 urges countries to ratify and implement UN Conventions and other relevant international conventions.

- UN conventions
  - UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988)
  - International Convention for the Suppression of the Financing of Terrorism (the SFT Convention, 1999)
• UN Convention against Transnational Organized Crime (the Palermo Convention, 2000)
• Conventions adopted by regional organizations that are applicable to specific regions

The UN Convention Against Corruption (2003) is, of course, an important additional instrument in the fight against financial crime. For more information on FATF Recommendation 35, see Appendix I.

Countries should implement the provisions of these conventions in their domestic laws—particularly those related to the criminal offense of money laundering, the criminal offense of terrorist financing, and international cooperation—that will enable them to take part in the mutual legal assistance arrangements these conventions provide. FATF Special Recommendation V stresses the importance of mutual legal assistance, information exchange, and the great possible measure of assistance in connection with criminal, civil enforcement, and administrative investigation among countries. It is important to note that ratifying a UN Convention or a convention adopted by a regional organization usually does not make this convention binding in the domestic legal framework; changes in the criminal code and in other laws are often necessary. For more information on FATF Special Recommendation V, see Appendix J.

**COMPLIANCE WITH THE FATF RECOMMENDATIONS AND OTHER SECTOR-SPECIFIC INTERNATIONAL STANDARDS**

Countries should comply with international standards. All international standard setters require adhering countries to establish international channels of cooperation with foreign partners. For example:

• FATF—the FATF Forty Recommendations and the FATF Nine Special Recommendations
• Basel Committee on Banking Supervision—Core Principles for Effective Banking Supervision
• Basel Committee on Banking Supervision—Customer Due Diligence Principles
• International Association of Insurance Supervisors (IAIS)
• International Organization of Securities Commissions (IOSCO)
• The Egmont Group
• The United Nations
• Regional instruments that are applicable to specific regions

**BUILDING COMPREHENSIVE AND EFFICIENT DOMESTIC CAPACITY**

Putting in place all the necessary authorities—and providing them with necessary powers, responsibilities, staffing, and budget—is a prerequisite for a country to cooperate effectively at the international level. Domestic agencies should be able to perform their duties efficiently.
For example, countries should establish administrative supervisory authorities to oversee financial institutions in each sector, effective police services having staff with special skills and offering training in money laundering and terrorist financing investigation, and a functioning, noncorrupt judicial/prosecutorial system to have an effective AML/CFT framework. In addition, clarity on the gateways for international cooperation is central to ensure that domestic AML/CFT officials have a good understanding and knowledge of the channels for them to require international support. Too often international cooperation is “measured” by the level of reactivity and responsiveness to requests for international assistance, where the practice of requesting international assistance is also key and should be monitored as well.

2.3 Modalities and channels for international assistance

As mentioned previously, international cooperation should take place at four different levels or stages: enforcement of prevention and detection requirements, financial intelligence gathering, investigation, and prosecution. The key objectives and various tools used to foster international cooperation described in the modules relate to:

- Legal requirements (Module 2)
- Regulation (Module 3)
- Investigation (Module 7)
- FIU (Module 4)

The reason for the emphasis on international cooperation is that money laundering and terrorist financing are cross-border activities and the prevention, detection, investigation, and prosecution of such operations often depend on information sharing among countries and their ability to cooperate efficiently and speedily with their foreign counterparts. Aside from the quality of the legal framework, it is essential that there are incentives for international cooperation at both ends that can be monitored.

On very practical grounds, exchanging staff is one of the best avenues for enhancing international cooperation. This can take place at various levels: the regulatory level, FIU level, and law enforcement level. Such an arrangement will be useful among countries at different levels of development of their AML/CFT regime. On-the-job training is one of the best methods to deliver technical assistance.

In some cases, so-called diagonal exchanges of information (i.e., where the request for information sharing or assistance does not take place between equivalent institutions) can become a challenge. The quality of domestic coordination and information sharing should allow for the creation of a “triangle” so that appropriate and legitimate communication can take place.
Examples of staff exchange

Staff exchange of supervisors
The Office of the Comptroller of the Currency (OCC), a bureau of the U.S. Department of the Treasury, invites foreign bank supervisors to participate in bank examinations.

Staff exchange of U.S. and Swiss law enforcement staff
With behind-the-scenes help from Operation Green Quest, the United States and Switzerland struck a historic agreement to exchange special agents to pursue and interrupt the sources of terrorist funding.1

Commissioner Robert Bonner and Green Quest Director Marcy Forman attended the signing, which took place in Washington, DC, on September 4, 2002.

This groundbreaking agreement, called an “operative working arrangement,” sets an international precedent: it allows investigators from Customs Operation Green Quest, the FBI’s Terrorist Financial Review Group, and Switzerland’s terrorist task force to serve in each other’s organizations.

You could think of it as an academic exchange program, only bigger. Much bigger. And because it’s devoted to pursuing terrorist activities, including and especially those of Al Qaeda, its stakes are much, much higher.

Under the agreement, agents from Switzerland’s investigative group, called Terror USA, will be assigned to Operation Green Quest and to the FBI’s Financial Review Group, while agents from the two American agencies will be assigned to Terror USA. Since the signing, two U.S. Customs agents were detailed to Switzerland for six weeks, and two Swiss agents were detailed to Washington for the same amount of time.

The arrangement is not only historic, it’s practical: unlike international treaties, which require Senate ratification, this one entails no particular international legal rights or obligations.

As transportation and telecommunications keep shrinking our planet, and whole continents can be leapt with a single mouse click, the good guys from all nations are becoming as dependent upon each other as police forces are in neighboring counties.

This new operative working arrangement leverages that growing interdependence by allowing countries to share each other’s law enforcement information in real time, without the redundancy of effort that would otherwise be involved.

It is also another instance of the Customs Service’s commitment to finding non-traditional ways of sharing information among, and cooperating with, international law enforcement agencies, especially those with cities that serve as key financial centers.

Staff exchange between FIUs
The Caribbean Anti-Money Laundering Programme (CALP) works mainly through regional governments and sector organizations to assist Caribbean states in developing comprehensive and effective anti-money laundering strategies. The Programme also offers technical assistance to industry and other professional associations.

For the financial sector, it provides training for financial sector employees and their regulators and offers technical advice on the establishment of financial intelligence units.

Countries around the world are parties to mutual legal assistance programs, which allow them to share expertise and information that will assist in the detection, investigation, and prosecution of offenses.

Key organizations in this initiative include:

- The United Nations
- FATF
- CFATF
- The Global Money Laundering Programme
- INTERPOL
- FBI
- The National Crimes Intelligence Service – London
- The Royal Canadian Mounted Police (RCMP)
- FinCEN
- The U.S. Federal Reserve Banks

For additional information, see http://www.cfatf.org/training/training.asp.

**Check your understanding**

**QUESTION 21.** According to the FATF Recommendations, which UN Conventions should be signed, ratified, and integrated into the domestic legal framework as a prerequisite for effective international cooperation?

**QUESTION 22.** What are the four levels of international cooperation?

**QUESTION 23.** How would you explain the emphasis by the FATF on the notion of gateways for international assistance?
QUESTION 24. To foster domestic coordination, an FIU should be given the following missions to make AML/CFT investigations possible: the supervision of banks’ compliance with AML/CFT requirements and the reception, analysis, and dissemination of STRs.
   a) True    b) False

QUESTION 25. Only the FIU should provide feedback to the private sector on AML/CFT.
   a) True    b) False

QUESTION 26. Preparing and publicizing a “national AML/CFT strategy” is not a requirement laid out by the FATF Recommendations.
   a) True    b) False

QUESTION 27. The private sector should be kept at arms’ length in the implementation of the AML/CFT framework, to avoid undue interference.
   a) True    b) False

QUESTION 28. It is possible to measure the quality of domestic and international coordination.
   a) True    b) False

QUESTION 29. The Vienna and the Palermo Conventions are the only multilateral instruments dealing with AML/CFT.
   a) True    b) False

QUESTION 30. When the banking regulator in country X requests international assistance from the police in country Z, the latter can ignore the request because it is not the counterpart of a financial sector supervisor.
   a) True    b) False

QUESTION 31. The only reason to take steps toward the provision of international assistance is to avoid being put on the FATF noncooperative countries and territories blacklist.
   a) True    b) False

QUESTION 32. Formal mechanisms of domestic and international cooperation are not the only tools for ensuring effectiveness.
   a) True    b) False
QUESTION 33. Government agencies should maintain contacts with the private sector only through professional associations and undertake consultations only on a sectoral basis.

a) True    b) False

QUESTION 34. The ability to respond quickly to requests for international cooperation is the main indicator of success for a given jurisdiction.

a) True    b) False

QUESTION 35. Staff exchange at the domestic and international levels cannot be used to promote cooperation because excessive constraints are in place to protect confidentiality.

a) True    b) False

Summary

In this module, we discussed:

- Why it is important to enhance domestic interagency cooperation
- What mechanisms and tools might be useful in improving domestic interagency cooperation
- Why it is important to enhance international cooperation
- The prerequisites for effective international cooperation
- What challenges international cooperation might present
- How to enhance international cooperation.
Appendix A: References

FATF Recommendations

- The Forty Recommendations (FATF, June 2003)
  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- Special Recommendations on Terrorist Financing (FATF, October 2001 and October 2004)

Useful Web sites

- Asia/Pacific Group on Money Laundering (APG)
  http://www.apgml.org/
- Basel Committee on Banking Supervision (BCBS)
  http://www.bis.org/bcbs/index.htm
- Caribbean Financial Action Task Force (CFATF)
  http://www.cfatf.org/eng/
- Egmont Group
  http://www.egmontgroup.org/
- Financial Action Task Force of South America Against Money Laundering (GAFISUD)
  http://www.gafisud.org/
- International Association of Insurance Supervisors (IAIS)
  http://www.iaisweb.org/
- International Organization of Securities Commissions (IOSCO)
  http://www.iosco.org
- Council of Europe Select Committee of Experts on the Evaluation of Anti–Money Laundering Measures (MONEYVAL) [European regional AML/CFT body for Europe jurisdictions that are not members of the FATF]
  http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/
- INTERPOL
  http://www.interpol.int/Default.asp
**Reference Documents**

- Core Principles for Effective Banking Supervision (Basel Core Principles) (BCBS, September 1997)
  [http://www.bis.org/publ/bcbsc102.pdf](http://www.bis.org/publ/bcbsc102.pdf)
- Customer Due Diligence for Banks (BCBS, October 2001)
  [http://www.bis.org/publ/bcbs85.pdf](http://www.bis.org/publ/bcbs85.pdf)
- Principles for Information Exchange between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases (The Egmont Group, Statement of Purpose, Annex) (The Egmont Group, June 2001)
- *Revised Statement of Purpose* (The Egmont Group, June 2004)
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances: Vienna Convention (UN, 1988)
- Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime: The Strasbourg Convention (Council of Europe, September 1990)
Appendix B: FATF Recommendation 31

Countries should ensure that policy makers, the FIU, law enforcement, and supervisors have effective mechanisms in place that enable them to cooperate, and, where appropriate, coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.
Appendix C: FATF Recommendation 32

Countries should ensure that their competent authorities can review 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. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions, and convictions; on property frozen, seized, and confiscated; and on mutual legal assistance or other international requests for cooperation.
The competent authorities should establish guidelines and provide feedback that will assist financial institutions and DNFBPs in applying national measures to combat money laundering and terrorist financing, and in particular, in detecting and reporting suspicious transactions (see Interpretative Note).

**Interpretative Note to Recommendation 25**

When considering the feedback that should be provided, countries should heed the FATF Best Practice Guidelines on Providing Feedback to Reporting Financial Institutions and Other Persons.
The primary goals of a national strategy are to:

- Lay out collective objectives and priorities.
- Better integrate the pillars of the national AML/CFT framework (prevention, detection, law enforcement and prosecution, domestic exchange of information, international cooperation) by
  
  - adopting effective preventive measures, in particular cooperative public-private efforts,
  
  - strengthening interagency collaboration and enhancing information sharing,
  
  - mobilizing the resources needed to implement the national strategy (human, financial, training, and so on), and
  
  - measuring the effectiveness of AML/CFT efforts.

- Align resources accordingly.
- Provide a framework to define qualitative and quantitative targets—and therefore to measure progress and impact.
- Lay out the main constraints to better international cooperation.

In addition, a national AML/CFT strategy constitutes a very good instrument for engaging policy makers and clarifying responsibilities and accountabilities—while raising awareness among the public.
Appendix F: FATF Recommendation 36

Countries should rapidly, constructively, and effectively provide the widest possible range of mutual legal assistance in relation to money laundering and terrorist financing investigations, prosecutions, and related proceedings. In particular, countries should:

a. Not prohibit or place unreasonable or unduly restrictive conditions on the provision of mutual legal assistance
b. Ensure that they have clear and efficient processes for the execution of mutual legal assistance requests
c. Not refuse to execute a request for mutual legal assistance on the sole ground that the offence is also considered to involve fiscal matters
d. Not refuse to execute a request for mutual legal assistance on the grounds that laws require financial institutions to maintain secrecy or confidentiality.

Countries should ensure that the powers of their competent authorities required under Recommendation 28 are also available for use in response to requests for mutual legal assistance, and if consistent with their domestic framework, in response to direct requests from foreign judicial or law enforcement authorities to domestic counterparts.

To avoid conflicts of jurisdiction, consideration should be given to devising and applying mechanisms for determining the best venue for prosecution of defendants in the interests of justice in cases that are subject to prosecution in more than one country.
Appendix G: FATF Recommendation 37

Countries should, to the greatest extent possible, render mutual legal assistance notwithstanding the absence of dual criminality.

Where dual criminality is required for mutual legal assistance or extradition, that requirement should be deemed to be satisfied regardless of whether both countries place the offence within the same category of offence or denominate the offence by the same terminology, provided that both countries criminalise the conduct underlying the offence.
Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

- Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.
- Countries should not invoke laws requiring financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.
- Competent authorities should be able to conduct inquiries, and where possible, investigations, on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with noncounterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorized manner, consistent with their obligations concerning privacy and data protection.

**Interpretative Note**

For the purposes of this Recommendation:

- “Counterparts” refers to authorities that exercise similar responsibilities and functions.
- “Competent authority” refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.
Depending on the type of competent authority involved and the nature and purpose of the co-operation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, and exchanges on the basis of reciprocity or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases, and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions to obtain relevant information.
Countries should take immediate steps to become party to and implement fully the Vienna Convention, the Palermo Convention, and the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.
Each country should afford another country, on the basis of a treaty, arrangement, or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries, and proceedings relating to the financing of terrorism, terrorist acts, and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts, or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

**Guidance notes**

This Recommendation contains five elements:

- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions through mutual legal assistance mechanisms.
- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions by means other than through mutual legal assistance mechanisms.
- Jurisdictions should have specific measures to permit the denial of “safe haven” to individuals involved in terrorist financing.
- Jurisdictions should have procedures that permit the extradition of individuals involved in terrorist financing.
- Jurisdictions should have provisions or procedures to ensure that “claims of political motivation are not recognized as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing.”

To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made for some questions in the (SAQTF) between international co-operation through mutual legal assistance mechanisms on the one hand and information exchange through means other than through mutual legal assistance.
For the purposes of SR V, the term mutual legal assistance means the power to provide a full range of both non-coercive and coercive legal assistance, including the taking of evidence; the production of documents for investigation or as evidence; the search and seizure of documents or things relevant to criminal proceedings or to a criminal investigation; and the ability to enforce a foreign restraint, seizure, forfeiture, or confiscation order in a criminal matter. In this instance, mutual legal assistance would also include information exchange through rogatory commissions (that is, from the judicial authorities in one jurisdiction to those in another).

Exchange of information by means other than through mutual legal assistance includes any arrangement other than those described in the preceding paragraph. Under this category should be included exchanges that take place among FIUs, police, and law enforcement agents or other agencies that communicate bilaterally on the basis of MOU, exchanges of letters, and so on—where required by the domestic legal framework.

With regard to the last three elements of SR V, these concepts should be understood as referred to in the relevant UN documents. These are S/RES/1373 (2001), paragraph 2c (for denial of safe haven); the UN Convention, Article 11 (for extradition); and the UN Convention, Article 14 (for rejection of claims of political motivation as related to extradition). The text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism.asp; the text of S/RES/1373 (2001) may be accessed at http://www.un.org/documents/scres.htm.

The term civil enforcement as used in SR V intended to refer only to the type of investigations, inquiries, or procedures conducted by regulatory or administrative authorities that have been empowered in certain jurisdictions to carry out such activities in relation to terrorist financing. Civil enforcement is not meant to include civil procedures and related actions as understood in civil law jurisdictions.
Answers
Module 5 Answers

Answers 1 and 2
In both cases, you should list some of the following institutions and agencies:

- Ministry of Justice and Prosecutor General
- Ministry of Finance
- Home Affairs/Interior Ministry/investigation agencies/police
- Central Bank and other supervisors/regulators of the financial sector
- Supervisory authorities for the DNFBPs (casinos, corporate service providers, bar associations)
- FIU
- Customs and Tax authorities

In addition, and depending on the depth of the analysis to be undertaken, it may be worthwhile to consider involving:

- Parliamentarians
- Representatives of professions subject to the AML/CFT framework
- Academics
- Representatives of civil society
- Journalists

Answer 3
Your response should mention the professional associations (lawyers, accountants, and so on) affected by the AML/CFT framework. In addition to these associations (depending on how they are organized in your country), it may be useful to involve individual professionals and practitioners to cope with the operational challenges of AML/CFT requirements. Self-regulatory bodies should fall under the same umbrella.

Answer 4
The following pieces of information (the list is not comprehensive) or documentation provide a helpful overview:

- Number of STRs transmitted by the FIU to law enforcement
- Number of AML/CFT-related indictments based on STRs
- Number of AML/CFT investigations launched domestically and those triggered by international cooperation or requests for information
- Number of AML/CFT-related international requests for information/cooperation launched/received by the FIU, police, judges, prosecutors, and/or financial sector supervisors
- Number of asset-freezing, seizing, and confiscating-related international requests sent and received
Other documents that might contain useful information include the annual report of the FIU, AML/CFT national strategy, the annual reports of the financial sector supervisors, and the amount of assets frozen.

Another indicator might be evidenced by the professional experience of the FIU staff and management (i.e., how diverse is it, proportion of staff with backgrounds in law enforcement, transactional and auditing, financial sector supervision, etc.).

**Answer 5**

Excessive bank and professional secrecy is often a key barrier to efficient and timely domestic and international cooperation. FATF Recommendation 4 states: “Countries should ensure that financial institution secrecy laws do not inhibit implementation of the FATF Recommendations.” Central to this recommendation is the setting of clear gateways.

**Answer 6**

1) International gatherings are good opportunities to foster international cooperation through informal meetings. In addition to arranging for adequate domestic coordination before international meetings, countries should consider their delegation’s position on agenda items.

2) Upstream coordination is key before such informal contacts are made at international meetings. In the example provided previously, prior dialogue with domestic agencies would have apprised you of the letter in question.

3) It is also surprising that the banking supervisor was not advised during the interagency discussions to share his concerns regarding international cooperation with his Begunia counterparts. Sharing such information at the domestic level can also help in engaging other countries at higher levels.

4) As for the dinner engagement, and the agreement to discuss international cooperation with regard to specific cases, one-on-one, the decision was risky for several reasons:

   - The issues at stake are not in the purview of the Ministry of Finance and therefore should not be discussed outside normal channels for mutual legal assistance.
   - Legally, you should not have access to individual information.
   - You are not legally a part of the mutual legal assistance process, so interference could jeopardize its success (i.e., specific steps must be followed to ensure that facts and testimony are allowed in a foreign court).

   Practically speaking, agreeing to bilateral discussions without consulting your colleagues is unwise.

5) Finally, it would be crucial to debrief appropriate counterparts—and possibly higher political levels—on the content of the discussion, including financial supervisors if financial institutions did not fully comply with due diligence obligations.
**Answer 7**

Some of the objectives of enhanced domestic coordination are to

- Bolster mobilization, commitment, and guidance at the political level.
- Permanently adapt the AML/CFT framework to identified weaknesses, emerging trends, and challenges.
- Ensure appropriate circulation of information on individual cases among the relevant authorities (usually a narrower set).
- Involve intelligence agencies in the AML/CFT coordination.

**Answer 8**

The FATF standards recommend that the supervisory authorities and the FIU provide feedback to the entities they supervise, on their application of AML/CFT measures (Recommendation 25); cooperation and coordination mechanisms should enable development and implementation of AML/CFT policies (Recommendation 31); and mechanisms for reviewing and monitoring effectiveness of AML/CFT systems should be in place (Recommendation 32). The FATF standards are purposely nonprescriptive on domestic coordination and focus instead on results: this underscores the need to embed domestic coordination tools in the country’s institutional framework. The true test, however, is the existence of efficient domestic coordination. The onus is on countries to evidence that.

**Answer 9**

Your response will likely mention some of the following tools: annual reports, specific confidential reports to institutions reporting on STR patterns, dedicated seminars, bilateral feedback—this may be better suited for minimum feedback on specific STRs and the collective sharing of experiences.

**Answer 10**

Because it is at the heart of AML/CFT expertise and information sharing, the FIU is best suited to conclude memoranda of cooperation.

**Answer 11**

The FATF standards do not specifically require this. However, a national strategy adopted by the government becomes a public document; it can then be an effective tool for fostering interagency coordination and dialogue with the private sector and other stakeholders. Of course, it is not a panacea.

**Answer 12**

Your response should be in the following list:

- Elaborate national objectives and priorities.
- Identify and delegate the new responsibilities/accountabilities that new national objectives/priorities will create.
• Describe how progress toward the achievement of the objectives/priorities and the impact of objectives/priorities will be measured.
• Delegate specific responsibility for interagency coordination and international cooperation.

A written national strategy can ensure coordination by delegating the responsibility, defining the various roles institutions and stakeholders should play, setting guidelines for coordination, and defining the method for measuring effectiveness. The strategy can include information on the following: the frequency for strategy assessment, revision, and by whom; identification of specific priorities; alignment of resources and tools; measures of achievement; awareness raising; and political mobilization. Other mechanisms can be used to achieve these objectives—the AML/CFT legislation itself, or even more informal mechanisms—provided they are credible.

**Answer 13**
The FIU is the only agency that collects and analyzes STRs from all entities. Thus, it has the expertise to analyze and understand reporting patterns of financial institutions. The FIU should share information with supervisory authorities of the various sectors in money laundering and other criminal activities, so supervisory agencies can fine-tune their risk-based framework, compliance policies, and procedures, and ensure the onsite inspection program is designed and prioritized accordingly. In addition, the FIU should keep supervisory authorities informed on the reporting patterns of the entities they supervise, so that inspection could be done more efficiently.

**Answer 14**
Inspectors may gather information on some transactions, which have not been reported to the FIU but are useful to the FIU because it indicates how reporting entities determine whether certain transactions are suspicious (or not). In addition, as focus turns more on “internal controls,” inspectors can inform the FIU on the compliance efficiency in financial institutions—thereby helping the FIU to better target the financial institutions with which it should engage in a more in-depth dialogue to improve suspicious transactions reporting.

**Answer 15**
Your three institutions should be in the following list: FIU, Justice Department, prosecutor general, courts, Ministry of Finance, any of the various law enforcement agencies, financial and non-financial sector regulators, and the central bank.

**Answer 16a**
The answer is B. There is no standard model recognized as the best for all countries; each country has to make its own choice, depending on its own circumstances. However, central to success is having the FIU spearhead domestic coordination and stress multidisciplinary features and staffing.
Answer 16b
The answer is E.

Answer 17
Usually individual information is gathered by and circulated within the FIU, the police, other law enforcement agencies, the prosecution, and the supervisors (mainly of the financial sector). The Customs Authority is privy to relevant information concerning suspicious transactions and can be a major asset to the AML/CFT framework. In some countries, central banks (through cross-border transactions or the freezing of assets) may also have important information that should be shared, but measures must be taken to protect confidential information; some of these measures are banking secrecy and prosecution secrecy. In any event, procedures for information sharing need to be clear and reasonable. There are also jurisdictions with informal channels of communication and their benefits should not be underestimated. It is critical that the fundamental rights of individuals are not violated and that abuse or misuse of information is punished.

Such agencies as the Ministry of Finance, the Ministry of Foreign Affairs, and supervisory bodies outside the financial sector are less likely to have access to individual information—but can participate in the policy-oriented exchanges of information and experience.

Answer 18
The following list could provide a useful reference:

- The total number of MOU signed with foreign counterparts—for the exchange of information
- The total number of requests for international assistance received from foreign counterparts
- The total number of requests for international assistance sent to foreign counterparts
- The total number of prosecution cases triggered by analysis and/or information, obtained from foreign counterparts
- The average time (number of days) it takes for the FIU to respond to requests from international counterparts

Answer 19
The following list could provide a reference:

- The total number of requests for international cooperation received by the FIU, which led to domestic inquiries directed to the financial sector supervisors or the police
- The total number of international requests for information received by the banking supervisor, which led to domestic inquiries directed to the FIU
• The total number of regulator to regulator requests for assistance launched by the banking supervisor, and directed to counterparts in countries where there are branches or subsidiaries of domestic banks
• The comparison of the distribution of all MOU signed by domestic AML/CFT entities with the structure (geographical dimensions) of international transactions (ins and outs)

**Answer 20**
Jurisdictions with relatively liberal tax regimes do not want their foreign investors to be concerned that their financial information can be communicated to authorities in other countries, which may then be used to prosecute cases of tax evasion. Such countries put restrictions (spelled out in MOU on information, which could be tax related). This approach can be legitimate but has been abused by some jurisdictions as a means to withhold information that could be used for criminal investigation purposes. It is critical that authorities make it very clear what the criteria and decision-making processes are for sharing information at the international level, when there are tax-related restrictions. Restrictions should not impede the sharing of data needed for the prosecution of criminal cases having to do with financial activities.

**Answer 21**
Those are the Vienna Convention (UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances [1988]), the UN Convention for the Suppression of the Financing of Terrorism (1999), and the Palermo Convention (The UN Convention against Transnational Organized Crime [2000]). In addition, even though it is not mentioned in the FATF Recommendations, the UN Convention against Corruption (2003) is another key international instrument to be signed, ratified, and integrated into the domestic legal framework.

**Answer 22**
Those are the prevention stage between regulators, the prevention and detection stage between FIUs, the investigative stage between police and law enforcement, and the prosecution stage in the context of mutual legal assistance.

**Answer 23**
Each country has its own mechanisms and institutions to provide international assistance, be it mutual legal assistance or through other forms. Depending on the country setting, the institutions involved might not be the same. For instance, in countries where the FIU is involved in supervising the compliance of financial institutions with AML/CFT requirements, it can be the counterpart of financial supervisors (banking/securities/insurance commissions) from other countries. Clarity on the “entry points,” on the mandates of the various bodies and procedures for international assistance, is key to facilitating requests from other countries and ensuring effectiveness by streamlining the bureaucratic process.
Answer 24
False: The scope of the FIU mission can have a bearing on the effectiveness of the coordination efforts, but what is most important is the integration of the functions and the ability to rely on cross-sectoral and interdisciplinary expertise. A large sphere of activity of the FIU can create tensions with other agencies at the expense of coordination and sharing of experiences. The Bank Supervision Agency should generally be responsible for supervising bank compliance with AML/CFT requirements; however, the FIU should work with the bank supervisory agency to assist in training bank supervisors and to provide information, if necessary.

Answer 25
False: The FIU has a leading role in providing feedback to illustrate the importance of STRs to reporting institutions and provide guidance on AML/CFT trends. But feedback from the police and the Justice Department/prosecutor’s office is also central, as the final objective of AML/CFT is to incarcerate criminals.

Answer 26
True: An AML/CFT strategy can be a useful tool at the domestic level to foster the fight against ML/FT and, in particular, to support domestic coordination efforts, but it is only best practice and not an FATF Recommendation. However, such an approach is a good benchmark to assess other options, increase awareness, improve domestic coordination, and measure progress.

Answer 27
False: Involving and associating the private sector is central to the effectiveness of AML/CFT efforts, as they strongly depend on private sector acceptance of the “partnership spirit” underlying it, particularly where reporting mechanisms are concerned. Taking into account its views and keeping track of implementation issues is central. Of course, this may lead in some instances to debates or disagreements, but they are usually better solved by acknowledging them than by trying to hide them.

Answer 28
True: Measurement of coordination is indeed difficult, as it is a qualitative endeavor. However, several indicators and proxies can help gain an objective assessment.

Answer 29
False: The UN Convention for the Suppression of the Financing of Terrorism is another key instrument. Other key multilateral instruments that have a regional basis but provide very important references are conventions adopted by the Council of Europe and the Organization of American States.
Answer 30
False: The spirit of the FATF Recommendation 40 is to go beyond counterparty-to-counterparty international assistance. When legal restrictions are placed on such exchanges of information, it is expected that the agency in country Z will help the requesting agency use appropriate gateways to gain assistance.

Answer 31
False: Participating in international cooperation is essential to each country’s AML/CFT efforts, as AML/CFT schemes are more often than not cross-border transactions.

Answer 32
True: Formal international cooperation is of course important, in particular when it comes to mutual legal assistance. However, there are other informal means of cooperation, based on trust and bilateral relationships, that also facilitate such cooperation.

Answer 33
False: Although professional associations are able to disseminate information en masse to their constituencies, direct contact with practitioners is indispensable. In addition, cross-sector dialogues bring two important benefits: benchmarking between sectors (experience gathered from the banking sector can be shared with others) and experience sharing. Cross-sector exchanges increase the sense of common ground and collective mobilization.

Answer 34
False: This is a key monitoring tool, but success in managing international cooperation also stems from the ability and willingness to request support and information from abroad and the information provided has value.

Answer 35
False: As in other endeavors, staff exchanges are very useful in fostering cooperation and dialogue. It helps in improving mutual understanding—and this is particularly relevant in context of significant differences in culture—in devising gateways and in promoting the adoption of new ways of doing business. However, confidentiality issues must be considered.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

Module 1: Effects on Economic Development and International Standards
Module 2: Legal Requirements to Meet International Standards
Module 3a: Regulatory and Institutional Requirements for AML/CFT
Module 3b: Compliance Requirements for Financial Institutions
Module 4: Building an Effective Financial Intelligence Unit
Module 5: Domestic (Inter-Agency) and International Cooperation
Module 6: Combating the Financing of Terrorism
Module 7: Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
6

Combating the Financing of Terrorism

Workbook

THE WORLD BANK
Combating the Financing of Terrorism

Workbook
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**Module 1: Effects on Economic Development and International Standards**
Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**Module 2: Legal Requirements to Meet International Standards**
Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**Module 3a: Regulatory and Institutional Requirements for AML/CFT**
Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**Module 3b: Compliance Requirements for Financial Institutions**
Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

The initial work was provided by Emiko Todoroki and Azuma Miura, the World Bank. Module 6 was further written and developed by Stuart Yikona and Eric Robert, International Monetary Fund. The draft was reviewed by Pierre-Laurent Chatain, the World Bank, and Walter Gehr and Irka Kuleshnyk, United Nations Office on Drugs and Crime. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by Emiko Todoroki and John McDowell, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Heba Mahmoud Mokhtar Shamseldin, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include “Financial Action Task Force on Money Laundering,” “The Forty Recommendations, 2003, Special Recommendations on Terrorist Financing, 2005,” and Paul Allan Schott, Reference Guide to Anti–Money Laundering and Combating the Financing of Terrorism, Second Edition with Supplement on Special Recommendation IX, the World Bank, 2004.

Capacity Enhancement Program on Anti–Money Laundering and Combating the Financing of Terrorism

Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The module starts with a brief review of the CFT issues raised in the previous modules, addresses some general questions related to CFT, and then discusses the Financial Action Task Force (FATF) Nine Special Recommendations on Terrorist Financing in combination with the international obligations of states. The Module covers the following issues:

1. **What does terrorist financing mean?** 4

2. **International norms and standards on CFT** 8
   - 2.1 The SFT Convention of 1999 8
   - 2.2 Resolutions of the UN Security Council 9
   - 2.3 The Nine FATF Special Recommendations on Terrorist Financing 9
   - 2.4 The UN Comprehensive Convention on International Terrorism 9
   - 2.5 Other international treaties on combating the financing of terrorism 10
   - 2.6 Human rights and financing of terrorism 10

3. **Is combating terrorist financing mandatory?** 11
   - 3.1 Are UN Security Council Resolutions binding on UN member states? 11
   - 3.2 The FATF Special Recommendations are emerging standards 12

4. **The targets of international policies on CFT** 13
   - 4.1 Individuals 13
   - 4.2 Groups and organizations 13
   - 4.3 Private sector 14
   - 4.4 States 14

5. **Ratification and implementation of UN instruments** 16
   - 5.1 What steps should be taken? 16
   - 5.2 What more should be done? 17
6. **Offenses to be criminalized**  
6.1 How is the offense of financing of terrorism defined? 18

7. **Freezing, seizing, and confiscating terrorist assets**  
7.1 Freezing, seizing, and confiscation: what are the differences? 20  
7.2 Taking the measures against terrorists’ assets 21  
7.3 Setting up the necessary national legal framework 22  
7.4 Challenges 22

8. **Reporting suspicious transactions related to terrorism**  
8.1 Under what circumstances should a transaction be reported? 24  
8.2 Challenges 25  
8.3 What types of institutions are expected to submit reports? 25

9. **Enhancing international cooperation**  
9.1 Mutual legal assistance 27  
9.2 Extradition of offenders and other forms of cooperation 28  
9.3 Challenges: A good legal framework is meaningless if states are not proactive 28

10. **Measures required for alternative remittance systems** 30

11. **Measures required for wire transfers** 33  
11.1 What is a wire transfer? 33  
11.2 What is the FATF’s standard on wire transfers? 34  
11.3 Who is covered by the wire transfer standard? 34

12. **Dealing with cash couriers** 36  
12.1 Why monitor cross-border transportation of cash? 36  
12.2 What is targeted? 36  
12.3 What sort of action is required? 37  
12.4 Implementation of sanctions 38  
12.5 Challenges to the implementation of FATF Special Recommendation IX 38

13. **Supervising nonprofit organizations and other legal entities** 40  
13.1 What entities should be under scrutiny? 40  
13.2 What kind of oversight is needed? By whom? 41
This module introduces

- the nine FATF Special Recommendations on Terrorist Financing.
- relevant resolutions of the United Nations Security Council (UNSC).
- the UN Convention for the Suppression of the Financing of Terrorism.

At the end of the module, you will be able to

- explain what countries must do to prevent, detect, and prosecute the financing of terrorism and terrorist acts;
- understand the rationale for combating the financing of terrorism;
- name the international conventions and resolutions that should be ratified and implemented;
- list the type of offenses that should be criminalized;
- clarify the meaning of freezing and confiscating terrorist assets;
- explain when to file suspicious transaction reports (STRs) related to the financing of terrorism;
- describe alternative remittance systems, wire transfers, cash couriers, and measures to prevent the financing of terrorism through such means; and
- discuss the relationship of nonprofit organizations to the financing of terrorism.
What does terrorist financing mean?

How much do you know?

Let us review what we discussed on the financing of terrorism in the previous modules. Please answer the following questions, using the space below each to jot down your thoughts if necessary.

**QUESTION 1.** What is the financing of terrorism?

**QUESTION 2.** What is the main difference between money laundering and terrorist financing? Select one.

a) They are the same.

b) Money laundering is done by criminals and noncriminals, whereas terrorist financing is done by terrorists only.

c) Money laundering involves only ill-gotten money, whereas terrorist financing involves both ill-gotten money and legitimate money.

**QUESTION 3.** What are the implications of terrorist financing for developing economies?
Valachia is a province of Rurithania. A group calling itself the Liberation Front of Valachia is fighting for independence. For many years, the group has bombed police stations and infrastructure. Free Valachia, a political party active in the province, also favors independence. It has condemned the police measures that the Rurithanian government has taken against members of the Liberation Front of Valachia. The government of Rurithania is considering sharing with foreign countries the names of members and representatives of both groups. Its goal is to seize their assets on the grounds that the Free Valachia party is supporting the Liberation Front of Valachia. To what extent could international norms on terrorist financing apply to such a situation?
To answer that question, one must understand what terrorism means.

Terrorist financing, you will recall, is providing financial support for terrorism or for those who encourage, plan, or engage in terrorism. Although that appears at first glance to be a very simple concept, the case of Valachia shows how complex the issues may be. Most of the difficulty lies in reaching agreement on what constitutes terrorism.

The financing of terrorism is defined by the UN Convention for the Suppression of the Financing of Terrorism (SFT Convention, 1999).

Financing of terrorism occurs when a person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that these should be used or in the knowledge that these will be used in full or in part, to carry out a terrorist act as defined in the above-mentioned convention.

But where can we find a definition of terrorism (as distinct from terrorist acts)?

- Not in the SFT Convention.
- Not in the UNSC resolutions on terrorism.
- Not in the UN’s comprehensive convention on terrorism—because the negotiations on the draft convention have stalled on precisely this question.

Terrorist acts, by contrast, are well defined:

- The SFT Convention defines a terrorist act as an “act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.”

Keep in mind that specific international conventions deal with particular types of terrorist activities. The SFT Convention includes the offenses set forth in nine treaties among the crimes that must be considered as acts of terrorism.

The Annex to the SFT Convention sets out the list of the nine international treaties that pertain to terrorist crimes, as follows:

1) Convention for the Suppression of Unlawful Seizure of Aircraft, at The Hague on December 16, 1970
2) Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, in Montreal on September 23, 1971
3) Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the UN on December 14, 1973
Knowledge check

QUESTION 5. Is it legitimate to finance terrorist acts if the financier’s motives are political or religious?

a) True  b) False

QUESTION 6. Are political actions such as strikes and peaceful demonstration acts of terrorism?

a) True  b) False

QUESTION 7. Are the actions of people against foreign occupation considered acts of terrorism?

QUESTION 8. Now back to the question posed in the introductory story. Do international standards on the financing of terrorism apply to the situation in Valachia? Think about your solution and then look for the answer.
Is international cooperation against terrorism:

a) A new issue,
b) A very old issue, or
c) An issue since the terrorist attacks of September 11, 2001?

The answer is b. Terrorism is a very old phenomenon, but international cooperation against terrorism began only in the 1970s. Since then, international treaties have addressed specific types of terrorist threats, such as the unlawful seizure of aircraft. For more information, see the list of treaties. In addition, in the past 10 years, the UN has intensified its efforts to combat terrorism. The SFT Convention was negotiated in the UN General Assembly and adopted in 1999. In the UNSC, the system of sanctions adopted against the Taliban in 1999 was a turning point. The terrorist attacks of September 11 triggered a qualitative jump in the scope and specificity of the measures that states must take to combat terrorism.

2.1 The SFT Convention of 1999

The SFT Convention had been ratified by just a few states before September 11, 2001. After September 11, member states were pressed to ratify the convention by UNSC Resolution 1373 (2001) and the FATF Special Recommendations. As of March 2007, with 156 parties, the convention is the most comprehensive international instrument for combating the financing of terrorism.

States that ratify this convention must:

• Establish in their criminal legislation the offense of financing terrorism
• Cooperate with other state parties and provide them with legal assistance
• Enact legislation concerning the role of financial institutions in the detection and reporting of evidence of terrorist financing
• Take appropriate measures for the identification, detection, and freezing or seizure of any funds used or allocated for the purpose of committing the financing of terrorism criminal offense as well as the proceeds derived from such offense, for purposes of possible confiscation.
2.2 Resolutions of the UN Security Council
The UNSC has been a driving force in combating the financing of terrorism. It has adopted two major resolutions.


**What is the objective of Resolution 1267?**
Resolution 1267 targets specific individuals, entities, or groups—among them Osama bin Laden, Al-Qaeda, and the Taliban—for the purpose of restoring peace and suppressing threats to international security. With respect to the financing of terrorism, its major application is to freeze the assets of the named individuals and entities. The legal regime set up by resolution 1267 (1999), and modified by the resolutions 1333 (2000) and 1390 (2002), has been adapted to new resolutions.

2) Resolution 1373 (2001)

**What is the objective of Resolution 1373?**
Resolution 1373 targets international terrorism in general. It was adopted after the attacks of September 11, 2001, but it is not aimed at identifying or punishing the perpetrators of the attacks. Instead, the resolution provides a set of measures (including the freezing of terrorist assets) aimed at combating terrorism and its financing. A Counter-Terrorism Committee set up under the resolution is responsible for monitoring its implementation by the members of the UN.

2.3 The Nine FATF Special Recommendations on Terrorist Financing
The FATF Special Recommendations were an immediate response to the events of September 11, 2001. Adopted in October 2001 and October 2004, they extend the FATF Forty Recommendations on money laundering to cover the particularities of terrorist financing. They also cover certain issues in greater detail than do the SFT Convention and UNSC Resolution 1373 (2001). The Special Recommendations also introduce new issues.

2.4 The UN Comprehensive Convention on International Terrorism
In 2002, the UN General Assembly began work on a comprehensive convention on international terrorism. When adopted, the convention will complement existing treaties by providing a universal convention that addresses globally the problems of terrorism. As noted above, negotiators are having trouble with the definition of terrorism and the scope of the convention.
2.5 Other international treaties on combating the financing of terrorism

Because combating the financing of terrorism is part of a broad international effort, other international instruments also can be used in this fight. Those instruments include the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention, 1988), the UN Convention against Transnational Organized Crime (the Palermo Convention, 2000), and the UN Convention against Corruption (the Merida Convention, 2003). At the regional level, one might cite the following Council of Europe conventions: the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds of Crime (the Strasbourg Convention, 1990); the Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (the Warsaw Convention, 2005); and the European Convention on the Suppression of Terrorism (1977) with the Amending Protocol (2003).

Examples of the possible connection between terrorism and other types of criminal activities

**Italy**

In April 2004, a top Italian anti-Mafia prosecutor announced evidence of links between the Italian Mafia and Muslim terrorist groups in Italy. According to the statement, the two groups had forged links in arms and drug trafficking.

**United States**


2.6 Human rights and financing of terrorism

States’ obligations to combat the financing of terrorism do not override their other international obligations, especially the observance of human rights. In other words, the necessity to combat terrorism efficiently cannot be used as justification for not applying human rights standards. The UNSC has recently affirmed this principle (see paragraph 6 of UNSC Resolution 1456). With respect to the fight against terrorist financing, this means that countries must respect human rights and due process when designing and implementing procedures for freezing, seizing, and confiscating terrorists’ assets.

Paragraph 6 of UN Security Council Resolution 1456 (2003) states, “States must ensure that any measures taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee, and humanitarian law.” For more information on this issue see the Council of Europe’s “Guidelines on Human Rights and the Fight against Terrorism.”
Is combating terrorist financing mandatory?

States are bound by international law to put in place certain policies and to ensure that their legislation complies with international norms and standards. Laws aside, the political cost of not acting against the financing of terrorism is clear. Few countries would wish to become known as havens for financial activities related to terrorism. As we have seen, money launderers are always looking for jurisdictions that are less stringent in their regulation of financial activities. The financiers of terrorism are likely to favor the same jurisdictions.

Concerns

The secretary general of the Pacific Islands Forum expressed his concern about the area becoming a weak link in the fight against terrorism and organized crime unless adequate measures were taken. Small island states are especially vulnerable to abuse because many lack strong uniform laws and have inadequate human, financial, and technical resources.

3.1 Are UN Security Council Resolutions binding on UN member states?

Not all UNSC Resolutions are binding. But when a resolution is adopted on the basis of Chapter VII of the UN Charter—because the situation is deemed a threat to international peace and security—the “decisions” reported in the resolution bind all member states. This is the case for the following resolutions on terrorism: 1267 (1999), 1333 (2000), 1373 (2001), and 1390 (2002). The “recommendations” presented in the same resolutions, however, are nonbinding.

However, states are bound to respect the terms and provisions of the treaties they sign and ratify. States that have ratified the SFT Convention have a legal obligation to incorporate the treaty into their domestic legislation. Those that have signed but not yet ratified the convention have at least a good faith obligation to refrain from taking actions incompatible with the legal framework of the treaty. Note that UNSC Resolution 1373 (2001) and the FATF Special Recommendations call upon the member states to become parties to the SFT Convention.
3.2 The FATF Special Recommendations are emerging standards

The FATF Special Recommendations are not a binding international convention; however, many countries have made a political commitment to combat terrorist financing by implementing the FATF Special Recommendations along with the FATF Forty Recommendations. In addition, the Boards of the World Bank and International Monetary Fund (IMF) have endorsed the FATF Special Recommendations and added the Special Recommendations to the list of standards and codes that are relevant to their operational work. As part of the evaluations conducted by the FATF, FATF-Style Regional Bodies (FSRBs), the World Bank, and the IMF, countries are now assessed on their CFT efforts based on the FATF Special Recommendations.

**UN Security Council Resolution 1526 (2004)**

Paragraph 4 of UNSC Resolution 1526 (2004) “calls upon States to move vigorously and decisively to cut the flows of funds and other financial assets and economic resources to individuals and entities associated with the Al-Qaeda organization, Osama bin Laden and/or the Taliban, taking into account, as appropriate, international codes and standards for combating the financing of terrorism, including those designed to prevent the abuse of nonprofit organizations and informal/alternative remittance systems” (emphasis added).

**Is that enough?**

The international standards established by the FATF describe minimum standards that states should meet. However, countries need not be satisfied with the minimum. It is important to look at best practices. For instance, in the case of the FATF Special Recommendations, “International Best Practices (SRIII, SRVI, SRVIII, and SRIX)” are providing practical and appropriate ways to implement the standards.

**What did you learn?**

- Combating the financing of terrorism is an inescapable obligation of all states.
- The formal obligations of individual states may vary slightly depending on whether they have ratified the SFT Convention.
- The international standards define the *minimum* acceptable conduct. States can always adopt a stricter regime.
Individuals, groups, organizations, and even states may be involved at different stages of terrorist activity. International standards deal with that involvement in different ways.

4.1 Individuals

Certain rules are directed against individuals. The UNSC has expressly mentioned Osama bin Laden as a person targeted by a regime of sanctions. Other individuals, without being named in the resolutions themselves, have been added to the list of persons (individuals or legal entities) targeted by the sanctions committee set up by under the UNSC Resolution 1267 (1999), (hereafter the ‘1267 Committee’), because of their presumed links with the Al-Qaeda organization or the Taliban. The 1267 Committee, an organ of the UNSC, reviews the list periodically, based on information provided by UN member states.

*Individuals: Osama bin Laden*

Resolution 1333 (2000) contains the decision “that all States shall […] freeze without delay funds and other financial assets of Osama bin Laden and individuals and entities associated with him as designated by the Committee, including those in the Al-Qaeda organization, and including funds derived or generated from property owned or controlled directly or indirectly by Osama bin Laden and individuals and entities associated with him, and to ensure that neither they nor any other funds or financial resources are made available, by their nationals or by any persons within their territory, directly or indirectly for the benefit of Osama bin Laden, his associates or any entities owned or controlled, directly or indirectly, by Osama bin Laden or individuals and entities associated with him including the Al-Qaeda organization.” (paragraph 8,c)

4.2 Groups and organizations

Some UNSC resolutions have targeted groups and organizations, such as the Taliban and Al-Qaeda. The 1267 Committee has some 100 groups or entities, such as the Jemaah Insamıyah, connected to Al-Qaeda.
4.3 Private sector

The private sector is not the immediate target of international rules and standards on combating terrorist financing. Bankers and money-transfer operators are called upon to implement policies to combat the financing of terrorism, but because the international standards are not immediately transferable to national systems of regulation and enforcement, individual states must ensure that private sector practice conforms with the goals set by the international standards. In practice, this usually means that states must adopt implementing legislation and regulations to guide enforcement of AML/CFT requirements.

Private sector compliance

FATF Special Recommendation VI states that “each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and nonbank financial institutions.” (Emphasis added.)

4.4 States

States are the main target of international rules on combating terrorist financing—as set forth, for example, in the SFT Convention, UNSC resolutions, and the FATF Special Recommendations. Even when rules are directed against individuals or groups, states are bound to take certain actions.

Groups and organizations: Entities belonging to or associated with the Al-Qaeda organization

<table>
<thead>
<tr>
<th>Entity identifiers</th>
<th>Alias</th>
<th>Address</th>
<th>Listed on</th>
<th>Other information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Jemaah Islamiyah</td>
<td>A.k.a.:</td>
<td></td>
<td>Oct. 25, 2002</td>
<td>The network in Southeast Asia. Founded by the late Abdullah Sungkar.</td>
</tr>
<tr>
<td>a) Jema’ah Islamiyah</td>
<td></td>
<td>Address:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>b) Jemaah Islamiya</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c) Jemaah Islamiah</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d) Jamaah Islamiyah</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>e) Jama’ah Islamiyah</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.k.a.:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

What have you learned?

- States are the main target of international rules and standards on combating terrorist financing.
- In the fight against terrorism, specific individuals and entities have been targeted for action at the international level.
- States are obliged to ensure that international standards and treaty obligations are implemented through their national legislation and that the legislation is enforceable and is enforced.

State compliance

Resolution 1373 (2001) provides “that all States shall [...] prevent those who finance, plan, facilitate or commit terrorist acts from using their respective territories for those purposes against other States or their citizens.” (Paragraph 2d, emphasis added.)
Ratification and implementation of UN instruments

Let us analyze a hypothetical scenario to understand these issues.

Case study: Rurithania

For many years, the state of Rurithania has had antiterrorist legislation aimed at combating terrorism at the domestic level. However, it has passed no law regarding international cooperation in the fight against terrorism. The question of preventing the abuse of the financial system by terrorist financiers is ignored in Rurithanian law because it was not an issue at the time the original antiterrorism legislation was adopted. Can Rurithania claim that it is in compliance with its international obligations and that its present legal framework is enough? Does the fact that Al-Qaeda and related organizations are not present in the country provide support for this assertion?

FATF Special Recommendation I requires states to ratify the SFT Convention and to implement relevant UNSC Resolutions on terrorist financing. For more information on FATF Special Recommendation I, see Appendix B.

5.1 What steps should be taken?

Every country should take immediate steps to ratify and implement fully the SFT Convention.

- Ratification means that states take legislative or executive steps to approve the convention.
- Implementation means that states adopt policies and measures, including legislation if needed, to ensure effective implementation of the SFT Convention under the state’s national legal system.

States should also take steps to implement UNSC Resolutions relating to the prevention and suppression of terrorist financing. Resolution 1373 (2001) is of primary importance for domestic legislative regimes. But Resolution 1267 (1999) and subsequent related resolutions also are important in defining the legal regime of sanctions against presumed terrorist individuals and entities.
5.2 What more should be done?

The members of the UN also have a duty to collaborate with the Counter-Terrorism Committee and the 1267 Committee:

- By providing feedback on their implementation measures in the form of periodic reports
- By supplying information on suspected terrorists or terrorist entities to be included on the list of the 1267 Committee
- By contributing to the removal of names that should no longer appear on the list.

FATF Recommendation 35 requires that other instruments should be ratified as well—among them the Palermo Convention on organized crime and the Vienna Convention on illicit drug trafficking. Countries should take immediate steps to become party to, and implement fully, the Vienna Convention, the Palermo Convention, and the 1999 UN International Convention for the Suppression of the Financing of Terrorism. Countries are also encouraged to ratify and implement other relevant international conventions, such as the 1990 Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime and the 2002 Inter-American Convention against Terrorism.

Note that in addition to these conventions, Resolution 1373 (2001) calls upon states to become party to other treaties related to the fight against terrorism.

QUESTION 9. Let us return now to the case on Rurithania. Can Rurithania assert that it has complied with its international obligations and that its existing legal framework is enough? Does the fact that Al-Qaeda and related organizations are not operating in the country support that assertion? Think about your solution, and jot down your answers in the space provided below.
FATF Special Recommendation II requires that countries criminalize terrorist financing, terrorist acts, and terrorist organizations. It is not sufficient to criminalize money laundering; the financing of terrorism must be criminalized as a separate offense. For more information on FATF Special Recommendation II, see Appendix C.

6.1 How is the offense of financing of terrorism defined?

The offense of financing of terrorism occurs when a “person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out” a terrorist act, by a terrorist organization or an individual. There are two key elements: the mental and material elements.

- The mental element – This means that the act must have been done willfully and intentionally, or with knowledge of the illegal intent of the use of the funds.
- The material element – Broadly defined, this means that there is the fact of providing or collecting funds.

Knowledge check

QUESTION 10. Does the simple fact of collecting funds for use in terrorist activity constitute the criminal offense of terrorist financing?

a) Yes  b) No

QUESTION 11. Is attempting to finance terrorism also an offense?

a) Yes  b) No

QUESTION 12. If terrorist financing occurs in a different jurisdiction, can it be prosecuted? Should it be?

a) Yes  b) No
QUESTION 13. What are the appropriate penalties for individuals and entities convicted of financing terrorism?

QUESTION 14. What is the link between the offense of terrorist financing and money laundering?
Freezing, seizing, and confiscating terrorist assets

Let us start by determining which of the following figures represent the total amount of terrorist assets blocked in the United States in 2003:

- a) $8,000,500
- a) $5,991,931
- b) $771,956
- c) $300,589

The answer is b. The assets blocked under three U.S. antiterrorist programs were as follows in 2003:

- AL-QAEDA: $771,956
- HAMAS: $5,196,634
- PALESTINIAN ISLAMIC JIHAD: $17,746
- KAHANE CHAI: $201
- TALIBAN: $5,394
- Total assets: $5,991,931

A key tenet of the fight against terrorism is that breaking the chain of financing will diminish terrorists’ capacities to carry out terrorist acts. If the financing chain is to be broken, countries must be able to take legal steps against the funds on which terrorists and their organizations depend. *Freezing, seizing, and confiscation* are the three major legal tools available for that purpose.

7.1 Freezing, seizing, and confiscation: what are the differences?

- *Freezing* indicates prohibition by a court or other competent authority of the transfer, conversion, disposition, or movement of property. The frozen funds or assets remain the property of the owner and under the administration,

---

control, or management of the financial institution that held the funds at the time of freezing.

- **Seizing** means prohibiting the transfer, conversion, disposition, or movement of property, but with the added qualification that the court or other competent authority temporarily assumes custody or control of the property. The assets or funds remain the property of the owner, but possession, administration, and management of the asset is taken over by a relevant competent authority or a court.

- **Confiscation**, which includes forfeiture, means the permanent deprivation of funds or other assets by order of a court or other competent authority, which transfers the ownership of funds or assets from the original owner to the state.

The objectives of these measures differ. The goal of freezing assets is preventive—to deprive the owner of control over the assets to prevent them from being spent or dispersed. Seizing and confiscation have both a preventive and a punitive objective: to deter future criminal acts by seizing property, temporarily or permanently.

### 7.2 Taking the measures against terrorists’ assets

Freezing, seizing, and confiscation are dealt with in slightly different ways in the SFT Convention, the UNSC Resolutions, and the Special Recommendations. FATF Special Recommendation III states that each country should immediately implement measures to freeze funds or other assets belonging to terrorists, those who finance terrorism, and terrorist organizations, in accordance with UN resolutions relating to the prevention and suppression of the financing of terrorist acts. In addition, the FATF recommends the adoption and implementation of measures for the seizure and confiscation of assets. For more information on FATF Special Recommendation III, see Appendix D.

The UNSC Resolutions impose on states an obligation to freeze terrorists’ assets. Resolution 1267 (1999) ordered the freezing of the assets of specific individuals and entities, whereas Resolution 1373 (2001) put in place a general obligation of states to freeze terrorist assets and left to each country the choice of the means to be used for that purpose. States may have national lists of terrorists and terrorist entities.

---

**Resolution 1373 and specially designated nationals**

**Resolution 1373**

Resolution 1373 (2001) calls for states to “freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting
The SFT Convention is the most comprehensive of all the instruments under discussion. It requires not only the freezing, seizing, and confiscation of the assets of terrorists, but it also obliges states to be able to identify and detect them.

### 7.3 Setting up the necessary national legal framework

FATF Special Recommendation III requires countries to “adopt and implement measures, including legislative ones, that would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organizations.” The FATF recommends similar legislative measures with respect to cash couriers. States should be able to stop or restrain currency or bearer instruments suspected to be related to the financing of terrorism or money laundering (see section 13, Supervising non-profit organizations and other legal entities, in this module).

In addition to having in place a legislative and administrative framework for freezing and confiscating terrorist assets, states are expected to designate “competent authorities” to assume these missions. In practice, this means that states must:

- Have effective systems for communicating information on the freezing of terrorist assets to the financial sector through the relevant agencies
- Have an adequate level of coordination among customs, immigration, and other related authorities for the purpose of preventing cash couriers from contributing to terrorist financing and money laundering
- Ensure that authorities have been designated to give effect, as needed, to freezing actions undertaken by foreign jurisdictions.

### 7.4 Challenges

Tracking the funds and assets of terrorists is a difficult and daunting task. On average, the seizure and confiscation of assets from terrorists and terrorist organizations are not large.
Another difficulty is that compared with other operations of military nature, terrorist attacks are relatively cheap to finance. For example, the IRA bomb attempt of the British Cabinet in 1984 probably costs less than £10,000.

Knowledge check

**QUESTION 15.** What should be targeted for seizures? Funds, assets, or properties?

a) Funds
b) Assets
c) Properties
d) All of the above

**QUESTION 16.** Mechanisms for freezing, seizure, and confiscation should be compatible with the rule of law.

a) True  b) False

For discussion

How are the three concepts—freezing, seizing, and confiscation—implemented in your country? What entity is responsible for freezing, seizing, and confiscating the assets of terrorist financiers?
Reporting suspicious transactions related to terrorism

According to FATF Special Recommendation IV, financial institutions should promptly report suspicious transactions to 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.” For more information on FATF Special Recommendation IV, see Appendix E.

As a prerequisite to the obligation to report suspicious transactions, financial institutions are required to implement customer due diligence (CDD) obligations (Article 18 of the SFT Convention).

8.1 Under what circumstances should a transaction be reported?

The FATF standard recommends filing a report with the relevant authority under the following circumstances:

- When it is suspected that funds are linked to terrorist financing, or
- When there are reasonable grounds to suspect that funds are linked to terrorist financing.

The first criterion, suspicion, entails a subjective analysis. The second, reasonable grounds, requires reporting under a broader set of circumstances and relies on an objective analysis. The same idea is reflected in Article 18 of the SFT Convention, which refers to unusual and suspicious transactions. The provision explains that “the unusual character of an operation” covers “all complex, unusual, large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose.”

Case study

An individual’s account activity and inclusion on a UN list indicate a possible link to terrorist activity

An individual residing in a neighboring country maintained a demand deposit account and a savings account in country N. The bank that maintained the accounts noticed in April 2001 that funds were being gradually withdrawn from the accounts. At that point it decided to monitor the accounts more closely.

The bank’s suspicions were reinforced when a name very similar to the account holder’s appeared in the consolidated list of suspected persons and entities issued by the UNSC’s Committee on Afghanistan (UNSC Resolution 1333/2000). The bank immediately filed a report with the financial intelligence unit (FIU) in country N.

—continued
8.2 Challenges

It should be acknowledged that the possibility that a bank or other financial institution will be able to identify an operation as involving terrorist financing is relatively low. Unless a bank identifies a party to a transaction as a terrorist (for example, because his name appears on a list of suspected terrorists), the most it can normally do is to review transactions and report those that appear to be suspicious.

8.3 What types of institutions are expected to submit reports?

Banks and nonbank financial institutions should comply with the country’s AML/CFT laws and regulations. The FATF recommends that the following types of financial institutions should be subject to compliance:

- Banks
- Bureaux de change (currency exchange offices)
- Stockbrokers
- Insurance companies
- Money transfer services

In addition, other businesses and professions that are subject to national AML/CFT laws should be covered by the reporting requirement—note, however, that some of the covered businesses and professions are only required to report for certain types of activities. The covered businesses and professions include:

- Casinos (including Internet casinos)
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Lawyers, notaries, other independent legal professionals, and accountants
- Trust services and providers of company service providers

The FIU analyzed the financial movements relating to the individual’s accounts using records requested from the bank. It appeared that both of the accounts had been opened in 1990 and had been fed primarily by cash deposits. In March 2000, the account holder made a sizeable transfer from his savings account to his checking account. Those funds were used to buy a single-premium life insurance policy and to purchase certificates of deposit.

From mid- to late April, there were transfers from the savings account to his demand deposit account. Those funds were then transferred by check to persons and companies located in neighboring countries and in other regions. In May and June 2001, the individual sold the certificates of deposit he had purchased and transferred the profits to the accounts of companies based in Asia and to that of a company in his country of origin. The individual also cashed in his life insurance policy before the maturity date and transferred the proceeds to an account at a bank in his country of origin. The last transaction was carried out on August 30, 2001, shortly before the September 11 attacks in the United States. Finally, the anti–money laundering unit in the individual’s country of origin sent to country N information on suspicious operations carried out by the account holder and by the companies that received the transfers. Many of these names also appeared in the files of the FIU. The case is currently under investigation.

Lawyers, notaries, other independent legal professionals, and accountants are required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction related to specific listed activities (see FATF Recommendation 12.d). These activities include the purchase and sale of real estate; the management of clients’ money, securities, or other assets; the management of bank, savings, or securities accounts; the organization of contributions for the creation, operation, or management of companies; and the creation, operation, or management of legal persons or arrangements, and buying and selling of business entities. Please also review Module 3a, SAR/STRs, for further information.

Connection with AML regimes

- Generally the same reporting regime should already be in place for anti-money laundering purposes.
- States should ensure that their regimes for fighting money laundering and terrorist financing are consistent.
Enhancing international cooperation

FATF Special Recommendation V states that “each country should afford another country [...] the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organizations.” For more information on Special Recommendation V, see Appendix F.

International cooperation in combating the financing of terrorism is essential for success in the fight against terrorism at the global and national levels. The SFT Convention (articles 10, 11, 12–15, 18.3) has established a comprehensive set of norms for international cooperation, whereas UNSC Resolution 1373 (2001) covers the issue in broad terms (paragraphs 2.c, 2.d and 2.f). Specifically, paragraph 2.f of Resolution 1373 (2001) provides that “states shall [...] afford one another the greatest measure of assistance in connection with criminal investigations or criminal proceedings relating to the financing or support of terrorist acts, including assistance in obtaining evidence in their possession necessary for the proceedings.”

9.1 Mutual legal assistance

The primary purpose of international cooperation is to foster a wide range of mutual legal assistance. This includes measures such as exchange of information and assistance in connection to criminal, civil enforcement, and administrative inquiries.

“Mutual legal assistance” should mean the authority to provide a full range of legal assistance.

Mutual legal assistance includes:

- Taking of evidence
- Production of documents for investigation or as evidence
- Search and seizure of documents or items relevant to criminal proceedings or investigations
- Ability to enforce a foreign restraining, seizure, confiscation, or forfeiture order in a criminal matter

The exchange of information generally occurs through mutual legal assistance mechanisms, which are generally established by treaties on a bilateral or
multilateral basis. But other means of mutual exchanges of information can be organized through:

- FIUs
- Other governmental agencies cooperating under a memorandum of understanding or letter of agreement.

### 9.2 Extradition of offenders and other forms of cooperation

A second purpose of international cooperation is to facilitate the extradition of individuals charged with financing of terrorism, terrorist acts, or terrorist organizations. This means that countries should

- take appropriate measures to ensure that they do not provide safe havens for individuals charged with financing terrorism, terrorist acts, or terrorist organizations; and
- have in place procedures for authorizing the extradition of terrorist financiers.

Political exceptions are not possible in cases involving the extradition of persons charged with financing of terrorism.

### 9.3 Challenges: A good legal framework is meaningless if states are not proactive

The best legislation in the world is of little use without the will to use it. States express their will to fight the financing of terrorism through international cooperation—for example, by communicating to the UN 1267 Committee the names of persons suspected of involvement in terrorist activities and by sharing that information with other interested states.

As another example, in the area of declaration and disclosure systems related to cash couriers (see section 13), states should take the necessary measures to retain, for use by the authorities responsible for mutual cooperation, information on the carrying of currency and bearer negotiable instruments.

UNSC Resolution 1373 imposes upon states a general obligation of due diligence in international cooperation. States must

- deny safe haven to those who finance, plan, support, or commit terrorist acts; and
- prevent those who finance, plan, facilitate, or commit terrorist acts from using their territories for those purposes, regardless of the territory in which the acts occur.

Please review Module 2 and Module 5 for further information.
Knowledge check

**QUESTION 17.** Is there any provision for a political exception with respect to the extradition of persons charged with the financing of terrorism?

- a) Yes
- b) No

**QUESTION 18.** The provision of mutual legal assistance is mandatory.

- a) True
- b) False

**QUESTION 19.** How can the exchange of information among the countries be established?

- a) By law
- b) By memorandum of understanding
- c) By treaty
- d) Any of the above
To fight terrorist financing effectively, mechanisms must be put in place to control the cross-border movements of currencies. A legal requirement to report suspicious transactions is of little use if only some of the intermediaries providing financial services are subject to it. By the same logic, freezing terrorist funds will not be effective if informal intermediaries that transfer funds from one country to another country are beyond the reach of legal controls. Experience shows that money transfer systems have indeed been used to finance terrorists’ operations. For that reason, and because of the need to improve the transparency of these systems, FATF Special Recommendation VI calls upon countries to ensure that all money and value transmission services are subject to all FATF Recommendations that apply to banks and other financial institutions. For more information on FATF Special Recommendation VI, see Appendix G.

Let us analyze the following case.

**Case study  Rurithania and hawalas**

Rurithania is a country with hard-working immigrant communities who remit funds to their home country to support their relatives. Instead of relying on the regulated financial sector, however, most immigrants prefer to use unorthodox money transfer systems that have grown up based on cultural traditions. Informal money transfers are cheaper and offer access to areas not served by formal systems. One informal system, the *hawala* system common in the Middle East and South Asia, makes it possible to transfer money without physical movement of funds. How? The *hawala* operator in the country of the originator of the transfer contacts his or her correspondent in the country of destination and instructs him or her to give cash to the recipient of the transfer. Just like banks, *hawala* operators later settle their mutual claims. Immigrants in Rurithania use money transfer businesses for legitimate and benign purposes. But recently the Rurithanian authorities have begun to fear that terrorist organizations are using these unregulated money remittance systems to finance terrorism. The sobering fact is that these small businesses can be used not only as storefront operations, but also as an entry point into the whole financial sector.

**Covering all money and value transfer services**

Special Recommendation VI aims to ensure that countries impose AML/CFT requirements on *all forms* of money and value transfer systems, formal and informal.
Informal money and value transfer systems are also called alternative remittance services. Formal money and value transfer services are provided by banks and other regulated financial institutions (nonbank financial institutions, or NBFIs). Informal money and value transfer services are a type of financial service in which money or another form of value is moved from one geographic location to another through informal or unsupervised networks or mechanisms. These services increase the risk of abuse by terrorists and those who collect and provide funds to terrorist organizations. Some of the informal systems are legal; others are not. Informal systems include the black market peso exchange, hundi, and hawala systems.

**Knowledge check**

**QUESTION 20.** Which of the following figures is closest to the actual amount of money sent abroad each year by people working outside their home country?

a) About US$500 million  
b) About US$900 million  
c) About US$50 billion  
d) About US$100 billion

**For discussion**

What do you think states should do about money transfer services? What is the situation in your country?

---

**Informal remittances**

Only the FATF Special Recommendations and the SFT Convention address the issue of informal money remitters. FATF Special Recommendation VI provides that states should:

- license or register all money and value transfer services, formal and informal;  
- subject all formal and informal money transfer services to the FATF Recommendations (in particular, Recommendations 4–16 and 21–25) and the FATF Special Recommendations; and  
- ensure that persons or legal entities that provide money transfer services illegally are subject to administrative, civil, or criminal sanctions.

The SFT Convention calls upon the states not only to supervise money transfer services (Article 18.2a), but also to consider measures for monitoring the cross-border transport of funds (Article 18.2b).
For discussion

Is the introductory case on Rurithania and _hawala_ unrealistic? What is the situation in your country?

**Two other possible scenarios:**

The United States and India

*The United States*

The situation in Rurithania is by no means implausible. Indeed, it could describe the current situation in many countries. The United States adopted legislation (The USA PATRIOT Act) to require informal money transfer services to register with the U.S. Treasury Department and, at the state level, to get a license for money transfers. In addition, these businesses must have adequate AML programs in place. This legislation does not resolve all the issues. Supervisory authorities must implement the controls and law enforcement authorities must ensure that informal money transfer businesses comply with the legislation. (31 USC 5330 and 31 CFR 103.41)

*India*

India’s approach is quite different. _Hawala_ transactions are banned under India’s Foreign Exchange Management Act. India has consistently taken the stand that “registration” of _hawala_ dealers is an oxymoron; by their very nature, in the Indian view, _hawala_ transactions, especially those relating to terrorist activities, are clandestine. Because the _hawala_ system is based on trust and, therefore, generates little in the way of records, neither licensing nor registration could ever succeed.

Source: Letter dated May 28, 2004, from the Permanent Representative of India to the Chairman of the UN Counter-Terrorism Committee, attached to UN document S/2004145 1, June 3, 2004
11

Measures required for wire transfers

Consider the following two situations. The answers to the questions will be discussed at the end of this section.

QUESTION 21. A bank receives a wire transfer from a bank located in a foreign country. The transfer does not contain the name or address of the originator of the wire. Is this

a) A minor concern?
b) Something that should alert the bank and trigger an internal check for a possible suspicious transaction?
c) Something that is not important as long as the other elements of the wire conform to proper financial practice?
d) Something that should immediately be reported to the authorities?

QUESTION 22. Bank A receives an international wire transfer through the intermediary services of the correspondent bank of a foreign bank B which does not contain meaningful originator information. Is this

a) A minor concern?
b) Something normal given that it is the role of the correspondent bank to conduct the necessary checking if need be?
c) Something that is irrelevant because the correspondent bank had already checked this information about the wire transfer?
d) Something that should alert the bank and justify an internal checking for a possible suspicious transaction to be reported?

11.1 What is a wire transfer?

According to the Interpretative Note to FATF Special Recommendation VII, the “terms wire transfer and funds transfer refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.”

As a means of moving funds across borders, wire transfers are just the sort of transaction that should be under scrutiny for possible money laundering and terrorist financing. For that reason FATF Special Recommendation VII sets forth a
special standard on wire transfers that is not directly reflected in the text of the SFT Convention and UNSC resolutions. For more information on FATF Special Recommendation VII, see Appendix H.

11.2 What is the FATF’s standard on wire transfers?
FATF Special Recommendation VII obliges states to take specific measures to ensure that financial intermediaries:

- Make sure that accurate and meaningful information on the originator (the name, address, account number) is included in the wire transfer or related message
- Retain the originator’s information with the wire transfer or related message through the chain of payment (correspondent banks are part of that chain)
- Enhance their scrutiny of wire transfers that do not include information on the originator and be alert to the possibility of suspicious transactions.

11.3 Who is covered by the wire transfer standard?
The standard is very clear—and it casts a wide net. All financial institutions, as defined by the FATF Forty Recommendations, should be subjected to these requirements. But Special Recommendation VII is particularly relevant to banks and other remittance service providers.

FATF Special Recommendation VII addresses only the lack of meaningful information on the originator of wire transfers. In broader terms, however, it is important to remember that Special Recommendation IV requires financial institutions to report transactions if they suspect that the funds may be used for terrorism.

---

Information on both the originator and the beneficiary deserves some scrutiny
The following case provides an example of the use of EFT (electronic funds transfer) to transfer funds from Canada to suspected terrorist organizations.

Suspicious use of wire transfers
FINTRAC, the Canadian FIU, received reports from various financial institutions regarding three individuals sending funds to the same person in a foreign country. These individuals had accounts at separate financial institutions and seemed unrelated.

The first individual is a student living in Canada (as reported by one of the financial institutions), who brought in large amounts of U.S. currency, exchanged it for Canadian currency, deposited checks drawn on financial institutions in the United States, requested a draft payable to a currency exchange company, and wired funds to a foreign country of concern. This individual had accounts with three different financial institutions and provided each institution with different addresses, phone numbers, and occupations. One of the addresses belonged to a mailbox service, one of many international mail forwarding centers in Canada. Another address was listed under the name of one of the other two individuals.

—continued
Now let us revisit the two situations presented at the beginning of this section.

**QUESTION 21.** A bank receives a wire transfer from a bank located in a foreign country. The transfer does not contain the name or address of the originator of the wire. Is this

a) A minor concern?
b) Something that should alert the bank and trigger an internal check for a possible suspicious transaction?
c) Something that is not important as long as the other elements of the wire conform to proper financial practice?
d) Something that should immediately be reported to the authorities?

**QUESTION 22.** Bank A receives an international wire transfer through the intermediary services of the correspondent bank of a foreign bank B which does not contain meaningful originator information. Is this

a) A minor concern?
b) Something normal given that it is the role of the correspondent bank to effect the necessary checking if need be?
c) Something that is irrelevant because the correspondent bank had already checked this information about the wire transfer?
d) Something that should alert the bank and justify an internal checking for a possible suspicious transaction to be reported?
12 Dealing with cash couriers

Consider the following case.

### Case study: Cross-border cash movement

The government of Rurithania appears to have been successful in regulating and controlling alternative remittance systems through the registration process. Entities that handle a daily volume of US$15,000 in remittances must now be licensed by the central bank for prudential purposes. But despite the success the government has achieved, the central bank has observed (through its monetary surveillance department) that the amount of remittances moving through registered and licensed entities has declined, while there has been an increase in people crossing the border with hard currency. Customs officials have confirmed this trend and indicated that because there is no limit on how much cash individuals can carry across the border there is little that can be done. The customs officials have asked the central bank to look into the matter.

### 12.1 Why monitor cross-border transportation of cash?

The objective of FATF Special Recommendation IX on cash couriers is to address the risk that terrorist financiers or money launderers may seek to avoid the effect of regulations on alternative remittance systems (Special Recommendation VI) by using cash couriers to move assets across international borders. This Special Recommendation requires the monitoring of cross-border transportation of cash and bearer negotiable instruments and the adoption of an appropriate domestic legal framework for the implementation of this new Recommendation. This is in line with the general recommendation of UNSC Resolution 1526 (2004), which urges “all States [...] to establish internal reporting requirements and procedures on the trans-border movement of currency based on applicable thresholds” (paragraph 5). Similar provision could also be found in article 18.2b of the SFT Convention. For more information on FATF Special Recommendation IX, see Appendix I.

### 12.2 What is targeted?

FATF Special Recommendation IX deals with the act of carrying *cash or its equivalent* across national borders. Under the recommendation, states are
required to monitor the carrying of currency or bearer negotiable instruments, whether by a natural person or by post or freight.

- Currency refers to banknotes and coins in circulation as a medium of exchange.
- Bearer negotiable instruments are monetary instruments in bearer form (checks, money orders, traveler’s checks, and so forth).

FATF Special Recommendation IX targets the cross-border transportation of cash or its equivalent under two sets of circumstances: first, when the currency or negotiable instrument is suspected to be related to terrorist financing or money laundering; and second, when it has been falsely disclosed or declared. The distinction is important. It means that states not only need to have a system for declaring or disclosing cross-border transportation of cash or cash equivalents, but also they need to be able to detect these operations when there is a suspicion of criminal activity.

12.3 What sort of action is required?
States should take several steps to comply with Special Recommendation IX. States should have:

- Measures in place to detect the transportation by couriers of cash or cash equivalents
- The power to stop or restrain the cash or cash equivalent
- Effective, proportionate, and dissuasive sanctions in case of violations of the law, including the possible confiscation of the cash or cash equivalent.

Detection systems may vary among states. They should not excessively inconvenience the public or overburden the customs agencies. The right balance must be found between the use of administrative mechanisms, on one hand, and intelligence information, on the other. There are two systems by which the physical transportation of cash or its equivalent may be detected.

i. Declaration system

Under a declaration system persons carrying across the border currency or bearer negotiable instruments exceeding a certain value (for example, EUR/US$ 15,000) are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the threshold is sufficiently low to meet the objectives of Special Recommendation IX.

ii. Disclosure system

Under a disclosure system persons carrying across the border currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.
12.4 Implementation of sanctions

FATF Special Recommendation IX requires that sanctions be applied in two situations:

- When a person makes a false declaration or disclosure (for example, declaring $500 but carrying $10,000). The sanctions should be effective, proportionate, and dissuasive.
- When the cash or bearer negotiable instruments transported are related to terrorist financing or money laundering. In this case, the cash or bearer negotiable instruments should be confiscated. To do this, states must have the proper confiscation regime in place.

When a customs official stops or restrains cash, this is not a sanction. It is a temporary interference with the rights of the courier or of the owner. However, the interference must not extend beyond a reasonable time—the time needed to collect further information or evidence of criminal activity.

12.5 Challenges to the implementation of FATF Special Recommendation IX

So far, few states have systems in place to comply with FATF Special Recommendation IX. Some may have legislation dealing with the specific case of cash couriers (usually in connection with drug trafficking). Others may hope to use their exchange control legislation to satisfy the requirement of the Recommendation. However, it should be kept in mind that the objective of the recommended monitoring system is both broader and more specific than the goal of exchange controls. It is broader because its aim is to ensure that terrorists and other criminals cannot finance their activities or launder the proceeds of their crime, whatever the crime may be. It is more specific because measures aimed at controlling the cross-border flow of currency, including cash or cash equiv-
lents, for balance-of-payments purposes are often not sufficient and adequate to combat terrorism.

When implementing the Special Recommendation IX, states respect their obligation not to interfere with legitimate trade. Nothing in this Recommendation should be construed to allow states to restrict trade payments between countries for goods and services, or to limit the movement of capital in contravention of their obligations under treaties, conventions, or other agreements.

Knowledge check

**QUESTION 23.** Is the physical transport of gold or precious metal covered by FATF Special Recommendation IX?

a) Yes  

b) No

**QUESTION 24.** If a customs officer discovers that a cash carrier has not disclosed the true amount of currency or bearer negotiable instruments he is carrying, should the officer have the authority to request and obtain further information with regard to the origin of the cash?

a) Yes  

b) No
FATF Special Recommendation VIII addresses the risk of abuse or misuse by terrorist organizations and terrorist financiers of entities legally created under domestic laws. Its aim is thus to prevent juridical persons from being used as a cover for or as a means of financing their activities. For more information on FATF Special Recommendation VIII, see Appendix J.

13.1 What entities should be under scrutiny?

Because it refers to “entities” in general, FATF Special Recommendation VIII is broad in scope. Remember that financing for terrorism may come from legitimate sources. Any juridical person, even businesses that appear perfectly legitimate, might conceivably be used as a screen for collecting funds for terrorists and their organizations. For these reasons, states must be sure that the legal definition of financing terrorism includes funds derived from legitimate sources and take the steps necessary to prevent this type of funding.

**Examples of entities under scrutiny**

Osama bin Laden and his organization, Al-Qaeda, have based their financial empire in part on ordinary business activities. Some of the businesses from which bin Laden and Al-Qaeda derive funds are quite substantial; others are very small. According to a researcher with the International Policy Institute for Counter-Terrorism, “Al-Qaeda has at one time operated ostrich farms and shrimp boats in Kenya, bought tracts of forest in Turkey, engaged in diamond trading in Africa and acquired agricultural holdings in Tajikistan. Many of these minor enterprises—such as the fishing business in Kenya—served as a cover for terrorist operations.” *(Source: Yael Shahar. “Tracing bin Laden’s Money—Easier said than done.” September 21, 2001. http://www.ict.org.il/articles/tabid/66/articlesid/71/)*

“Terrorist groups are increasingly using ‘front companies,’ commercial enterprises that engage in legitimate business, but which are also used to mix illicit revenues with legitimate profits from commercial enterprise. These front businesses are involved in everything from convenience stores to international investment management services.”

FATF Special Recommendation VIII also stresses the vulnerabilities of nonprofit organizations, warning that charities, religious, educational, social, and fraternal organizations can be misused by terrorists. According to the standard, countries should ensure that nonprofits cannot be misused

- by terrorist organizations posing as legitimate entities;
- to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or
- to conceal or obscure the clandestine diversion to terrorist organizations of funds intended for legitimate purposes.

**Nonprofit organizations**

“One nonprofit organization solicited donations from local charities in a donor region, in addition to fund raising efforts conducted at its headquarters in a beneficiary region. This nonprofit organization falsely asserted that the funds collected were destined for orphans and widows. In fact, the finance chief of this organization served as the head of organized fundraising for Osama bin Laden. Rather than providing support for orphans and widows, funds collected by the nonprofit organization were turned over to al-Qaeda operatives.” For another example, see Module 1: Where do money laundering and terrorist financing operations take place?


FATF Special Recommendation VIII is necessarily rather general because the different entities categorized as nonprofit organizations take many different legal forms—among them associations, foundations, fundraising committees, community service organizations, corporations in the public interest, and limited companies—and because the nature of their operations varies from one jurisdiction to the next. Thus, the standard suggests a form of self-assessment by each country. States are asked to review their national legislation for risks and weaknesses.

### 13.2 What kind of oversight is needed? By whom?

*States are not required to adopt any specific solution.* FATF Special Recommendation VIII does not impose a particular model.

- Steps should be taken to ensure the transparency and accountability of nonprofit organizations and action taken to address serious risks and vulnerabilities.
- These actions should be guided by the principle that the oversight should be flexible, effective and proportional to the risk of abuse. Note that FATF’s “International Best Practices” are a good source of direction and practical advice.
Who ensures the oversight? Solutions vary among countries. For instance, the United Kingdom set up a Charity Commission and has in place a system of registration. Tax authorities might play a role in certain jurisdictions. But traditionally, the objective of tax authorities, in respect of charities, is to verify that the benefits of tax relief are passed on to recipients (through projects and grants). Implementation of the FATF standard, therefore, entails consequently that the agencies responsible for such oversight functions broaden their focus.

Knowledge check

Please answer the following questions.

QUESTION 25. Can the fight against terrorist financing justify restrictions on charitable activities?


QUESTION 26. Should states be more flexible regarding the activities of religious nonprofit organizations?


QUESTION 27. When nonprofit organizations disburse funds to foreign organizations should this cause special concern?


For discussion

Based on your personal experience and your knowledge of circumstances in your country, do you believe that the measures outlined in international standards on preventing the financing of terrorism are likely to be effective? Can
measures such as the freezing and confiscation of assets prevent terrorist acts and curtail the activities of terrorist organizations?

Should states try to supervise informal money transfer services? Is it possible to control informal business? What about the risk that remitters will seek and find unregulated ways to provide this type of underground business?

**Check your understanding**

**QUESTION 28.** Although the SFT Convention does not offer a definition of ________________________, it does define ________________________. That definition emphasizes two aspects of the financing of terrorism: providing funds and ________________________ funds with the intention that they should be used, or with the knowledge that they will be used, to carry out terrorist acts.

**QUESTION 29.** Various international instruments deal with the issue of the financing of terrorism. From the list that follows, select the assertions that are true.

a) The SFT Convention is the most comprehensive international instrument on the financing of terrorism.
b) The SFT Convention is the only instrument that covers the freezing of funds.
c) UNSC Resolution 1373 (2001) sets up a general framework of anti-terrorism measures and is mandatory for all states.
d) The FATF Special Recommendations cover specific issues of the financing of terrorism that are not always addressed by other instruments.

**QUESTION 30.** International standards and obligations concerning the financing of terrorism fall principally on ________________________. However, some rules also target specific ________________________ and terrorist ________________________. The UN 1267 Committee has established a system of periodically reviewing ________________________ of suspected terrorists and terrorist organizations.

**QUESTION 31.** Is ratification of the SFT Convention the only measure states should take to comply with international rules on terrorist financing?
QUESTION 32. According to the SFT Convention and UNSC Resolution 1373, must states criminalize the financing of terrorism when the offense is committed abroad by one of their nationals?

QUESTION 33. Which of the following statements is true?

a) States have a duty to freeze or seize the assets of terrorists. Actual confiscation is optional and may be done at the discretion of states.

b) States are obliged to establish a legal framework for the freezing, seizure, and confiscation of assets of terrorists. They may choose the means of implementing those measures in their national legal system.

c) States have no obligation to freeze the assets of terrorists and terrorist organizations listed by the UN 1267 Committee provided they maintain their own list of terrorists and terrorist organizations.

QUESTION 34. States should make sure that their legislation obligates their financial institutions and, for certain types of activities, other professionals (such as dealers in precious _______ and _______ lawyers, notaries, and so on) to report suspicious transactions. This duty applies not only to the CFT regime, but also to the state’s _______ regime. Under the CFT regime, institutions must report to the authorities when they suspect that funds are linked to the financing of terrorism or when there is _______ to suspect that funds are so linked (for example, when a party to a suspicious transaction is listed as terrorist).

QUESTION 35. States’ obligation to cooperate at the international level extends only to the criminal dimension of the fight against terrorist financing.

a) True   b) False

QUESTION 36. Which assertion is most accurate?

a) The FATF Special Recommendations address the issue of the weakness of formal financial systems to specifically cover the problem of wire transfers and impose duties on financial intermediaries, such as requiring meaningful information on the originator of a wire.

b) The FATF Special Recommendations address the issue of the weakness of formal and informal financial systems by imposing specific duties on financial intermediaries with respect to wire transfers and remittance systems.
QUESTION 37. With respect to charities and nonprofit organizations, there is no specific model that states must adopt. Special Recommendation VIII essentially requires that states ensure the transparency and accountability of nonprofit organizations and take corrective action where serious vulnerabilities exist.

a) True  b) False

Summary

In this module, we discussed the following:

- The rationale for combating the financing of terrorism
- The UN instruments that must be ratified and implemented
- The kind of offenses that should be criminalized
- The measures required to freeze, seize, and confiscate terrorist assets
- How to report suspicious transactions related to terrorism
- How to enhance international cooperation
- The nature of alternative remittance systems and the measures required to monitor them
- The measures applicable to wire transfers and cash couriers
- The supervision of nonprofit organizations
Appendix A: References

**FATF Recommendations**
- The Forty Recommendations (FATF, June 2003)  
  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- Special Recommendations on Terrorist Financing (FATF, October 2004)  

**Useful Web sites**
- Fight against Terrorism, Council of Europe  
  http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against_terrorism/default.asp
- Terrorism, United Nations Office on Drugs and Crime  
  http://www.unodc.org/unodc/terrorism.html
- UN action against terrorism, United Nations [conventions, declarations, news, and developments]  
  http://www.un.org/terrorism/

**Reference Documents**
- Combating the Abuse of Nonprofit Organizations: International Best Practices (FATF, October 2002)  
- Guidance Notes for the Special Recommendations on Terrorist Financing and the Self-Assessment Questionnaire (FATF, March 2002)  
- Guidance for Financial Institutions in Detecting Terrorist Financing (FATF, April 2002)  
• United Nations Security Council Resolution 1267 (UN, October 1999)
• United Nations Security Council Resolution 1269 (UN, October 1999)
• United Nations Security Council Resolution 1373 (UN, September 2001)
  http://www.un.org/Docs/sc/unsc_resolutions03.html
  http://www.un.org/Docs/sc/unsc_resolutions03.html
• Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols (UNODC, 2003)
I. Ratification and implementation of UN instruments

Each country should take immediate steps to ratify and to implement fully the 1999 UN International Convention for the Suppression of the Financing of Terrorism.

Countries should also immediately implement the UN resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly UN Security Council resolution 1373.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)

SR I: Ratification and implementation of UN instruments

This Recommendation contains six elements:


For the purposes of this Special Recommendation, ratification means having carried out any necessary national legislative or executive procedures to approve the UN Convention and having delivered appropriate ratification instruments to the UN. Implementation as used here means having put measures in place to bring the requirements indicated in the UN Convention and UNSC Resolutions into effect. The measures may be established by law, regulation, directive, decree, or any other appropriate legislative or executive act according to national law.

The UN Convention was open for signature from January 10, 2000 to December 31, 2001, and upon signature is subject to ratification, acceptance, or approval. Ratification, acceptance, or approval instruments must be deposited with the Secretary-General of the UN in New York. Those countries that have not signed the Convention may accede to it (see Article 25 of the Convention). The full text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism.asp. As of March 19, 2002, 132 countries have signed, and 24 have deposited ratification instruments. On March 10, 2002, the UN Convention
II. Criminalising the financing of terrorism and associated money laundering

Each country should criminalize the financing of terrorism, terrorist acts, and terrorist organisations. Countries should ensure that such offenses are designated as money laundering predicate offenses.

INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION II:
CRIMINALISING THE FINANCING OF TERRORISM AND ASSOCIATED MONEY LAUNDERING

Objective

1) Special Recommendation II (SR II) was developed with the objective of ensuring that countries have the legal capacity to prosecute and apply criminal sanctions to persons that finance terrorism. Given the close connection between international terrorism and \textit{inter alia} money laundering, another objective of SR II is to emphasize this link by obligating countries to include terrorist financing offences as predicate offences for money laundering. The basis for criminalising terrorist financing should be the UN International Convention for the Suppression of the Financing of Terrorism, 1999.3

Definitions

2) For the purposes of SR II and this Interpretative Note, the following definitions apply:

a) The term \textit{funds} refers to assets of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such assets, including, but not limited to, bank credits, traveler’s checks, bank check, money orders, shares, securities, bonds, drafts, letters of credit.

b) The term \textit{terrorist} refers to any natural person who (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts;

---

3 Although the UN Convention had not yet come into force at the time that SR II was originally issued in October 2001, and thus is not cited in the SR itself, the intent of the FATF has been from the issuance of SR II to reiterate and reinforce the criminalization standard as set forth in the Convention (in particular, Article 2). The convention came into force in April 2003.
(iii) organises or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.


d) The term terrorist financing includes the financing of terrorist acts, and of terrorists and terrorist organisations.

e) The term terrorist organisation refers to any group of terrorists that (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.

Characteristics of the Terrorist Financing Offense

3) Terrorist financing offences should extend to any person who willfully provides or collects 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: (a) to carry out a terrorist act(s); (b) by a terrorist organisation; or (c) by an individual terrorist.
4) Criminalising terrorist financing solely on the basis of aiding and abetting, attempt, or conspiracy does not comply with this Recommendation.

5) Terrorist financing offences should extend to any funds whether from a legitimate or illegitimate source.

6) Terrorist financing offences should not require that the funds: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

7) It should also be an offence to attempt to commit the offense of terrorist financing.

8) It should also be an offence to engage in any of the following types of conduct:

   a) Participating as an accomplice in an offence as set forth in paragraphs 3 or 7 of this Interpretative Note
   b) Organizing or directing others to commit an offence as set forth in paragraphs 3 or 7 of this Interpretative Note
   c) Contributing to the commission of one or more offence(s) as set forth in paragraphs 3 or 7 of this Interpretative Note by a group of persons acting with a common purpose. Such contribution shall be intentional and shall either: (i) be made with the aim of furthering the criminal activity or criminal purpose of the group, where such activity or purpose involves the commission of a terrorist financing offense; or (ii) be made in the knowledge of the intention of the group to commit a terrorist financing offense

9) Terrorist financing offences should be predicate offences for money laundering.

10) Terrorist financing offenses should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organisation(s) is located or the terrorist act(s) occurred/will occur.

11) The law should permit the intentional element of the terrorist financing offense to be inferred from objective factual circumstances.

12) Criminal liability for terrorist financing should extend to legal persons. Where that is not possible (for example, due to fundamental principles of domestic law), civil or administrative liability should apply.

13) Making legal persons subject to criminal liability for terrorist financing should not preclude the possibility of parallel criminal, civil, or administrative proceedings in countries in which more than one form of liability is available.

14) Natural and legal persons should be subject to effective, proportionate and dissuasive criminal, civil, or administrative sanctions for terrorist financing.
GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)†

SR II: Criminalising the financing of terrorism and associated money laundering

This Recommendation contains two elements:

- Jurisdictions should criminalize “the financing of terrorism, of terrorist acts and of terrorist organizations.”
- Jurisdictions should establish terrorist financing offenses as predicate offenses for money laundering.

In implementing SR II, jurisdictions must either establish specific criminal offenses for terrorist financing activities, or they must be able to cite existing criminal offenses that may be directly applied to such cases. The terms financing of terrorism or financing of terrorist acts refer to the activities described in the UN Convention (Article 2) and S/RES/1373(2001), paragraph 1b (see the UN Web site at http://www.un.org/documents/scres.htm for text of this Resolution).

It should be noted that each jurisdiction should also ensure that terrorist financing offences apply as predicate offences even when carried out in another state. This corollary interpretation of SR II is then consistent with FATF Recommendation 4.

FATF Recommendation 4 already calls for jurisdictions to designate “serious offences” as predicates for the offence of money laundering. SR II builds on Recommendation 4 by requiring that, given the gravity of terrorist financing offences, terrorism financing offences should be specifically included among the predicates for money laundering. For the full text of the FATF Forty Recommendations, along with their Interpretative Notes, see the FATF Web site at http://www.fatfgaafi.org/40Recs_en.htm.

Finally, as in general with other predicates for money laundering, jurisdictions should ensure that terrorist financing offences are predicate offences even if they are committed in a jurisdiction different from the one in which the money laundering offence is being applied.

†Please note that the reference to Recommendation 4 in the guidance note refers to the 1996 version of the FATF 40 Recommendations.
III. Freezing and confiscating terrorist assets

Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with the UN resolutions relating to the prevention and suppression of the financing of terrorist acts.

Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organizations.

**INTERPRETATIVE NOTE TO SPECIAL RECOMMENDATION III:**

**FREEZING AND CONFISCATING TERRORIST ASSETS**

**Objectives**

1) FATF Special Recommendation III consists of two obligations. The first requires jurisdictions to implement measures that will freeze or, if appropriate, seize terrorist-related funds or other assets without delay in accordance with relevant UN resolutions. The second obligation of Special Recommendation III is to have measures in place that permit a jurisdiction to seize or confiscate terrorist funds or other assets on the basis of an order or mechanism issued by a competent authority or a court.

2) The objective of the first requirement is to freeze terrorist-related funds or other assets based on reasonable grounds, or a reasonable basis, to suspect or believe that such funds or other assets could be used to finance terrorist activity. The objective of the second requirement is to deprive terrorists of these funds or other assets if and when links have been adequately established between the funds or other assets and terrorists or terrorist activity. The intent of the first objective is preventative; the intent of the second objective is mainly preventative and punitive. Both requirements are necessary to deprive terrorists and terrorist networks of the means to conduct future terrorist activity and maintain their infrastructure and operations.

**Scope**

3) Special Recommendation III is intended, with regard to its first requirement, to complement the obligations in the context of the UNSC resolutions relating to the prevention and suppression of the financing of terrorist
acts—S/RES/1267(1999) and its successor resolutions, S/RES/1373(2001) and any prospective resolutions related to the freezing, or if appropriate seizure, of terrorist assets. It should be stressed that none of the obligations in SR III is intended to replace other measures or obligations that may already be in place for dealing with funds or other assets in the context of a criminal, civil or administrative investigation or proceeding.\(^4\) The focus of SR III instead is on the preventative measures that are necessary and unique in the context of stopping the flow or use of funds or other assets to terrorist groups.

4) S/RES/1267(1999) and S/RES/1373(2001) differ in the persons and entities whose funds or other assets are to be frozen, the authorities responsible for making these designations, and the effect of these designations.

5) S/RES/1267(1999) and its successor resolutions obligate jurisdictions to freeze without delay the funds or other assets owned or controlled by Al-Qaeda, the Taliban, Osama bin Laden, or persons and entities associated with them as designated by the United Nations Al-Qaeda and Taliban Sanctions Committee established pursuant to UN Security Council resolution 1267 (the Al-Qaeda and Taliban Sanctions Committee), including funds derived from funds or other assets owned or controlled, directly or indirectly, by them or by persons acting on their behalf or at their direction, and ensure that neither these nor any other funds or other assets are made available, directly or indirectly, for such persons’ benefit, by their nationals or by any person within their territory. The Al-Qaeda and Taliban Sanctions Committee is the authority responsible for designating the persons and entities that should have their funds or other assets frozen under S/RES/1267(1999). All jurisdictions that are members of the United Nations are obligated by S/RES/1267(1999) to freeze the assets of persons and entities so designated by the Al-Qaeda and Taliban Sanctions Committee.\(^5\)

6) S/RES/1373(2001) obligates jurisdictions\(^6\) to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual jurisdiction has the authority to designate the persons and entities that should have their funds or other

\(^4\) For instance, both the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) and UN Convention against Transnational Organised Crime (2000) contain obligations regarding freezing, seizure, and confiscation in the context of combating transnational crime. Those obligations exist separately and apart from obligations that are set forth in S/RES/1267(1999), S/RES/1373(2001) and SR III.

\(^5\) When the UNSC acts under Chapter VII of the UN Charter, the resolutions it issues are mandatory for all UN members.

\(^6\) The UNSC was acting under Chapter VII of the UN Charter in issuing S/RES/1373(2001) (see previous footnote).
assets frozen. Additionally, to ensure that effective cooperation is developed among jurisdictions, jurisdictions should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other jurisdictions. When (i) a specific notification or communication is sent and (ii) the jurisdiction receiving the request is satisfied, according to applicable legal principles, that a requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, the jurisdiction receiving the request must ensure that the funds or other assets of the designated person are frozen without delay.

Definitions

7) For the purposes of SR III and this Interpretive Note, the following definitions apply:

a) The term freeze means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of, and for the duration of the validity of, an action initiated by a competent authority or a court under a freezing mechanism. The frozen funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the freezing and may continue to be administered by the financial institution or other arrangements designated by such person(s) or entity(ies) prior to the initiation of an action under a freezing mechanism.

b) The term seize means to prohibit the transfer, conversion, disposition, or movement of funds or other assets on the basis of an action initiated by a competent authority or a court under a freezing mechanism. However, unlike a freezing action, a seizure is affected by a mechanism that allows the competent authority or court to take control of specified funds or other assets. The seized funds or other assets remain the property of the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the seizure, although the competent authority or court will often take over possession, administration or management of the seized funds or other assets.

c) The term confiscate, which includes forfeiture where applicable, means the permanent deprivation of funds or other assets by order of a competent authority or a court. Confiscation or forfeiture takes place through a judicial or administrative procedure that transfers the ownership of specified funds or other assets to be transferred to the state. In this case, the person(s) or entity(ies) that held an interest in the specified funds or other assets at the time of the confiscation or forfeiture loses all rights, in principle, to the confiscated or forfeited funds or other assets.7

7 Confiscation or forfeiture orders are usually linked to a criminal conviction or a court decision whereby the confiscated or forfeited property is determined to have been derived from or intended for use in a violation of the law.
d) The term *funds or other assets* means financial assets, property of every kind, whether tangible or intangible, movable or immovable, however acquired, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or interest in, such funds or other assets, including, but not limited to, bank credits, traveler’s checks, bank checks, money orders, shares, securities, bonds, drafts, or letters of credit, and any interest, dividends, or other income on or value accruing from or generated by such funds or other assets.

e) The term *terrorist* refers to any natural person who (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts or terrorist financing; (iii) organizes or directs others to commit terrorist acts or terrorist financing; or (iv) contributes to the commission of terrorist acts or terrorist financing by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or terrorist financing or with the knowledge of the intention of the group to commit a terrorist act or terrorist financing.

f) The phrase *those who finance terrorism* refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commission of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the 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.

g) The term *terrorist organization* refers to any legal person, group, undertaking, or other entity owned or controlled directly or indirectly by a terrorist(s).

h) The term *designated persons* refers to those persons or entities designated by the Al-Qaeda and Taliban Sanctions Committee pursuant to S/RES/1267(1999) or those persons or entities designated and accepted, as appropriate, by jurisdictions pursuant to S/RES/1373(2001).

i) The phrase *without delay*, for the purposes of S/RES/1267(1999), means, ideally, within a matter of hours of a designation by the Al-Qaeda and

---

The phrase \textit{without delay} means upon having reasonable grounds, or a reasonable basis, to suspect or believe that a person or entity is a terrorist, one who finances terrorism or a terrorist organization. The phrase \textit{without delay} should be interpreted in the context of the need to prevent the flight or dissipation of terrorist-linked funds or other assets, and the need for global, concerted action to interdict and disrupt their flow swiftly.

\textbf{Freezing without delay terrorist-related funds or other assets}

8) To fulfill the preventive intent of SR III, jurisdictions should establish the necessary authority and adopt the following standards and procedures to freeze the funds or other assets of terrorists, those who finance terrorism and terrorist organizations in accordance with both S/RES/1267(1999) and S/RES/1373(2001):

\begin{itemize}
\item \textbf{a) Authority to freeze, unfreeze, and prohibit dealing in funds or other assets of designated persons.} Jurisdictions should prohibit by enforceable means the transfer, conversion, disposition, or movement of funds or other assets. Options for providing the authority to freeze and unfreeze terrorist funds or other assets include the following:
\begin{itemize}
\item (i) Empowering or designating a competent authority or a court to issue, administer, and enforce freezing and unfreezing actions under relevant mechanisms
\item (ii) Enacting legislation that places responsibility for freezing the funds or other assets of designated persons publicly identified by a competent authority or a court on the person or entity holding the funds or other assets and subjecting them to sanctions for noncompliance.
\end{itemize}

The authority to freeze and unfreeze funds or other assets should also extend to funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by such terrorists, those who finance terrorism, or terrorist organizations.

Whatever option is chosen there should be clearly identifiable competent authorities responsible for enforcing the measures.

The competent authorities shall ensure that their nationals or any persons and entities within their territories are prohibited from making any funds or other assets, economic resources or financial or other related services available, directly or indirectly, wholly or jointly, for the benefit of: designated persons, terrorists; those who finance terrorism; terrorist organizations; entities owned or controlled, directly or indirectly, by such persons or entities; and persons and entities acting on behalf of or at the direction of such persons or entities.

\item \textbf{b) Freezing procedures.} Jurisdictions should develop and implement procedures to freeze the funds or other assets specified in paragraph (c) below
without delay and without giving prior notice to the persons or entities concerned. Persons or entities holding such funds or other assets should be required by law to freeze them and should furthermore be subject to sanctions for noncompliance with this requirement. Any delay between the official receipt of information provided in support of a designation and the actual freezing of the funds or other assets of designated persons undermines the effectiveness of designation by affording designated persons time to remove funds or other assets from identifiable accounts and places. Consequently, these procedures must ensure (i) the prompt determination whether reasonable grounds or a reasonable basis exists to initiate an action under a freezing mechanism and (ii) the subsequent freezing of funds or other assets without delay upon determination that such grounds or basis for freezing exist. Jurisdictions should develop efficient and effective systems for communicating actions taken under their freezing mechanisms to the financial sector immediately upon taking such action. As well, they should provide clear guidance, particularly financial institutions and other persons or entities that may be holding targeted funds or other assets on obligations in taking action under freezing mechanisms.

c) **Funds or other assets to be frozen or, if appropriate, seized.** Under Special Recommendation III, funds or other assets to be frozen include those subject to freezing under S/RES/1267(1999) and S/RES/1373(2001). Such funds or other assets would also include those wholly or jointly owned or controlled, directly or indirectly, by designated persons. In accordance with their obligations under the UN International Convention for the Suppression of the Financing of Terrorism (1999) (the Terrorist Financing Convention (1999)), jurisdictions should be able to freeze or, if appropriate, seize any funds or other assets that they identify, detect, and verify, in accordance with applicable legal principles, as being used by, allocated for, or being made available to terrorists, those who finance terrorists or terrorist organizations. Freezing or seizing under the Terrorist Financing Convention (1999) may be conducted by freezing or seizing in the context of a criminal investigation or proceeding. Freezing action taken under Special Recommendation III shall be without prejudice to the rights of third parties acting in good faith.

d) **De-listing and unfreezing procedures.** Jurisdictions should develop and implement publicly known procedures to consider delisting requests upon satisfaction of certain criteria consistent with international obligations and applicable legal principles, and to unfreeze the funds or other assets of de-listed persons or entities in a timely manner. For persons and entities designated under S/RES/1267(1999), such procedures and criteria should be in accordance with procedures adopted by the Al-Qaeda and Taliban Sanctions Committee under S/RES/1267(1999).
e) *Unfreezing upon verification of identity.* For persons or entities with the same or similar name as designated persons, who are inadvertently affected by a freezing mechanism, jurisdictions should develop and implement publicly known procedures to unfreeze the funds or other assets of such persons or entities in a timely manner upon verification that the person or entity involved is not a designated person.

f) *Providing access to frozen funds or other assets in certain circumstances.* Where jurisdictions have determined that funds or other assets, which are otherwise subject to freezing pursuant to the obligations under S/RES/1267(1999), are necessary for basic expenses; for the payment of certain types of fees, expenses, and service charges, or for extraordinary expenses, jurisdictions should authorize access to such funds or other assets in accordance with the procedures set out in S/RES/1452(2002) and subject to approval of the Al-Qaeda and Taliban Sanctions Committee. On the same grounds, jurisdictions may authorize access to funds or other assets, if freezing measures are applied pursuant to S/RES/1373(2001).

g) *Remedies.* Jurisdictions should provide for a mechanism through which a person or an entity that is the target of a freezing mechanism in the context of terrorist financing can challenge that measure with a view to having it reviewed by a competent authority or a court.

h) *Sanctions.* Jurisdictions should adopt appropriate measures to monitor effectively the compliance with relevant legislation, rules or regulations governing freezing mechanisms by financial institutions and other persons or entities that may be holding funds or other assets as indicated in paragraph 8(c) above. Failure to comply with such legislation, rules or regulations should be subject to civil, administrative, or criminal sanctions.

**Seizure and Confiscation**

9) Consistent with FATF Recommendation 3, jurisdictions should adopt measures similar to those set forth in Article V of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), Articles 12 to 14 of the UN Convention on Transnational Organized Crime (2000), and Article 8 of the Terrorist Financing Convention (1999), including legislative measures, to enable their courts or competent authorities to seize and confiscate terrorist funds or other assets.

**GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) [EXTRACT]**

This recommendation contains three major elements:

- Jurisdictions should have the authority to freeze funds or assets of (a) terrorists and terrorist organizations and (b) those who finance terrorist acts or terrorist organizations.

---

9 See Article 1, S/RES/1452(2002) for the specific types of expenses that are covered.
• They should have the authority to **seize** (a) the proceeds of terrorism or of terrorist acts, (b) the property used in terrorism, in terrorist acts or by terrorist organizations, and (c) property intended or allocated for use in terrorism, in terrorist acts, or by terrorist organizations.

• They should have the authority to **confiscate** (a) the proceeds of terrorism or of terrorist acts; (b) the property used in terrorism, in terrorist acts, or by terrorist organizations; and (c) property intended or allocated for use in terrorism, in terrorist acts or by terrorist organizations.

The term **measures**, as used in SR III, refers to explicit (legislative or regulatory) provisions or “executive powers” that permit the three types of action. As with the preceding recommendation, it is not necessary that the texts authorizing these powers mention terrorist financing in particular. However, jurisdictions with already existing laws must be able to cite specific provisions that permit them to freeze, to seize, or to confiscate terrorist-related funds and assets within the national legal/judicial context.

The definitions of the concepts of freezing, seizure, and confiscation vary from one jurisdiction to another. For the purposes of general guidance, the following descriptions of these terms are provided:

**Freezing:** In the context of this recommendation, a competent government or judicial authority must be able to freeze, to block, or to restrain specific funds or assets and thus prevent them from being moved or disposed of. The assets/funds remain the property of the original owner and may continue to be administered by the financial institution or other management arrangement designated by the owner.

**Seizure:** As with freezing, competent government or judicial authorities must be able to take action or to issue an order that allows them to take control of specified funds or assets. The assets/funds remain the property of the original owner, although the competent authority will often take over possession, administration, or management of the assets/funds.

**Confiscation (or forfeiture):** Confiscation or forfeiture takes place when competent government or judicial authorities order that the ownership of specified funds or assets be transferred to the state. In this case, the original owner loses all rights to the property. Confiscation or forfeiture orders are usually linked to a criminal conviction and a court decision whereby the property is determined to have been derived from or intended for use in a violation of the law.

With regard to freezing in the context of SR III, the terms **terrorists**, **those who finance terrorism**, and **terrorist organizations** refer to individuals and entities identified pursuant to S/RES/1267(1999) and S/RES/1390(2002), as well as to any other individuals and entities designated as such by individual national governments.
IV. Reporting suspicious transaction related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, 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, they should be required to report promptly their suspicions to the competent authorities.

GUIDANCE NOTES FOR THE SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING (MARCH 27, 2002) (EXTRACT)†

This recommendation contains two major elements:

- Jurisdictions should establish a requirement for making a report to competent authorities when there is a suspicion that funds are linked to terrorist financing.
- Jurisdictions should establish a requirement for making a report to competent authorities when there are reasonable grounds to suspect that funds are linked to terrorist financing.

For SR IV, the term financial institutions refers to both banks and NBFIs. In the context of assessing implementation of FATF Recommendations, NBFIs include, at a minimum, the following types of financial services: bureaus de change, stockbrokers, insurance companies, and money remittance/transfer services. This definition of financial institutions is also understood to apply to SR IV to be consistent with the interpretation of the FATF Forty Recommendations. With regard specifically to SR IV, if other types of professions, businesses, or business activities currently fall under anti-money laundering reporting obligations, jurisdictions should also extend terrorist financing reporting requirements to those entities or activities.

The term competent authority, for the purposes of SR IV, is understood to be either the jurisdiction’s FIU or another central authority that has been designated by the jurisdiction for receiving disclosures related to money laundering. With regard to the terms suspect and have reasonable grounds to suspect, the

†Please note that the reference to Recommendation 15 in the guidance note below refers to the 1996 version of the FATF 40 Recommendations.
distinction is being made among levels of mental certainty that could form the basis for reporting a transaction. The first term—that is, a requirement to report to competent authorities when a financial institution suspects that funds are derived from or intended for use in terrorist activity—is a subjective standard and transposes the reporting obligation called for in FATF Recommendation 15 to SR IV. The requirement to report transactions when there are reasonable grounds to suspect that the funds are derived from or intended for use in terrorist activity is an objective standard, which is consistent with the intent of Recommendation 15 although somewhat broader. In the context of SR IV, jurisdictions should establish a reporting obligation that may be based either on suspicion or on having reasonable grounds to suspect.
V. International cooperation

Each country should afford another country, on the basis of a treaty, arrangement, or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts, and terrorist organizations. Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts, or terrorist organizations, and should have procedures in place to extradite, where possible, such individuals.

Guidance Notes for the Special Recommendations on Terrorist Financing
(March 27, 2002) (Extract)

This recommendation contains five elements:

- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions through *mutual legal assistance mechanisms*.
- Jurisdictions should permit the exchange of information regarding terrorist financing with other jurisdictions by means *other than through mutual legal assistance mechanisms*.
- Jurisdictions should have specific measures to permit the denial of “safe haven” to individuals involved in terrorist financing.
- Jurisdictions should have procedures that permit the extradition of individuals involved in terrorist financing.
- Jurisdictions should have provisions or procedures to ensure that “claims of political motivation are not recognized as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing.”

To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made for some questions in the SAQTF [Self Assessment Questionnaire on Terrorist Financing] between international cooperation through *mutual legal assistance* mechanisms on the one hand and information exchange through means *other than through mutual legal assistance*. 

---

Appendix F: FATF Special Recommendation V
For the purposes of SR V, the term *mutual legal assistance* means the power to provide a full range of both noncoercive legal assistance, including the taking of evidence, the production of documents for investigation or as evidence, the search and seizure of documents or things relevant to criminal proceedings or to a criminal investigation, the ability to enforce a foreign restraint, seizure, forfeiture, or confiscation order in a criminal matter. In this instance, *mutual legal assistance* would also include information exchange through rogatory commissions (that is, from the judicial authorities in one jurisdiction to those in another).

Exchange of information by means *other than through mutual legal assistance* includes any arrangement other than those described in the preceding paragraph. Under this category should be included exchanges that take place between FIUs or other agencies that communicate bilaterally on the basis of memoranda of understanding (MOU), exchanges of letters, and so on.

With regard to the last three elements of SR V, these concepts should be understood as referred to in the relevant UN documents. These are S/RES/1373 (2001), paragraph 2c (for denial of safe haven); the UN Convention, Article 11 (for extradition); and the UN Convention, Article 14 (for rejection of claims of political motivation as related to extradition). The text of the UN Convention may be consulted at http://untreaty.un.org/English/Terrorism.asp; the text of S/RES/1373 (2001) may be accessed at http://www.un.org/documents/scres.htm.

The term *civil enforcement* as used in SR V is intended to refer only to the type of investigations, inquiries, or procedures conducted by regulatory or administrative authorities that have been empowered in certain jurisdictions to carry out such activities in relation to terrorist financing. *Civil enforcement* is not meant to include civil procedures and related actions as understood in civil law jurisdictions.
VI. Alternative remittance

Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and NBFIs. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil, or criminal sanctions.

Interpretative Note to Special Recommendation VI: Alternative Remittance

General

1) Money or value transfer systems have shown themselves vulnerable to misuse for money laundering and terrorist financing purposes. The objective of Special Recommendation VI is to increase the transparency of payment flows by ensuring that jurisdictions impose consistent anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems, particularly those traditionally operating outside the conventional financial sector and not currently subject to the FATF Recommendations. This Recommendation and Interpretative Note underscore the need to bring all money or value transfer services, whether formal or informal, within the ambit of certain minimum legal and regulatory requirements in accordance with the relevant FATF Recommendations.

2) Special Recommendation VI consists of three core elements:

a) Jurisdictions should require licensing or registration of persons (natural or legal) that provide money/value transfer services, including through informal systems.

b) Jurisdictions should ensure that money/value transmission services, including informal systems (as described in paragraph 5 below), are subject to applicable FATF Forty Recommendations (2003) (in particular, Recommendations 4–6 and 21–25) and the Eight Special Recommendations \(^{10}\) (in particular SR VII).

\(^{10}\) After the ninth special recommendation was added in 2004, it is now FATF Nine Special Recommendations.
c) Jurisdictions should be able to impose sanctions on money/value transfer services, including informal systems, that operate without a license or registration and that fail to comply with relevant FATF Recommendations.

Scope and Application

3) For the purposes of this recommendation, the following definitions are used.
4) *Money or value transfer service* refers to a financial service that accepts cash, checks, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, or transfer or through a clearing network to which the money/value transfer service belongs. Transactions performed by such services can involve one or more intermediaries and a third-party final payment.
5) A money or value transfer service may be provided by persons (natural or legal) formally through the regulated financial system or informally through NBFIs or other business entities or any other mechanism either through the regulated financial system (for example, use of bank accounts) or through a network or mechanism that operates outside the regulated system. In some jurisdictions, informal systems are frequently referred to as *alternative remittance services* or *underground (or parallel) banking systems*. Often these systems have ties to particular geographic regions and are therefore described using a variety of specific terms. Some examples of these terms include *hawala*, *hundi*, *fei-chien*, and the *black market peso exchange*.11
6) *Licensing* means a requirement to obtain permission from a designated competent authority to operate a money/value transfer service legally.
7) *Registration* in this recommendation means a requirement to register with or declare to a designated competent authority the existence of a money/value transfer service in order for the business to operate legally.
8) The obligation of licensing or registration applies to agents. At a minimum, the principal business must maintain a current list of agents, which must be made available to the designated competent authority. An *agent* is any person who provides money or value transfer service under the direction of or by contract with a legally registered or licensed remitter (for example, licensees, franchisees, concessionaires).

Applicability of Special Recommendation VI

9) Special Recommendation VI should apply to all persons (natural or legal), which conduct for or on behalf of another person (natural or legal) the types of activity described in paragraphs 4 and 5 above as a primary or substantial part of their business or when such activity is undertaken on a regular or recurring basis, including as an ancillary part of a separate business enterprise.

---

11 The inclusion of these examples does not suggest that such systems are legal in any particular jurisdiction.
10) Jurisdictions need not impose a separate licensing/registration system or designate another competent authority in respect to persons (natural or legal) already licensed or registered as financial institutions (as defined by the FATF Forty Recommendations) within a particular jurisdiction, which under such license or registration are permitted to perform activities indicated in paragraphs 4 and 5 above and which are already subject to the full range of applicable obligations under the FATF Forty Recommendations (2003) (in particular, Recommendations 4–16 and 21–25) and the Eight Special Recommendations (in particular SR VII).

**Licensing or Registration and Compliance**

11) Jurisdictions should designate an authority to grant licences and/or carry out registration and ensure that the requirement is observed. There should be an authority responsible for ensuring compliance by money/value transfer services with the FATF Recommendations (including the Eight Special Recommendations). There should also be effective systems in place for monitoring and ensuring such compliance. This interpretation of Special Recommendation VI (for example, the need for designation of competent authorities) is consistent with FATF Recommendation 23.

**Sanctions**

12) Persons providing money/value transfer services without a license or registration should be subject to appropriate administrative, civil, or criminal sanctions.Licensed or registered money/value transfer services that fail to comply fully with the relevant measures called for in the FATF Forty Recommendations or the Eight Special Recommendations should also be subject to appropriate sanctions.

**Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) [Extract]**

This recommendation consists of three major elements:

- Jurisdictions should require licensing or registration of persons or legal entities providing money/value transmission services, including through informal systems or networks.
- Jurisdictions should ensure that money/value transmission services, including informal systems or networks, are subject to FATF Recommendations 10–12 and 15.

---

12 Jurisdictions may authorize temporary or provisional operation of money/value transfer services that are already in existence at the time of implementing this special recommendation to permit such services to obtain a license or to register.

1 Please note that the reference to recommendations in the guidance note below refers to the 1996 version of the FATF 40 Recommendations.
• Jurisdictions should be able to impose sanctions on money/value transmission services, including informal systems or networks, that fail to obtain a license/register and that fail to comply with relevant FATF Recommendations.

Money or value transfer systems have shown themselves vulnerable to misuse for money laundering or terrorist financing purposes. The intention of SR VI is to ensure that jurisdictions impose anti-money laundering and counter-terrorist financing measures on all forms of money/value transfer systems. To obtain a clear picture of the situation in each jurisdiction through the self-assessment process, an artificial distinction has been made between formal and informal transfer systems in some questions.

The term **money remittance or transfer service** refers to a financial service—often provided by a distinct category of non-bank financial institutions—whereby funds are moved for individuals or entities through a dedicated network or through the regulated banking system. For the purposes of assessing compliance with the FATF Recommendations, money remitter/transfer services are included as a distinct category of NBFI and are thus considered part of the regulated financial sector. Nevertheless, such services are used in some laundering or terrorist financing operations, often as part of a larger alternate remittance or underground banking scheme.

The term **informal money or value transfer system** also refers to a financial service whereby funds or value are moved from one geographic location to another. However, in some jurisdictions, these informal systems have traditionally operated outside the regulated financial sector in contrast to the “formal” money remittance/transfer services described in the preceding paragraph. Some examples of informal systems include the parallel banking system found in the Americas (often referred to as the “Black Market Peso Exchange”), the hawala or hundi system of South Asia, and the Chinese or East Asian systems. For more information on this topic, see the FATF-XI Typologies Report (3 February 2000), available through the FATF Web site at [http://www.fatfgafi.org/FATDocs_en.htm#Trends](http://www.fatfgafi.org/FATDocs_en.htm#Trends), or the Asia Pacific Group Report on Underground Banking and Alternate Remittance Systems (18 October 2001), available through the APG Web site at [http://www.apgml.org/content/typologies_reports.jsp](http://www.apgml.org/content/typologies_reports.jsp).

Where licensing or registrations are indicated in the questionnaire, either licensing or registration is considered sufficient to meet the requirements of the Recommendation. Licensing in this recommendation means a requirement to obtain permission from a designated government authority in order to operate a money/value transmission service. Registration in this recommendation means a requirement to register or declare the existence of a money/value transmission service in order for the business to operate. It should be noted that the logical consequence of the requirements of SR VI is that jurisdictions should designate a licensing or registration authority and an authority to ensure compliance with FATF Recommendations for money/value transmission services, including infor-
mal systems or networks. This corollary interpretation of SR VI (for example, the need for designation of competent authorities) is consistent with FATF Recommendation 26.

The reference to “all FATF Recommendations that apply to banks and non-bank financial institutions” includes as a minimum Recommendations 10, 11, 12, and 15. Other applicable Recommendations include Recommendations 13, 14, 16–21, and 26–29. The full text of these and all other FATF Recommendations may be consulted on the FATF Web site (http://www.fatf-gafi.org/40Recs_en.htm).
Appendix H: FATF Special Recommendation VII

VII. Wire transfers

Countries should take measures to require 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 monitoring of suspicious activity funds transfers that do not contain complete originator information (name, address and account number).

Interpretive Note to Special Recommendation VII: Wire Transfers

Objective

1) Special Recommendation VII (SR VII) was developed with the objective of preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting such misuse when it occurs. Specifically, it aims to ensure that basic information on the originator of wire transfers is immediately available (i) to appropriate law enforcement and/or prosecutorial authorities to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing the assets of terrorists or other criminals, (ii) to financial intelligence units for analyzing suspicious or unusual activity and disseminating it as necessary, and (iii) to beneficiary financial institutions to facilitate the identification and reporting of suspicious transactions. Due to the potential terrorist financing threat posed by small wire transfers, countries should aim for the ability to trace all wire transfers and should minimize thresholds taking into account the risk of driving transactions underground. It is not the intention of the FATF to impose rigid standards or to mandate a single operating process that would negatively affect the payment system. The FATF will continue to monitor the impact of SR VII and conduct an assessment of its operation within three years of full implementation.
Definitions

2) For the purposes of this interpretive note, the following definitions apply.

a) The terms *wire transfer* and *funds transfer* refer to any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution. The originator and the beneficiary may be the same person.
b) *Cross-border transfer* means any wire transfer where the originator and beneficiary institutions are located in different countries. This term also refers to any chain of wire transfers that has at least one cross-border element.
c) *Domestic transfer* means any wire transfer where the originator and beneficiary institutions are located in the same country. This term therefore refers to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the wire transfer may be located in another country.
d) The term *financial institution* is as defined by the FATF Forty Recommendations (2003). The term does not apply to any persons or entities that provide financial institutions solely with message or other support systems for transmitting funds.
e) The *originator* is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the wire transfer.

Scope

3) SR VII applies, under the conditions set out below, to cross-border and domestic transfers between financial institutions.

Cross-border wire transfers

4) Cross-border wire transfers should be accompanied by accurate and meaningful originator information. However, countries may adopt a de minimus threshold (no higher than USD or EUR 1,000). For cross-border transfers below this threshold:

a) Countries are not obligated to require ordering financial institutions to identify, verify record, or transmit originator information.
b) Countries may nevertheless require that incoming cross-border wire transfers contain full and accurate originator information.

5) Information accompanying qualifying cross-border wire transfers must always contain the name of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number must be included.
6) Information accompanying qualifying wire transfers should also contain the address of the originator. However, countries may permit financial institutions to substitute the address with a national identity number, customer identification number, or date and place of birth.

7) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they shall be exempted from including full originator information, provided they include the originator’s account number or unique reference number (as described in paragraph 8), and the batch file contains full originator information that is fully traceable within the recipient country.

Domestic wire transfers

8) Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless full originator information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, financial institutions need only include the account number or a unique identifier provided that this number or identifier will permit the transaction to be traced back to the originator.

9) The information must be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate authorities. Law enforcement authorities should be able to compel immediate production of such information.

Exemptions from SR VII

10) SR VII is not intended to cover the following types of payments:

   a) Any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction. However, when credit or debit cards are used as a payment system to effect a money transfer, they are covered by SR VII, and the necessary information should be included in the message.

   b) Financial institution-to-financial institution transfers and settlements where both the originator person and the beneficiary person are financial institutions acting on their own behalf.

Role of ordering, intermediary, and beneficiary financial institutions

Ordering financial institution

11) The ordering financial institution must ensure that qualifying wire transfers contain complete originator information. The ordering financial institution must also verify this information for accuracy and maintain this information in accordance with the standards set out in the FATF Forty Recommendations (2003).
Intermediary financial institution

12) For both cross-border and domestic wire transfers, financial institutions processing an intermediary element of such chains of wire transfers must ensure that all originator information that accompanies a wire transfer is retained with the transfer.

13) Where technical limitations prevent the full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer (during the necessary time to adapt payment systems), a record must be kept for five years by the receiving intermediary financial institution of all the information received from the ordering financial institution.

Beneficiary financial institution

14) Beneficiary financial institutions should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and, as appropriate, whether they are thus required to be reported to the financial intelligence unit or other competent authorities. In some cases, the beneficiary financial institution should consider restricting or even terminating its business relationship with financial institutions that fail to meet SRVII standards.

Enforcement mechanisms for financial institutions that do not comply with wire transfer rules and regulations

15) Countries should adopt appropriate measures to monitor effectively the compliance of financial institutions with rules and regulations governing wire transfers. Financial institutions that fail to comply with such rules and regulations should be subject to civil, administrative, or criminal sanctions.

Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) (Extract)

This recommendation consists of three elements:

- Jurisdictions should require financial institutions to include originator information on funds transfers sent within or from the jurisdiction.
- Jurisdictions should require financial institutions to retain information on the originator of funds transfers, including at each stage of the transfer process.
- Jurisdictions should require financial institutions to examine more closely or to monitor funds transfers when complete originator information is not available.

For the purposes of SR VII, three categories of financial institutions are specifically concerned (banks, bureaux de change, and money remittance/transfer
services), although other financial services (for example, stockbrokers, insurance companies, and so on) may be subject to such requirements in certain jurisdictions.

The list of types of accurate and meaningful originator information indicated in the Special Recommendation (that is, name, address and account number) is not intended to be exhaustive. In some instances—in the case of an occasional customer, for example—there may not be an account number. In certain jurisdictions, a national identity number or a date and place of birth could also be designated as required originator information.

The term enhanced scrutiny for the purposes of SR VII means examining the transaction in more detail in order to determine whether certain aspects related to the transaction could make it suspicious (origin in a country known to provide safe haven to terrorists or terrorist organizations, for example) and thus warrant eventual reporting to the competent authority.
IX. Cash couriers

IX. Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate, and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and SR III, which would enable the confiscation of such currency or instruments.

**Interpretive Note to SR IX: Cash couriers**

**Objectives**

1) FATF SRIX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures (i) to detect the physical cross-border transportation of currency and bearer negotiable instruments, (ii) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, (iii) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed, (iv) to apply appropriate sanctions for making a false declaration or disclosure, and (v) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. Countries should implement SR IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.
Definitions

2) For the purposes of SR IX and this Interpretative Note, the following definitions apply.

3) The term bearer negotiable instruments includes monetary instruments in bearer form, such as traveler’s checks; negotiable instruments (including checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including check, promissory notes, and money orders) signed, but with the payee’s name omitted.13

4) The term currency refers to banknotes and coins that are in circulation as a medium of exchange.

5) The term physical cross-border transportation refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (i) physical transportation by a natural person, or in that person’s accompanying luggage or vehicle, (ii) shipment of currency through containerized cargo, or (iii) the mailing of currency or bearer negotiable instruments by a natural or legal person.

6) The term false declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

7) The term false disclosure refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

8) When the term related to terrorist financing or money laundering is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organizations; or (ii) laundered proceeds from money laundering or predicate offences, or instrumentalities used in or intended for use in the commission of these offences.

13 For the purposes of this Interpretative Note, gold, precious metals, and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals, or precious stones, it should consider notifying, as appropriate, the Customs Service, or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.
The types of systems that may be implemented to address the issue of cash couriers

9) Countries may meet their obligations under SR IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

a) Declaration system: The key characteristics of a declaration system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a preset, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the preset threshold is sufficiently low to meet the objectives of SR IX.

b) Disclosure system: The key characteristics of a disclosure system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

Additional elements applicable to both systems

10) Whichever system is implemented, countries should ensure that their system incorporates the following elements:

a) The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.

b) Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.

c) Information obtained through the declaration/disclosure process should be available to the FIU either through a system whereby the FIU is notified about suspicious cross-border transportation incidents or by making the declaration/disclosure information directly available to the FIU in some other way.

d) At the domestic level, countries should ensure that there is adequate co-ordination among customs, immigration, and other related authorities on issues related to the implementation of SR IX.

e) In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering or terrorist financing may be found: (i) where there is a suspicion of
money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

f) The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with SR V and Recommendations 35–40. To facilitate such cooperation, in instances when (i) a declaration or disclosure which exceeds the maximum threshold of EUR/USD 15,000 is made, or (ii) where there is a false declaration or false disclosure, or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by the appropriate authorities. At a minimum, this information will cover: (i) the amount of currency or bearer negotiable instruments declared/disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

Sanctions

11) Persons who make a false declaration or disclosure should be subject to effective, proportionate, and dissuasive sanctions, whether criminal civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil, or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and SR III, which would enable the confiscation of such currency or bearer negotiable instruments.
VIII: Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Nonprofit organizations are particularly vulnerable, and countries should ensure that they cannot be misused:

- By terrorist organizations posing as legitimate entities
- To exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures
- To conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organizations.

**Interpretive Note to Special Recommendation VIII:**

**Nonprofit Organizations**

**INTRODUCTION**

1) Nonprofit organizations play a vital role in the world economy and in many national economies and social systems. Their efforts complement the activity of the governmental and business sectors in providing essential services, comfort and hope to those in need around the world. The ongoing international campaign against terrorist financing has unfortunately demonstrated, however, that terrorists and terrorist organizations exploit the nonprofit organization sector to raise and move funds, provide logistical support, encourage terrorist recruitment, or otherwise support terrorist organizations and operations. This misuse not only facilitates terrorist activity but also undermines donor confidence and jeopardizes the very integrity of nonprofit organizations. Therefore, protecting the nonprofit organization sector from terrorist abuse is both a critical component of the global fight against terrorism and a necessary step to preserve the integrity of nonprofit organizations.

2) Nonprofit organizations may be vulnerable to abuse by terrorists for a variety of reasons. Nonprofit organizations enjoy the public trust, have access to considerable sources of funds, and are often cash-intensive. Furthermore, some nonprofit organizations have a global presence that provides a framework for national and international operations and financial transactions, often within or near those areas that are most exposed to terrorist activity. Depending on the legal form of the nonprofit organization and the country, NPOs may often be subject to little or no governmental oversight (for
example, registration, record keeping, reporting, and monitoring), or few formalities may be required for their creation (for example, there may be no skills or starting capital required, no background checks necessary for employees). Terrorist organizations have taken advantage of these characteristics of nonprofit organizations to infiltrate the sector and misuse nonprofit organization funds and operations to cover for or support terrorist activity.

**Objectives and General Principles**

3) The objective of SR VIII (SR VIII) is to ensure that nonprofit organizations are not misused by terrorist organizations: (i) to pose as legitimate entities; (ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; or (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes but diverted for terrorist purposes. In this Interpretative Note, the approach taken to achieve this objective is based on the following general principles:

a) Past and ongoing abuse of the nonprofit organizational sector by terrorists and terrorist organizations requires countries to adopt measures both (i) to protect the sector against such abuse and (ii) to identify and take effective action against those nonprofit organizations that either are exploited by or actively support terrorists or terrorist organizations.

b) Measures adopted by countries to protect the nonprofit organization sector from terrorist abuse should not disrupt or discourage legitimate charitable activities. Rather, such measures should promote transparency and engender greater confidence in the sector, across the donor community and with the general public that charitable funds and services reach intended legitimate beneficiaries. Systems that promote achieving a high degree of transparency, integrity and public confidence in the management and functioning of all nonprofit organizations are integral to ensuring the sector cannot be misused for terrorist financing.

c) Measures adopted by countries to identify and take effective action against nonprofit organizations that either are exploited by or actively support terrorists or terrorist organizations should aim to prevent and prosecute as appropriate terrorist financing and other forms of terrorist support. Where nonprofit organizations suspected of or implicated in terrorist financing or other forms of terrorist support are identified, the first priority of countries must be to investigate and halt such terrorist financing or support. Actions taken for this purpose should to the extent reasonably possible avoid any negative impact on innocent and legitimate beneficiaries of charitable activity. However, this interest cannot excuse the need to undertake immediate and effective actions to advance the immediate interest of halting terrorist financing or other forms of terrorist support provided by nonprofit organizations.
d) Developing cooperative relationships among the public, private, and non-profit organization sector is critical to raising awareness and fostering capabilities to combat terrorist abuse within the sector. Countries should encourage the development of academic research on and information sharing in the nonprofit organization sector to address terrorist financing related issues.

e) A targeted approach in dealing with the terrorist threat to the nonprofit organization sector is essential given the diversity within individual national sectors, the differing degrees to which parts of each sector may be vulnerable to misuse by terrorists, the need to ensure that legitimate charitable activity continues to flourish, and the limited resources and authorities available to combat terrorist financing in each jurisdiction.

f) Flexibility in developing a national response to terrorist financing in the nonprofit organization sector is also essential to allow it to evolve over time as it faces the changing nature of the terrorist financing threat.

**The types of systems that may be implemented to address the issue of cash couriers**

4) For the purposes of SR VIII and this interpretative note the following definitions apply:

a) The term *nonprofit organization* refers to a legal entity or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social, or fraternal purposes, or for the carrying out of other types of “good works.”

b) The terms FIU, legal arrangement, and legal person are as defined by the FATF Forty Recommendations (2003) (the FATF Recommendations).

c) The term funds is as defined by the Interpretative Note to FATF Special Recommendation II.

d) The terms freezing, terrorist, and terrorist organization are as defined by the Interpretative Note to FATF Special Recommendation III.

e) The term appropriate authorities refers to competent authorities, self-regulatory bodies, accrediting institutions, and other administrative authorities.

f) The term *beneficiaries* refers to those natural persons, or groups of natural persons who receive charitable, humanitarian, or other types of assistance through the services of the nonprofit organization.

**Measures**

5) Countries should undertake domestic reviews of their nonprofit organization sector or have the capacity to obtain timely information on its activities, size, and other relevant features. In undertaking these assessments, countries should use all available sources of information to identify features and types of nonprofit organizations, which by virtue of their activities or characteristics, are at risk of being misused for terrorist financing.14 Countries should also

14 For example, such information could be provided by regulators, tax authorities, FIUs, donor organizations, or law enforcement and intelligence authorities.
periodically reassess the sector by reviewing new information on the sector’s potential vulnerabilities to terrorist activities.

6) There is a diverse range of approaches in identifying, preventing, and combating terrorist misuse of nonprofit organizations. An effective approach, however, is one that involves all four of the following elements: (a) outreach to the sector, (b) supervision or monitoring, (c) effective investigation and information gathering, and (d) effective mechanisms for international cooperation. The following measures represent specific actions that countries should take with respect to each of these elements to protect their nonprofit organization sector from terrorist financing abuse.

a) Outreach to the nonprofit sector concerning terrorist financing issues

(i) Countries should have clear policies to promote transparency, integrity, and public confidence in the administration and management of all nonprofit organizations.

(ii) Countries should encourage or undertake outreach programs to raise awareness in the nonprofit organization sector about the vulnerabilities of nonprofit organizations to terrorist abuse and terrorist financing risks, and the measures that nonprofit organizations can take to protect themselves against such abuse.

(iii) Countries should work with the nonprofit organization sector to develop and refine best practices to address terrorist financing risks and vulnerabilities and thus protect the sector from terrorist abuse.\(^\text{15}\)

(iv) Countries should encourage nonprofit organizations to conduct transactions via regulated financial channels, wherever feasible, keeping in mind the varying capacities of financial sectors in different countries and in different areas of urgent charitable and humanitarian concerns.

b) Supervision or monitoring of the nonprofit organization sector

Countries should take steps to promote effective supervision or monitoring of their nonprofit organization sector. In practice, countries should be able to demonstrate that the following standards apply to nonprofit organizations which account for (1) a significant portion of the financial resources under control of the sector; and (2) a substantial share of the sector’s international activities.

(i) Nonprofit organizations should maintain information on (1) the purpose and objectives of their stated activities; and (2) the identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. This information

\(^{15}\) The FATF’s Combating the Abuse of Nonprofit Organizations: International Best Practices provides a useful reference document for such exercises.
should be publicly available either directly from the nonprofit organization or through appropriate authorities.

(ii) Nonprofit organizations should issue annual financial statements that provide detailed breakdowns of incomes and expenditures.

(iii) Nonprofit organizations should be licensed or registered. This information should be available to competent authorities.16

(iv) Nonprofit organizations should have appropriate controls in place to ensure that all funds are fully accounted for and are spent in a manner that is consistent with the purpose and objectives of the nonprofit organization’s stated activities.

(v) Nonprofit organizations should follow a “know your beneficiaries and associate nonprofit organizations17” rule, which means that the nonprofit organization should make best efforts to confirm the identity, credentials and good standing of their beneficiaries and associate nonprofit organizations. Nonprofit organizations should also undertake best efforts to document the identity of their significant donors and to respect donor confidentiality.

(vi) Nonprofit organizations should maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organization. This also applies to information mentioned in paragraphs (i) and (ii) above.

(vii) Appropriate authorities should monitor the compliance of nonprofit organizations with applicable rules and regulations.18 Appropriate authorities should be able to properly sanction relevant violations by nonprofit organizations or persons acting on behalf of these nonprofit organizations.19

c) Effective information gathering and investigation

(i) Countries should ensure effective cooperation, coordination, and information sharing to the extent possible among all levels of appropriate authorities or organizations that hold relevant information on nonprofit organizations.

16 Specific licensing or registration requirements for counter terrorist financing purposes are not necessary. For example, in some countries, nonprofit organizations are already registered with tax authorities and monitored in the context of qualifying for favorable tax treatment (such as tax credits or tax exemptions).

17 The term associate nonprofit organizations includes foreign branches of international nonprofit organizations.

18 In this context, rules and regulations may include rules and standards applied by self-regulatory bodies and accrediting institutions.

19 The range of such sanctions might include freezing of accounts, removal of trustees, fines, decertification, de-licensing, and deregistration. This should not preclude parallel civil, administrative, or criminal proceedings with respect to nonprofit organizations or persons acting on their behalf where appropriate.
(ii) Countries should have investigative expertise and capability to examine those non-profit organisations suspected of either being exploited by or actively supporting terrorist activity or terrorist organisations.

(iii) Countries should ensure that full access to information on the administration and management of a particular non-profit organisation (including financial and programmatic information) may be obtained during the course of an investigation.

(iv) Countries should establish appropriate mechanisms to ensure that when there is suspicion or reasonable grounds to suspect that a particular non-profit organisation: (1) is a front for fundraising by a terrorist organisation; (2) is being exploited as a conduit for terrorist financing, including for the purpose of escaping asset freezing measures; or (3) is concealing or obscuring the clandestine diversion of funds intended for legitimate purposes, but redirected for the benefit of terrorists or terrorist organisations, this information is promptly shared with all relevant competent authorities in order to take preventive or investigative action.

d) Effective capacity to respond to international requests for information about an non-profit organisation of concern

Consistent with SR V, countries should identify appropriate points of contact and procedures to respond to international requests for information regarding particular non-profit organisations suspected of terrorist financing or other forms of terrorist support.

Guidance Notes for the Special Recommendations on Terrorist Financing (March 27, 2002) (Extract)

The intent of SR VIII is to ensure that legal entities (juridical persons), other relevant legal arrangements, and in particular non-profit organisations may not be used by terrorists as a cover for or a means of facilitating the financing of their activities. This recommendation consists of two elements:

- Jurisdictions should review the legal regime of entities, in particular non-profit organizations, to prevent their misuse for terrorist financing purposes.
- With respect specifically to non-profit organisations, jurisdictions should ensure that such entities may not be used to disguise or facilitate terrorist financing activities, to escape asset freezing measures or to conceal diversions of legitimate funds to terrorist organisations.

As stated above, the intent of SR VIII is to ensure that legal entities, other relevant legal arrangements, and non-profit organisations may not be misused by terrorists. Legal entities have a variety of forms that differ from one jurisdiction to another. The degree to which a particular type of entity may be vulnerable to misuse in terrorist financing may also vary from one jurisdiction to another.
For this reason, a selection of types of legal entities and other legal arrangements has been presented in the SAQTF in an attempt to obtain a clear picture of the situation in individual jurisdictions. The selection is based on types of entities that have been observed as being involved in money laundering and/or terrorist financing activities in the past. Individual categories may overlap, and in some instances, a jurisdiction may not have all the categories indicated in the SAQTF.

Similarly it should be pointed out that non-profit organisations, a particular focus of SR VIII, may exist in legal forms that vary from one jurisdiction to another. Again, the selection of entity types in the SAQTF has been made with the intention of permitting jurisdictions to find entities or arrangements that correspond to their individual situation. The term non-profit organisation can be generally understood to include those types of entities that are organized for charitable, religious, educational, social, or fraternal purposes, or for the carrying out of other types of “good works.” In addition, the earnings of such entities or activities should normally not benefit any private shareholder or individual, and they may be restricted from direct or substantial involvement in political activities. In many jurisdictions, non-profit organisations are exempt from fiscal obligations.

In the SAQTF, the term off-shore companies refers to what are usually established as limited liability juridical persons in certain jurisdictions and which often fall under a separate or privileged regulatory regime. Such entities may be used to own and operate businesses (a shell or holding company), issue shares or bonds, or raise capital in other manners. They are generally exempt from local taxes or subject to a preferential rate and may be prohibited from doing business in the jurisdiction in which they are incorporated. The International Business Corporation (IBC) is an example of such an entity. In the SAQTF, jurisdictions should only respond to relevant offshore questions if they have an offshore sector within their jurisdiction.

The SAQTF also includes a category “trusts and/or foundations” under SR VIII. Trusts are legal arrangements available in certain jurisdictions. Although they are not strictly speaking legal entities, they are used as a means for holding or transmitting assets and may, as with certain legal entities, be misused as a means for hiding or disguising true ownership of an asset. The term foundations refers primarily to “private foundations or establishments” that exist in some civil law jurisdictions and which may engage in commercial and/or non-profit activities. Some examples of these include Stiftung, stichting, Anstalt, and so on.
Module 6 Answers

Answer 1
The financing of terrorism is providing financial support for terrorism or for those who encourage, plan, or engage in terrorism. The source of terrorist financing may be legitimate, in contrast to the source of laundered money. CFT efforts are aimed at impeding terrorist financing. (See section 1.3 in Module 1: What is terrorist financing and how does it contrast with money laundering?)

Answer 2
The answer is (c). The main difference between money laundering and terrorist financing is that terrorist financing may come from legitimate sources, such as donations to charities, as well as illegitimate sources. By contrast, money laundering involves only ill-gotten funds obtained by illicit acts.

Answer 3
Terrorist financing not only poses a threat to security; it also undermines economic prosperity and poses a long-term threat to development by diverting money from productive to unproductive uses, damaging the country’s reputation in the eyes of investors and tourists, and generating crime and corruption. It can have a devastating impact on stability, transparency, and the efficiency of financial systems. (See section 2 in Module 1: The implications of money laundering and terrorist financing for development.)

Answer 4
In reality all of these characteristics are part of a weak AML/CFT regime. (See section 2 in Module 1: The implications of money laundering and terrorist financing for development.) Countries have a great deal of flexibility in meeting the international AML/CFT standards. Among the few universal requirements are ratification and implementation of the Vienna and Palermo Conventions, criminalization of money laundering and terrorist financing, and implementation of procedural measures, such as laws that allow for freezing and confiscation. (See section 2, in Module 2: What legal and institutional arrangements satisfy international standards.) Otherwise, it is up to each country to adopt laws that are consistent with its own domestic legal system. (See section 4 in Module 2: Where can one find model laws?)

It is also up to each country to designate the “competent authorities” that supervise financial institutions and other non-financial businesses and professions. Given the wide scope of financial institutions, it is likely that countries will need
to create more than one supervisory body. (Review the country examples presented in Section 1 in Module 3: Responsibility for effective supervision.)

Answer 5
No. The terms of the SFT Convention do not leave room for any such justification. According to Article 6 of the Convention, states should “ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious, or other similar nature.”

Answer 6
No. Although people disagree on what terrorism is, there is general agreement about what it is not. The right to strike is not in question. Nor is peaceful demonstration. Some jurisdictions have decided to insert expressly in their CFT legislation exceptions for this type of political activity.

Answer 7
This is a key issue blocking the adoption of a definition of terrorism for the draft United Nations comprehensive convention on international terrorism. So far, no exception of this type has been inserted in the draft. But it is safe to say that groups struggling against foreign occupation will have to comply with humanitarian law (for example, protection of civilians). In addition, an armed conflict, even noninternational, is not justification for armed groups to commit terrorist acts.

Answer 8
The acts committed by the Liberation Front of Valachia are terrorist acts. Bombing infrastructure endangers civilians and is clearly a situation covered by the SFT Convention. Providing financial support for such acts is financing terrorism. By contrast, there is no reason to consider the Free Valachia party as an organization that has committed terrorist acts. Individuals must have the right to exercise their right to demonstrate and their right of free speech through a political party. Unless it can be proved that the party has financed specific terrorist acts, a terrorist, or a terrorist organization, international standards on the financing of terrorism may not apply.

Answer 9
The fact that a country has already adopted legislation on terrorism does not mean that no further steps need to be taken at the domestic level to ensure the efficiency of the legal framework for combating terrorist financing. The fact that Al-Qaeda and connected groups have not attacked the country and that evidence of terrorist financing has not yet been reported is not a valid reason for not acting. Rurithania should ratify the SFT Convention and ensure that its
national legislation and legal framework enable it to comply with international rules and standards on combating the financing of terrorism.

**Answer 10**
Yes. If the intentional element described above is present, the simple fact of collecting funds constitutes the criminal offense of financing terrorism under FATF Special Recommendation II. It is not relevant whether the funds collected were actually used to carry out a terrorist act or whether they were connected to a particular terrorist act.

**Answer 11**
Yes. The SFT Convention is very clear on this issue. The attempt to commit an offense of financing terrorism is also an offense for the purpose of the SFT Convention (Article 2.4).

**Answer 12**
Yes. Financing terrorism is a criminal offense even if the offenders are located in another jurisdiction. The extraterritorial dimension of terrorist activities cannot be a pretext for doing nothing. There is no doubt that states must criminalize the financing of terrorism on their territory. It should be equally clear that when a national of country A commits the offense of financing terrorism on the territory of country B, that action should be a prosecutable offense under the legislation of country A. (See article 7 of the SFT Convention for other extraterritorial situations and paragraph 1.b of Resolution 1373 (2001).

**Answer 13**
According to the SFT Convention, the offense of financing of terrorism should be punishable by appropriate penalties (Article 4.2). Actually, the convention and the Resolution 1373 (2001) stress the fact that the offense of financing terrorism has a “grave nature” or is a “serious criminal offense” (Resolution Paragraph 2.e). This standard leaves to each party the right to define the exact penalties entailed by the acts of financing of terrorism. Examples of penalties are long-term imprisonment, punitive fines, withdrawal or suspension of business licenses, or suspension or removal of management or directors of legal entities.

The SFT Convention requires of states that legal entities (such as shell banks and international corporations) located on their territory or organized under their laws must be held liable when an individual responsible for management or control of the entity has, in that capacity, committed an offense of financing terrorism. In addition, if cash is transported across borders and used in terrorist financing, states are required by FATF SR IX on cash couriers to adopt confiscation measures (see section 13).
**Answer 14**
The financing of terrorism must be considered a predicate offense of money laundering. In the many legal systems where the financing of terrorism is already considered a serious crime, the law on money laundering—which applies to the laundering of the proceeds of *serious crimes*—will automatically cover the financing of terrorism among the predicate offenses of money laundering. In countries that maintain a list of the predicate offenses of money laundering, terrorist financing must be added to the list.

**Answer 15**
The answer is (d). The SFT Convention refers only to “funds” of terrorists. FATF SR III, on the other hand, covers “funds and other assets.” In the same vein, Resolution 1373 (2001) requires broadly the seizure of “funds and other financial assets or economic resources of a person.” But looking at the definition of funds in the SFT Convention, it appears that the three instruments have similar coverage. A state may not interpret the term “funds” restrictively in order to exclude other forms of property from the scope of the international obligations.

**Answer 16**
True: Measures for freezing and confiscation of terrorists’ assets should proceed in accordance with national legislation and in conformity with human rights and international obligations. For example:

a) States should allow persons whose funds have been frozen to challenge the measure in court.

b) States should have procedures for considering requests to be removed from lists of suspected terrorists and to unfreeze the assets of de-listed persons.

c) States should ensure that the rights of third parties acting in good faith are not impaired by the freezing of assets.

d) States should authorize access to funds frozen pursuant to Resolution 1267 (1999) if access is needed to cover basic expenses or certain fees recognized under Resolution 1452 (2002).

**Answer 17**
No. There is no room for a political exception.

**Answer 18**
True. The scope of the obligation may vary from state to state depending on the international instruments it has accepted. But as a matter of principle, states are bound to provide assistance in the suppression of terrorist financing.
Answer 19
The answer is (d). Exchange of information may occur on the basis of a bilateral or multilateral treaty, or under the terms of domestic legislation. Less formal methods, such as a memorandum of understanding among agencies, may be preferred by the parties.

Answer 20
The answer is (d). According to the World Bank, workers’ remittances have climbed steadily since 1998, reaching US$93 billion in 2003, up 20 percent from 2001. They are now the second most important financial flow to developing countries after foreign direct investment. Remittances are almost twice as great as flows of official aid. (Source: Global Development Finance 2004.)

Answer 21
The answer is (b). If a bank receives a wire transfer from a bank located in a foreign country that does not contain the name or address of the originator of the wire, it should consider this omission as a cause for concern. The standard of enhanced scrutiny, and FATF SR IV, oblige banks to have in place a mechanism for monitoring and detecting suspicious transactions.

Answer 22
The answer is (d). When bank A receives an international wire transfer from foreign bank B through a financial intermediary and that transfer does not contain meaningful originator information, it is the duty of bank A to give the transfer the same enhanced scrutiny that it would give to a direct wire. That a correspondent bank was involved does not change this. FATF SR VII underlines the importance of retaining the wire information through the entire chain of payment. But this requirement does not relieve the bank at the end of the payment chain from its duty to monitor possible suspicious transactions.

Answer 23
No. Gold, other precious metals, and precious stones are not among the assets considered as cash equivalents, despite their high liquidity and their use in certain situations as a means of exchange or of transmitting value. But the cross-border transportation of these items may be subject to other control mechanisms established by customs laws and regulations.

Answer 24
Yes. Although SR IX does not mention it expressly, the accompanying Interpretative Note makes it clear that state agencies responsible for implementing a declaration or disclosure system should be entitled to request further informa-
tion on the origin of cash from a person who provides false information in the course of carrying it across a border. This power is necessary if the monitoring process is to be effective.

Answer 25
FATF SR VIII does not suggest that countries should crack down on the entire nonprofit sector. The vast majority of charities provide important services to their communities; for that reason, states should balance the pros and cons of oversight mechanisms to avoid interference with legitimate charitable activities.

FATF Best Practice explains “the charitable sector is a vital component of the world economy and of many national economies and social systems that complements the activity of the governmental and business sectors in supplying a broad spectrum of public services and improving quality of life. We wish to safeguard and maintain the practice of charitable giving and the strong and diversified community of institutions through which it operates.”

Answer 26
FATF SR VIII does not impose a single oversight model. States retain the flexibility to choose the best means of achieving the goal set by the standard. Measures should be based on an objective assessment of the risks of abuse. Thus, considerations of religion, per se, should not interfere with the level of oversight.

Answer 27
Oversight of charities should focus on the financial operations of the organizations in question. Greater scrutiny would be recommended in the case of disbursements to foreign recipients. In such cases, there is a clear risk that charities are being used to finance international terrorist activities.


Answer 28
Terrorism—the financing of terrorism—collecting

Answer 29
The correct assertions are (a), (c), and (d).

Answer 30
States—individuals—organizations or entities—lists
Answer 31
No. In addition to ratifying the SFT Convention states must implement the convention in their national legal system. States also should ensure that they comply with the mandatory terms of relevant UN Security Council resolutions and should take the necessary measures for implementing the FATF Special Recommendations.

Answer 32
Yes. This is supported by the instruments cited above. States should criminalize offenses committed abroad by their nationals as well as those committed on their territory.

Answer 33
The answer is (b).

Answer 34
stones—metals—anti-money laundering—reasonable grounds

Answer 35
False. The duty of states to cooperate pertains not only to criminal procedures but also to civil enforcement and administrative investigations related to the fight against the financing of terrorism.

Answer 36
Assertion (b) is most accurate.

Answer 37
True
Money laundering and the financing of terrorism are global problems that not only threaten a country's security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank's Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide's modules are:

- **Module 1:** Effects on Economic Development and International Standards
- **Module 2:** Legal Requirements to Meet International Standards
- **Module 3a:** Regulatory and Institutional Requirements for AML/CFT
- **Module 3b:** Compliance Requirements for Financial Institutions
- **Module 4:** Building an Effective Financial Intelligence Unit
- **Module 5:** Domestic (Inter-Agency) and International Cooperation
- **Module 6:** Combating the Financing of Terrorism
- **Module 7:** Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Investigating Money Laundering and Terrorist Financing

Workbook
7

Investigating Money Laundering and Terrorist Financing

Workbook
About the Training Modules

Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide is one of the products of the Capacity Enhancement Program on Anti–Money Laundering and Combating the Funding of Terrorism (AML/CFT), which has been co-funded by the Governments of Sweden, Japan, Denmark, and Canada. The program offers countries the tools, skills, and knowledge to build and strengthen their institutional, legal, and regulatory frameworks to successfully implement their national action plan on these efforts.

This workbook is one of the following training course modules:

**MODULE 1: EFFECTS ON ECONOMIC DEVELOPMENT AND INTERNATIONAL STANDARDS**

Module 1 introduces the fundamental concepts of money laundering and terrorist financing; their implications for development from economic, social, and governance perspectives; and existing international standards and key international players in the fight against money laundering and terrorist financing.

**MODULE 2: LEGAL REQUIREMENTS TO MEET INTERNATIONAL STANDARDS**

Module 2 covers satisfying the international standards on AML/CFT and the legislative action that this usually requires. In exploring those implications and possible legislative needs, this workbook answers the following questions:

- What are the international conventions and treaties that deal with AML/CFT?
- What legal and institutional arrangements satisfy international standards?
- What are the legal issues related to international cooperation?
- Where can one find model laws?

**MODULE 3A: REGULATORY AND INSTITUTIONAL REQUIREMENTS FOR AML/CFT**

Module 3a introduces the regulatory and institutional requirements for AML/CFT and addresses the following issues:

- Responsibility for effective supervision
- Institutions subject to AML/CFT compliance
- The principal regulatory and institutional requirements
- Internal audit and compliance programs
- Professional associations and their roles
- Enforcement of AML/CFT requirements

**MODULE 3B: COMPLIANCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS**

Module 3b considers AML/CFT from the perspective of a bank or other financial institution and provides the necessary information for employees of such institutions who deal with a wide range of AML/CFT issues. It also provides additional inputs for compliance officers of financial institutions. A separate section of the workbook deals with some issues that are more pertinent to compliance officers.
Module 4: Building an Effective Financial Intelligence Unit

Module 4 examines the financial intelligence unit (FIU) and its role in the national AML/CFT regime and addresses the following issues:

- Basic concepts of the FIU, suspicious transaction reports, and how they fit into AML/CFT regimes
- Building FIU functionality
- Coordination and cooperation at the policy and operational levels
- Skills, integrity, and security of FIU personnel

Module 5: Domestic (Interagency) and International Cooperation

Module 5 introduces the importance of interagency and international cooperation in the fight against money-laundering activities.

Module 6: Combating the Financing of Terrorism

Module 6 focuses on combating the financing of terrorism (CFT), a new area for many countries compared to the anti-money laundering (AML) effort. The workbook starts with a brief review of the CFT issues raised in the previous workbooks, addresses some general questions related to CFT, and then discusses the FATF Nine Special Recommendations on Terrorist Financing in combination with the international obligation of states.

Module 7: Investigating Money Laundering and Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime and discusses investigations of terrorist financing activities.

Acknowledgments

Module 7 was written by Fred Meyers. The draft was reviewed by Martin Comley, the World Bank, and Matthew Byrne and Louise Schultz, AUSTRAC. Pedagogical guidance was provided by Sheila Jagannathan, and peer-review was given by Emiko Todoroki and John McDowell, the World Bank. In 2007 and 2008, updates and reviews were provided by Klaudijo Stroligo, Paul Allan Schott, and Emiko Todoroki, the World Bank. Key sources for this workbook include “Financial Action Task Force on Money Laundering,” “The Forty Recommendations,” 2003, and “Special Recommendations on Terrorist Financing,” 2005.

Capacity Enhancement Program on Anti–Money Laundering and Combating the Financing of Terrorism

Program Director: Latifah Merican Cheong
Task Team Leader: Emiko Todoroki
Instructional Design: Sheila Jagannathan
Production: Miguel Nicolas De La Riva, Jr.
Illustrations: James Quigley
Composition: Precision Graphics, Champaign, Illinois
Investigating
Money Laundering and
Terrorist Financing

Module 7 introduces the practice of investigating activities that involve laundering of the proceeds of crime. Module 7 will also discuss investigations of terrorist financing activities. The following key issues will be addressed:

1. Basic concepts in investigations of money laundering and terrorist financing 3
   1.1 What is money laundering? 4
   1.2 What is terrorist financing? 4
   1.3 How do money laundering investigations differ from terrorist financing investigations? 4
   1.4 Who investigates money laundering and terrorist financing cases? 5

2. What are the sources of information for money laundering and terrorist financing cases? 6
   2.1 Financial intelligence units 6
   2.2 Criminal cases 11
   2.3 Informants 12
   2.4 Cooperating defendants 14
   2.5 Law enforcement agencies 14
   2.6 Referrals from banks and other financial institutions 16
   2.7 Cross-border operations 17

3. The stages of investigation in money laundering and terrorist financing cases 20
   3.1 (a) Planning a money laundering investigation 20
   3.1 (b) Planning a terrorist financing investigation 21
   3.2 Methods of gathering evidence 22
      3.2.1 Financial interviews 22
      3.2.2 Search warrants 23
      3.2.3 Surveillance 24
      3.2.4 Trash pickup 24
      3.2.5 Analysis of bank records 25
      3.2.6 Forensic science 26
3.3 Special investigative techniques 27
  3.3.1 Consensual monitoring 27
  3.3.2 Undercover operations 28

This module covers the following Recommendations:
• Financial Action Task Force (FATF) Recommendations 26, 27, 28, 30
• FATF Special Recommendation IX

All of these deal with institutional issues relevant to money laundering and terrorist financing investigation.

At the end of Module 7, you will be able to
• develop leads to a money laundering or terrorist financing case;
• plan a criminal investigation of money laundering or terrorist financing;
• identify evidence to be collected in a criminal investigation of money laundering or terrorist financing;
• describe the variety of investigative techniques that can be used to gather evidence of money laundering or terrorist financing; and
• identify various ways to request and obtain evidence from banks, businesses, and individuals in a foreign country.
1 Basic concepts in investigations of money laundering and terrorist financing

How much do you know?

**QUESTION 1.** What is the main difference between money laundering and financing of terrorism in terms of their sources of funds?

**QUESTION 2.** Do international standards require countries to investigate money laundering and terrorist financing cases?

a) Yes, the FATF and international organizations require countries to do so.
b) No, there are no specific requirements in this matter.

**QUESTION 3.** Name two types of reports that the financial intelligence units (FIUs) receive from financial institutions.

**QUESTION 4.** Name two sources of information that can lead to the opening of a money laundering investigation.
1.1 What is money laundering?
Money laundering is a part of most criminal activities that generate profits (or proceeds) for criminals. Most criminals and criminal organizations, regardless of their crimes or structure, have three objectives related to the proceeds of their illegal activity. These are (1) to pay expenses connected to their illegal activity; (2) to invest their proceeds in furtherance of their illegal activity; and (3) to enjoy the profits of their criminal activity. Laundering illegal funds accomplishes these goals.

Money laundering by a criminal or criminal organization can expose the criminal to investigation and prosecution. It also can expose the higher echelons of a criminal organization—those who make the profit but are not closely involved in the predicate criminal activity.

1.2 What is terrorist financing?
Terrorism needs money to operate. Terrorists need funds to purchase weapons, equipment, supplies, and services. Financing for terrorist activity may come from public (government-sponsored terrorism) or private (individuals, businesses, charities, nongovernmental organizations [NGOs]) sources, often in the form of many small donations. Funds may be generated from legal or criminal activity.

Activities to prevent and deter terrorist financing activities are varied and many. The FATF 9 Special Recommendations on Terrorist Financing suggest some methods of combating those activities. Governments are encouraged to put the recommendations into effect.

This module will discuss techniques to investigate the crime of terrorist financing.

1.3 How do money laundering investigations differ from terrorist financing investigations?
Investigations of terrorist financing and money laundering are similar in that both require the gathering of information on financial transactions. That information may come in the form of financial records obtained from domestic and international sources or from the testimony of witnesses.

In other ways, the two types of investigations differ. In money laundering cases, money often follows the path from the criminal activity to the criminal, and often into the purchase of assets (e.g., cars, jewelry, or homes). In terrorist financing cases, monies are traced from their origin (e.g., criminal activity or donations) to a terrorist organization, and then to terrorists or terrorist cells who use the funds to support themselves and/or to carry out their terrorist activities.
1.4 Who investigates money laundering and terrorist financing cases?

Each country determines by law or common practice the authorities that are empowered to conduct money laundering investigations. Some countries have formed special “financial investigative units” to investigate money laundering cases and other financial crimes. Others have authorized their police to investigate money laundering. The police, in turn, assign the investigations to their fraud or financial crime units. Still others have state security officers who investigate financial crimes, including money laundering. In some countries investigating magistrates pursue money laundering crimes. In others, the agency charged with investigating the crime that generated the criminal proceeds (such as a drug or fraud agency) also has the authority to investigate money laundering.

Responsibility for investigating crimes of terrorist financing also varies by country. Some countries have formed task forces composed of representatives from the police, state security, customs, immigration, and the FIU to work together to investigate terrorist financing. Others have given the responsibility to the police or state security agencies.

Several of the FATF 40 Recommendations deal with law enforcement:

FATF Recommendation 27 states, in part, “countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations.” For more information on FATF Recommendation 27, see Appendix B.

FATF Recommendation 30 states, in part, “countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources.” For more information on FATF Recommendation 30, see Appendix C.

The choice of whether to create a new investigative unit to pursue crimes of money laundering or terrorist financing, or to assign such investigations to an existing investigative unit or police force, is a decision that each country must make. In each case, the unit needs educated, trained, and dedicated investigators who can conduct complex financial investigations. In addition, it must be adequately funded.
What are the sources of information for money laundering and terrorist financing cases?

Many different sources can provide information for use in initiating or pursuing money laundering investigations:

- FIUs, or anti–money laundering units—the primary sources in most countries
- Criminal cases, open or closed
- Informants
- Cooperating defendants in civil or criminal cases
- Law enforcement agencies
- Banks and financial institutions
- Cross-border operations from any of the above

Sources of information for terrorist financing investigations are similar to those for money laundering investigations. An additional source for terrorist financing investigations may be intelligence gathered by police or other authorities on terrorist groups and their associates. As you read the material that follows, keep in mind that much of the information on money laundering investigations also applies to terrorist financing investigations.

In conducting investigations of money laundering, terrorist financing, and underlying predicate offences, FATF Recommendation 28 stresses that competent authorities should be able to obtain documents and information for use in those investigations and in prosecutions. For more information on FATF Recommendation 28, see Appendix D.

**2.1 Financial intelligence units**

FIUs receive (and, as permitted, request), analyze, and disseminate to competent authorities financial information that the financial institutions and designated non-financial businesses and professions (DNFBPs) are obligated to disclose in the form of suspicious activity reports or suspicious transaction reports (SARs/STRs).

FATF Recommendation 26 specifies that each country should establish an FIU for the purpose of gathering and analyzing information on possible financial crime and other abuses of the financial system. The FATF also encourages FIUs to join the Egmont Group, which is an association of FIUs formed for cooperation, coordination, and mutual assistance. For more information on FATF Recommendation 26, see Appendix E.
After analysis, the FIU forwards SARs/STRs or case referrals to investigating agencies for review. Under the guidelines of the Egmont Group, and according to FATF Recommendation 40, the FIU also may request information from FIUs in other countries. It may request other FIUs to search their databases for information on a suspect and on a transaction(s). In any investigation of a financial crime, such a database search should be requested.

FIUs prepare reports from information they gather from many sources. Law enforcement authorities should review those reports carefully for information that may warrant initiation of a money laundering investigation. A detailed discussion of FIUs and their operation is contained in Module 4 of this course.

---

**How do FIUs handle referrals?**

*Review and consideration of FIU referrals*

FIUs receive reports of suspected money laundering, terrorist financing, or financial crimes from financial institutions and DNFBPs. The FIU queries its own, government, and commercial databases about the persons, businesses, or entities mentioned in the report. The FIU may also try to determine if any of the subjects has a criminal record by querying judicial or police records.

After compiling all the information from databases and other sources, the FIU prepares a report that includes an analysis of the transaction(s) reported. If the information is available, the FIU will analyze money movement between banks or bank accounts, companies, individuals, and countries. If allowed by the local law, the FIU may also decide to postpone or suspend a suspicious transaction in order to analyze the transaction and confirm the suspicion.

The investigator must review the FIU’s report for information that might cause the law enforcement agency to open a criminal investigation on the subject(s) of the report. Certain circumstances are especially likely to lead to the opening of an investigation:

- The subject of the report has a prior criminal record, and the amount of the reported financial transaction is large or very unusual.
- A suspected intermediary—lawyer, accountant, or financial institution—is involved in the transaction.
- The transaction appears to have been made in the name of someone other than the ultimate beneficiary, indicating an attempt to avoid scrutiny by authorities.
- The transaction is of a higher value than might be expected from the individuals concerned, considering their income or business.
- The investigator already has intelligence about the subject of the SAR/STR (or other report).
- The FIU referral details multiple reports of suspicious activities and/or transactions from one or more reporting entities.

—continued
A document prepared by the Egmont Group titled “100 Cases from the Egmont Group” details money laundering cases that began as referrals to law enforcement from FIUs worldwide. Since it was prepared before September 11, 2001, the document does not relate to terrorist financing.

Financial transaction reports can be a good source of intelligence for any investigation—for example, the details of the address provided at the time of the transaction can help investigators locate a suspect.

The reports that an FIU receives can be grouped into such categories as:

- SARs/STRs
- Currency transaction reports (CTRs)
- Currency transaction reports by casinos (CTRCs)
- Wire transfer reports
- Cross-border reports

The above list of categories is not exhaustive. Some of the reports are discussed in the following sections.

**Suspicious transaction or activity reports**

Many countries now require financial institutions and DNFBPs to report to the FIU suspicious financial transactions, activities, and other transactions, such as significant cash transactions and wire transfers (see module 4). Although the form and content of the report differ from country to country, SARs/STRs generally are excellent leads to possible money laundering, terrorist financing, or other financial crime.

The investigator or analyst reviewing the SAR/STR should first of all look for the following items that raise the intelligence value or investigative potential of a given STR:

- References to known criminals, or to individuals or companies that appear in numerous SARs/STRs
- Reports of the movement of money to countries that are sources of or transit locations for narcotics, or that are international tax havens or money centers
Investigating Money Laundering and Terrorist Financing

References to financial activities that are known to be used in money laundering or financial fraud

- Reports from different financial institutions in the same area or region that detail similar financial activity, but by different individuals
- Conflicting data on individuals or entities mentioned in the SAR/STR, or data conflicts between SAR/STRs
- Reports of deposits of domestic or foreign currency to business or individual accounts that are not justified by the size or nature of the business

Currency transaction reports

Many countries require financial institutions and DNFBPs, to file with the FIU a CTR whenever they make cash transactions over a set monetary threshold—such as $10,000 U.S. dollars, 50,000 Mexican pesos, or 10,000 euros. Analysis of CTRs can identify individuals and businesses that are involved in financing of terrorism or money laundering activities. The investigator or analyst reviewing the CTR should look in particular for the following items that raise the intelligence value or investigative potential of the CTR:

- References to known criminals, or to individuals or companies that appear in numerous CTRs
- Reports of the movement of money to countries that are sources of or transit locations for narcotics, or that are international tax havens or money centers
- CTRs that report financial activity that is a known money laundering technique or financial fraud activity, such as the exchange of small bills for large ones
- Reports from different financial institutions in the same area or region that detail similar financial activity, but by different individuals
- Conflicting data on individuals or entities mentioned in the CTR, or data conflicts between CTRs, indicating an attempt to avoid scrutiny
- Reports of transactions by businesses that are not large enough to justify the amounts deposited
- Reports of individuals who attempted to dissuade the bank or financial institution from filing the CTR

Currency transaction reports by casinos

Some countries require that casinos report to the FIU large currency transactions made by their customers. In the United States, for example, cash transactions within the casino of more than $10,000 must be reported. Qualifying transactions include buying chips for cash, redeeming chips for cash, paying off a line of credit with cash, or receiving winnings in cash. Analysis of these reports, known as CTRCs, can identify individuals who may be involved in money laundering or other financial crimes. The investigator or

—continued
QUESTION 5. What types of records do casinos maintain?

a) Casinos maintain records of gambling activity, including gambling histories of “high rollers,” who may receive complimentary rooms, meals, and airfare.

b) Casinos maintain records of payouts made by check or wire transfer.

c) If required by local law, casinos maintain records of chips purchased and cashed in, over a certain amount.

d) All of the answers are correct.

QUESTION 6. Are casinos required to file SARs/STRs?

a) Yes

b) No

c) It depends on national laws and regulations
2.2 Criminal cases

Before you begin this section, answer this question.

**QUESTION 7.** Can information obtained from a closed criminal case or an open criminal investigation be used to start a money laundering investigation?

- a) Yes
- b) No
- c) It depends on the law of the country

In many countries, information obtained from ongoing criminal investigations (see the subsequent box for more information) or from the files of closed cases (see the subsequent box for more information) can be used to initiate or pursue a money laundering investigation. Financial information obtained from financial institutions, businesses, and witnesses in criminal investigations can be leads to evidence of money laundering activity.

---

**Information from an ongoing criminal investigation**

The most direct way to identify money laundering is to follow financial leads in an ongoing criminal case. If the crime involves money and financial transactions, the buying and selling of contraband (narcotics, illegal guns or weapons, stolen property), or criminal services (abuse of power, insider trading, public corruption), investigators should “follow the money.”

Every interview you do in your investigation should include questions about money: “Who paid you?” “Who collected from you?” “Who paid the expenses?” “Who took the money to the bank? Was the person an attorney or an accountant, and if so which one(s)?” “Who counted the money?”

After a few such interviews, a picture of the proceeds of the crime should begin to emerge. You will learn who receives the money, counts it, banks it, and launders it.
WHY ARE OPEN CASES SUCH GOOD SOURCES OF INFORMATION FOR INVESTIGATIONS INTO MONEY LAUNDERING AND TERRORIST FINANCING?

Because most crimes are committed for money, the collection, transfer, and payment of money are part of most criminal activities. Gathering evidence about the movement of money can lead to evidence of money laundering. That is why open criminal cases are excellent sources of information for a money laundering investigation.

Information from closed investigations

Another source of a money laundering investigation is to open a money laundering investigation of a known criminal who is involved in financial crimes. If attempts to prosecute a known criminal failed in the past, conducting a financial investigation of that individual financial activity might make a successful money laundering case.

During the investigation, follow the money! Ask everyone you talk to about the money: Who pays whom? Who collects from whom? Who counts? Who is the banker? Who is the lawyer? Who is the accountant? Where does the money come from? Where does the money go?

Knowledge check

QUESTION 8. What is meant by the phrase “follow the money”? Provide your answer in the space below.

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

2.3 Informants

QUESTION 9. Can information obtained from an informant be used to initiate an investigation?

a) Yes
b) No
c) It depends on the law of the country

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________
Informants can provide valuable information in a money laundering investigation. An informant is a person who possesses direct or indirect knowledge of criminal or other unlawful activity and who makes that information available to a representative of law enforcement. Some informants may wish to remain anonymous and may not want to testify in future criminal proceedings. Some informants provide information to law enforcement officers on an ongoing basis.

The potential role of informants in money laundering investigations should not be underestimated. Informants can reduce the time spent on an investigation. Informants can give investigators valuable insight into the inner workings of criminal organizations and provide leads that would not have been available through other investigative means. They can even be used in undercover situations, where warranted. For example, an informant may be a member of the criminal group under investigation or a friend of the group’s members. In such cases, the informant can be used to introduce an undercover police officer to the group so that the officer can collect evidence of criminal activity.

The useful tips in this matter are:

- Thoroughly interview informants who have information on the movement of money from criminals and criminal organizations.
- Be sure to establish the parameters of what the informant can or cannot do to ensure the integrity of the investigation.
- Develop all information provided by the informant to the fullest extent possible.
- Cross-check it with other sources of intelligence.

---

**How to know your informants and be aware of their motives**

When cultivating informants, it is important to consider motives. An individual’s motives for becoming an informant may be an indicator of reliability or credibility. Generally, an informant’s motives will fall into one or more of the following categories:

- **Monetary gain.** The informant may be looking to be rewarded for participating in an investigation.
- **Revenge.** The informant may be attempting to get even with someone by providing information in an investigation.
- **Altruism.** The informant may be concerned about the well being of others.
- **Self-aggrandizement.** The informant may seek to present an exaggerated image of himself or herself.
- **Personal gain.** The person is seeking some sort of personal gain in exchange for his or her cooperation, such as the elimination of his or her competition.

Other motives might include a fascination with law enforcement or the pursuit of some kind of thrill.

---

*—continued*
2.4 Cooperating defendants

Like informants, cooperating defendants can be an invaluable tool in developing leads or otherwise assisting in investigations. Cooperating defendants are persons who have been convicted or are facing legal action for having committed a crime. Their primary motive is usually personal gain. They are looking to “cut a deal” or obtain leniency in exchange for providing information or testimony relative to criminal activity. Like informants, they can offer insight into the criminal operation that may not be available through other investigative means.

In a money laundering investigation, the cooperating defendant can provide valuable information on the movement of money to or from a criminal organization and testimony about the extent of the organization’s money laundering. He or she also may be able to identify additional coconspirators and professionals, attorneys, or accountants, who have assisted in any money laundering scheme. Finally, such an individual can be useful in identifying assets derived from criminal ventures and in interpreting ledgers, books, and other records maintained by the criminal organization.

2.5 Law enforcement agencies

Other law enforcement agencies are valuable sources of information that can lead to the opening of a money laundering investigation. Narcotics enforcement agencies and customs agencies, in particular, may have valuable information in their case files. Often they are the first to recognize criminal activity linked to financial transactions. Examples of some other agencies are:

- State security services
- Anticorruption agencies
- Tax or other financial police.

We have discussed some of the agencies in the following boxes.
For discussion

Country laws differ, but generally, a defendant may cooperate with government officials and provide information on codefendants and other criminals. In your country, may a defendant cooperate with investigators and prosecutors and provide information on codefendants or other criminals?

In your country, do the narcotics and customs agencies have a role in fighting money laundering?

In your country, can the narcotics and customs authorities forward information about possible money laundering activity to the FIU or agency that investigates money laundering crimes? Most countries do allow their narcotics and customs agencies to share information with the FIU and money laundering investigators.
2.6 Referrals from banks and other financial institutions

Another source of a potential money laundering investigation is referrals from bank and financial services regulators. Regulators of banks and other financial institutions are responsible for ensuring that financial service providers comply with pertinent laws and regulations. They examine financial institutions for safety and soundness, assessing compliance with regulations related to credit practices, liquidity, capital adequacy, and operational risks in a wide range of areas. Examinations shall also include checks of institutions’ anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

Most countries require financial regulators to share information about potential money laundering or financing of terrorism with investigators. The FATF encourages countries to promote cooperation in money laundering and terrorist financing matters. For example, in Europe, the third European Union Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing in Article 25 requires member states to ensure that, if in the course of inspections carried out in the obliged entity by the supervisory authorities, or in any other way, these authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU. In your country, can regulators of financial institutions forward information on possible money laundering matters to the FIU?

---

**Information uncovered through examination**

In the course of their work, examiners are also likely to do “transaction testing” in risk areas, such as account deposits, wire transfers, loan portfolios, transactions or business relationships with politically exposed persons, correspondent banking relationships, and private banking.

Some examples of information that could be uncovered during transaction testing:

- Suspicious wire transfer activity, such as a high volume of transfers, or simultaneous transfers
- Evidence of account “structuring” not readily observed in daily banking activity
- Incomplete account information, such as omitted identifiers of nationality
- Questionable loans and loan practices
- Early payoffs of large loans
- Cash reserves at a level inconsistent with banking volume
- Transactions with shell banks
2.7 Cross-border operations

**QUESTION 10.** Can customs, immigration, and state security agencies detect and deter money laundering and terrorist financing activity? Provide your answer in the space below.

Money launderers often smuggle currency, financial instruments, precious stones, or metals from the country in which the crime was committed to another country. The currency or financial instruments are then placed in the other country’s financial institutions, such as banks.

The detection of currency smuggling by customs or immigration authorities at borders and entry ports can lead to or assist money laundering or financing of terrorism investigations.

Each country may have different agencies responsible for border control activities and investigations. Each country must decide which agency will investigate illegal cross-border movement of funds related to money laundering or terrorist financing.

**Border operations to detect currency smuggling at ports of entry**

Many countries’ customs services, immigration services, and state security departments conduct enforcement programs at ports of entry to identify currency smuggling operations. Countries that require currency and monetary instruments to be declared or reported upon entry into or exit from the country will often conduct compliance programs to enforce the reporting requirements.

For example, customs officials may conduct enforcement programs to identify currency smuggling at airports hosting flights to or from known money centers, such as London, Moscow, New York, Nassau, and so on.

Currency-smuggling compliance programs may be designed to identify outbound or inbound activity at airports and other ports of entry. Passenger lists and customs declaration forms may be reviewed for passengers who travel frequently between major money centers or known tax havens and offshore banking centers. Foreign visitors who travel frequently to or from your country may be screened. Many techniques can be used to build an “inbound/outbound” compliance program to detect currency smuggling or illegal cross-border movement of currency.
QUESTION 11. How can customs play a larger role in AML/CFT operations? Provide your answer in the space below.

Customs services, immigration, state security agencies, and other agencies should be included in a country’s AML/CFT strategy. All countries should have in place programs to detect and investigate currency smuggling and the illegal cross-border movement of currency related to money laundering and terrorist financing.

FOR DISCUSSION

In your country, do the customs, immigration, and state security services have a role in fighting money laundering and terrorist financing? Do they have a program to detect and investigate currency smuggling or illegal cross-border movements of currency related to money laundering or terrorist financing?
What are the international standards in this matter?
FATF Special Recommendation IX states, in part: “Countries should have measures in place to detect the physical cross-border transportation of currency and bearer instruments, including a declaration system or other disclosure obligation. Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed.” For more information on FATF Special Recommendation IX and the Interpretative Note to this Special Recommendation, see Appendix F.
Any criminal investigator who has the authority to investigate serious financial fraud—such as bank embezzlement or check fraud—can investigate money laundering. The difference between money laundering and other financial fraud is the time it may take to investigate the money laundering scheme and the underlying criminal activity that generates the funds. Planning the investigation may also require a great deal of time.

### 3.1 (a) Planning a money laundering investigation

In any financial investigation (including money laundering) it takes time to obtain bank and business records. Even more time is required if the records are in another country. Proper planning will alert the investigator to seek foreign records early in the investigation and to initiate contact with his or her counterpart in the country in question. Although bank and business records figure in most financial investigations, they rarely provide sufficient evidence, on their own, to justify a conviction.

### Planning the investigation

A money laundering case should be guided by a work plan that specifies:

- Witnesses to be contacted
- Domestic and international financial records needed
- Procedures for managing documents
- Surveillance requirements
- Desired evidence of criminal activity and proceeds
- Analysis, summaries, and graphic representations of evidence
- Any special investigative techniques required.

The initial phases of the investigation should proceed as discreetly as possible. Surveillance of the subject and associates early in an investigation can provide valuable leads to evidence. But early disclosure of an investigation can cause the subject and associates to take precautions that may make surveillance useless. It may also cause the suspect or key witnesses to destroy or alter records.

Bank records should be obtained early and discreetly. One set of records usually leads the investigator to seek another. When records are needed from other countries, the delay can be months. Delays in obtaining records can slow an investigation down, so begin collecting them early on in the investigation.
Planning an investigation of terrorist financing begins with the formation of the investigative team. Who are its members? In addition to investigators from the police and other investigative agencies, other specialists may be needed, such as intelligence officers and analysts, military officers, financial analysts (representing the FIU), accountants, and auditors. Who will direct and manage the investigation? It could be the police, military, an intelligence service, or another appropriately qualified and authorized government entity. What are the roles and duties of each member of the team? Who gathers evidence from the public (such as banks, charities, NGOs, witnesses)?

The financial evidence gathered in a terrorist financing case is similar to that gathered in a money laundering case. Where was the money obtained? Who gathered it? Who deposited it? Who carried it across the border? Were wire transfers used? What banks or bankers were involved? Were attorneys or accountants involved?

Once evidence from financial institutions, businesses, NGOs, and witnesses is collected, it must be analyzed. Leads to additional evidence may be gathered from informants or with search warrants and special investigative techniques.

Knowledge check

**QUESTION 12.** What are some of the items that must be addressed when planning an investigation into money laundering or terrorist financing? Provide your answer in the space below.

---

Plan the use of search warrants. Time their execution to maximize chances of obtaining evidence. Surveillance will provide information that can be used to set the time of the search (after a delivery, after a meeting, during a meeting, and so on). Sometimes, it is good practice to interview suspects or witnesses at the time of the search warrant execution.

If allowed by law, consider using special investigative techniques to assist in gathering evidence. The use of undercover operations, wire taps, or consensual telephone monitoring can produce valuable evidence.
3.2 Methods of gathering evidence

3.2.1 Financial interviews

Financial information obtained from defendants, witnesses, and informants is critical in money laundering or financing of terrorism investigations.

Types of interviews

Interviews of defendants

Subjects of an investigation often agree to be interviewed. They usually will answer questions on financial matters because they feel such questions are “harmless.” Ask such questions as:

- Where do you bank?
- What type of accounts do you have?
- Do you have investment accounts with a stockbroker?
- Do you have accounts in any foreign countries?
- Who is your accountant?

Asking questions of a financial nature rather than questions on criminal activity often disarms subjects and leads them to talk.

Interviews of witnesses and informants

Ask witnesses and informants about the financial activity being investigated.

- Who collected the money involved in the activity under investigation?
- Where was the money stored?
- What bank was used?
- What bankers were involved?
- How were you paid and by whom?

If you concentrate your questions on financial transactions, money handling, and banking activity, a picture will soon emerge of how the individual or group handles money—and of how it may be laundering money.
Knowledge check

**QUESTION 13.** What is the meaning of the following sentence: "Ask questions about the who, what, when, where, why, and the how of money handling?"

---

3.2.2 Search warrants

**QUESTION 14.** Can search warrants be used in a money laundering (or terrorist financing) investigation?

---

Local law and practice set forth the circumstances under which searches may be made. Use of this investigative technique must follow local law.

Search warrants are used routinely in criminal investigations. If local law permits, they can be used in a money laundering or terrorist financing investigation. If the investigating officer has knowledge of the existence and location of evidence (books, records, or other documents) that can help prove a money laundering or terrorist financing crime, a search warrant often can be obtained and used. Normally a search warrant is obtained through the courts and must be signed by a judge or magistrate. The search warrant authorizes the authorities to search a particular location—house, business location, car, boat—for items that could constitute evidence of money laundering, such as bank records, business records, money counting machines, currency wrappers, currency, or any record that could contain information on the movement of money. Searches can yield investigative leads, evidence, contraband, high-value goods, and even cash. The timing of searches is very important. Should search warrants be executed early or late in an investigation? Should the residence or office to be searched be empty? Or should the search be made when the suspects are present? Should the warrant be executed at night or during the day? The answer to each of these questions varies depending upon the circumstances of each case. Often, the need to protect evidence demands that the action be conducted as soon as possible. In all cases, however, searches must be performed in accordance with local law.
3.2.3 Surveillance

**QUESTION 15.** How useful is surveillance of people and places in a money laundering or terrorist financing investigation? Provide your answer in the space below.

If allowed by local laws, surveillance can yield valuable leads and evidence in a money laundering or terrorist financing investigation. It is recommended that the suspect in the investigation, as well as the suspect’s employees or associates, be placed under surveillance. The suspect’s residence and business location are equally important. If a bank or other financial institution or remittance agent is suspected of being used for money laundering or terrorist financing activity, surveillance of the institution can yield evidence of individuals or organizations using the institution to launder money.

Surveillance operations should be conducted by trained operatives working in teams. Operatives should be skilled in surveillance techniques. Where possible, physical surveillance should be combined with electronic surveillance of the suspect, couriers, associates, and premises. Vehicles, luggage, and assets purchased with the proceeds of crime should be tracked electronically, if possible.

3.2.4 Trash pickup

**QUESTION 16.** Is it permissible to collect trash from a suspect’s residence or business and use it to develop leads or provide evidence in a money laundering case? Provide your answer in the space below.

A “trash pickup” is an investigative technique to obtain evidence or investigative leads. Abandoned trash often contains items that could be used as evidence or leads in a criminal money laundering case.


3.2.5 **Analysis of Bank Records**

**QUESTION 17.** What role do bank and business records play in an investigation of money laundering or terrorist financing? Provide your answer in the space below.

Bank records are usually essential to an investigation of money laundering or terrorist financing. Bank accounts used to receive the proceeds of crime (or “dirty money”) must be identified—and records of those accounts obtained and analyzed. The legal steps required to obtain bank records are different in each country. Generally, investigators obtain records by a court order or subpoena, or an investigating magistrate or prosecutor. In many countries the bank records are usually enclosed with the FIU’s reports on SARs/STRs sent to the investigators. Check local laws or practices to determine how you should obtain bank records. All money entering the accounts must be identified; all movements of that money traced. Money must be traced from bank account to bank account; and from domestic bank accounts to foreign bank accounts. Records of foreign bank accounts must be obtained and analyzed. Obtaining bank records (or other evidence) from foreign sources is covered in Module 5 of this course.

---

**Planning and executing a trash pickup**

- Locate the residence or business at which trash might yield evidence or leads.
- Contact the trash hauler or use surveillance to determine the day and time the trash is collected.
- Through surveillance, learn when trash is placed in cans or containers at the location.
- Through surveillance, determine the best time for an investigator to pick up the trash from the location without being observed. Early morning and late evening are often the best times.

To carry out the pickup, approach the location by foot and pick up the trash bag. A short distance from the pickup location, have a second investigator in a car or van pick up the first investigator and the trash bag. When in a safe location, sort through the trash (wearing rubber gloves) to find discarded items that may have value as leads or evidence. Such items include bank deposit tickets, used airline ticket stubs, hotel receipts, and so on.
How are bank records analyzed?

Investigators begin by obtaining documents relating to a particular bank account for the time under scrutiny. These include the document used to open the account, the account application, copies of signature cards, copies of identification documents used to open account, letters of referral or introduction, and so on. Other documents may include monthly statements, cancelled checks, deposit tickets, copies of checks deposited, debit and credit memos, wire transfer instructions and documents, and any documents related to account activity.

Analyzing the bank records requires the investigator to review and record the financial activity presented in the bank account records. Begin by adding up the deposits—by week, month, and year. Is there a pattern?

Look at the deposit tickets and the items making up the deposited items. Are they cash or checks? What percentage is cash and what percentage is check? Is there a pattern of unusual (suspicious) deposits? Were funds wired into or out of the account? Is there a pattern of unusual transfers (suspicious activities or transactions)?

Information obtained from analysis of the bank records will yield the names of witnesses, including the bank employees, to interview and businesses to contact for more information.

- Determine the flow of money and amounts.
- Identify money laundering operators.

3.2.6 Forensic Science

QUESTION 18. How can forensic science assist the investigator in a money laundering or financing of terrorism investigation? Provide your answer in the space below.

Forensic science is sometimes required to analyze evidence in a money laundering or terrorist financing case. A document may be analyzed to determine who prepared it, who signed it, and who handled it.

The types of forensic analysis include:

- Handwriting analysis
- Ink analysis
- Paper analysis
- Typewriter/printer analysis
- Fingerprint analysis
Obtaining foreign evidence

Among the formal methods of obtaining bank records, documents, or testimony from foreign countries are: letters rogatory, legal assistance treaties, and executive agreements. These formal methods of obtaining foreign evidence require written requests between “competent authorities” in government, usually ministries of foreign affairs or justice. Module 5 (laws and regulations) discusses effective international cooperation.

Other methods of obtaining foreign information involve direct contact between other relevant agencies in two countries—for example, among police departments, central banks and other regulators/supervisors of financial institutions, or FIUs, as well as requests made through INTERPOL. The Egmont Group has guidelines for exchanges of information between FIUs and in case of Europe, the Council of Europe Warsaw Convention also contain provisions on cooperation between FIUs. Some of these issues have been covered in Module 4.

All of the above methods of requesting information from foreign countries usually require written requests using specific formats. Check with your ministry of foreign affairs, ministry of justice, or FIU to determine the form of request required in your country. You may also refer to the Guidelines of the Egmont Group on exchange of information between FIUs.

3.3 Special investigative techniques

FATF Recommendation 27 encourages countries “to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques.” For more information on FATF Recommendation 27, see Appendix B.

Similar provisions are also included in the UN Palermo Convention (see Article 20) and the UN Convention against Corruption (see Article 50), as well as in regional instruments that are applicable to specific regions, for example, the Council of Europe Strasbourg Convention (see paragraph two of Article 4) and the Council of Europe Warsaw Convention (see paragraph three of Article 7).

3.3.1 Consensual monitoring

Consensual monitoring is the interception, overhearing, or recording of a private conversation by use of mechanical, electronic, or other device with the consent of at least one of the parties. Listening to and recording the conversation of criminals discussing past or future activity can provide valuable evidence for an investigation. Among the types of exchange subject to consensual monitoring are telephone conversations; live conversations carried on in a public or private place; and Internet messaging.

Local law will dictate whether, and under what circumstances, the technique of consensual monitoring can be used. Use of this technique must follow local law.
3.3.2 Undercover Operations

An undercover operation is the infiltration or joining of a criminal enterprise by an informant or law enforcement officer for the purpose of securing information or evidence relating to criminal activity. Local law and practices address the use of undercover operations. Local law will dictate whether, and under what circumstances, undercover operations may be used, as well as any other requirements that must be followed.

Undercover operations can aid a criminal investigation by:

- Determining the illegal activity from which money is generated
- Identifying unknown violators (including money launderers or those who finance terrorist or terrorist organizations)
- Identifying coconspirators and key witnesses
- Identifying and tracing the proceeds from crime or funds to be used in financing of terrorism.

An undercover operation may take one of two forms in a money laundering investigation:

- Law enforcement officers may launder money for a criminal or criminal organization, or
- A money laundering organization may be recruited to launder government money.

The goal of such undercover operations is to gather evidence against the persons handling the money (bankers, attorneys, accountants, or others) or to establish the movement of money (to and from banks, businesses, countries).

Investigation checklist

Identifying and developing leads in money laundering/financing of terrorism investigations

1. Financial intelligence unit
   - Referral to law enforcement by the FIU
2. Suspicious transaction reports
   - From domestic FIU
   - From foreign FIU
   - Routine analysis
   - Special analysis
   - Geographical
   - Industry
   - Products
   - Services
3. Open investigations
   • Start financial investigation as a parallel investigation to an already open investigation
   • Open a financial investigation on a known criminal involved in economic crimes
4. Referrals from bank or other financial sector regulators or examiners
   • Information found during normal examinations of banks and other financial institutions
   • Analysis of currency flows within financial system (financial institutions likely to be involved in money laundering)
   • Information to trace monies
5. Informants
   • Used to identify criminal organization’s money laundering managers
   • Knowledge of finances and money handling
   • Knowledge of illegal activity
6. Cooperating defendants
   • Provide information or evidence relative to a criminal matter in which he or she is involved, including money laundering for the criminal organization
7. Border operations to detect movement of cash
   • Reports of currency or bearer negotiable instruments out of or into the country (forms used when entering/leaving the country)

**Investigative techniques for money laundering investigations**

1. Financial interviews
   • Defendant/target
   • Witnesses
   • Informants
   • Financial institutions
2. Search warrant
   • Issued by a judge or magistrate
   • Authorizes the search and seizure of records that may reveal money laundering operations or property that constitutes evidence of the commission of a crime, contraband, proceeds (fruits) of the crime, instrumentalities, or things criminally possessed
3. Surveillance
   • Obtain information or evidence
   • Probable cause for search warrants
   • Apprehend violators
   • Develop investigative leads
4. Trash pickup
   • Used to identify leads
   • Gather evidence
5. Analysis of bank/financial records
   • Determine flow of money and amounts
   • Identify money laundering operators

—continued
QUESTION 19. List four investigative items to be included in the work plan for a money laundering/terrorist financing investigation. Provide your answers in the space below.

- Forensic science
  - Handwriting analysis
  - Ink and paper analysis
  - Typewriting analysis
  - Fingerprints
  - Computer and information technology

- Analysis of documentary evidence of financial transactions
  - Bank transactions, domestic and foreign
  - Deposits
  - Withdrawals
  - Credit/debit memos
  - Bank checks/money orders

- Other documentary evidence from:
  - Banks and other financial institutions
  - Currency transactions
  - Wire transfers
  - Safe deposit boxes
  - Currency exchanges
  - Credit card records
  - Management companies
  - Stock brokers, securities dealers
  - Insurance companies
  - Money transfer operators such as Western Union and Money Gram
  - Casinos
  - Automobile, boat, and airplane dealers
  - Investment funds
  - Leasing businesses
  - Other organizations or services that receive, transport, send, exchange, or keep funds
  - Offices that conduct legal, notary, accounting, or financial or banking-type services
QUESTION 20. List three types of evidence that are needed in a money laundering/terrorist financing investigation. Provide your answer in the space below.


QUESTION 21. List four investigative techniques used to gather evidence in a money laundering/terrorist financing investigation. Provide your answer in the space below.


QUESTION 22. List two methods to request and obtain evidence from banks or businesses in a foreign country. Provide your answer in the space below.


Summary

In this module, we discussed:

- How to find or develop a money laundering or terrorist financing case to investigate
- How to plan a money laundering or terrorist financing investigation
- What type of evidence needs to be collected in a criminal money laundering investigation
- What investigative techniques are used in gathering evidence of money laundering
- How to obtain evidence from a foreign country
Appendix A: References

FATF Recommendations

- The Forty Recommendations (FATF, June 2003)
  http://www.fatf-gafi.org/dataoecd/7/40/34849567.pdf
- Special Recommendations on Terrorist Financing (FATF, October 2004)

Useful Websites

- Asia & Pacific Amphetamine-Type Stimulants Information Centre (APAIC)
  http://www.apaic.org
- Asia/Pacific Group on Money Laundering (APG)
  http://www.apgml.org/
- Caribbean Financial Action Task Force (CFATF)
  http://www.cfatf.org/eng/
- Council of Europe
  http://www.coe.int/defaultEN.asp
- Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) [European regional AML body for Eastern Europe and offshore jurisdictions that are not members of the FATF]
  http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Money_laundering/
- Department of Foreign Affairs and Trade, Australian Government
- Egmont Group
  http://www.egmontgroup.org/
- European Union (EU)
  http://europa.eu.int/
- Fight against Terrorism, Council of Europe
  http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Fight_against-terrorism/default.asp
- Financial Action Task Force on Money Laundering (FATF)
  http://www.fatf-gafi.org/pages/0,2966,en_32250379_32235720_1_1_1_1_1_1,00.html
- Financial Sector Reform and Strengthening (FIRST) Initiative
  http://www.firstinitiative.org/index.cfm
• Foreign and Commonwealth Office, United Kingdom  
  http://www.fco.gov.uk/
• International Monetary Fund (IMF)  
  http://www.imf.org
• INTERPOL  
  http://www.interpol.int/Default.asp
• Office of Technical Assistance, U.S. Department of the Treasury  
  http://www.ustreas.gov/offices/international-affairs/assistance/enforcement-team.shtml
• Organisation for Economic Co-operation and Development  
  http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html
• Organization for Security and Co-operation in Europe  
  http://www.osce.org/
• Western European Union  
  http://www.ewe.int/
• World Bank  
  http://www.worldbank.org
• World Trade Organization (WTO)  
  http://www.wto.org

Other Useful Web sites
• Centre for Defense and International Security Studies  
  http://www.cdiss.org/
• Economist Intelligence Unit  
  http://www.eiu.com/
• International Crisis Group  
  http://www.crisisgroup.org/home/index.cfm
• Institute for Counter-Terrorism [terrorist organization profiles]  
  http://www.ict.org.il/
• moneylaundering.com  
  http://moneylaundering.com/
• National Memorial Institute for the Prevention of Terrorism (MIPT)  
  http://www.mipt.org/
• MIPT Terrorism Knowledge Base  
  http://www.tkb.org/Home.jsp
• Oanda Foreign Exchange Converter  
  http://oanda.com/convert/classic
• Privacy International [Visit “Privacy and Human Rights”]  
  http://www.privacyinternational.org/index.shtml
• Transparency International [See “Corruption Perceptions Index”]  
  http://www.transparency.org/index.html
• Terrorism Research Center [terrorist organization profiles incidents, attacks and events, country profiles]  
  http://www.terrorism.com/
• UN action against terrorism, United Nations [conventions, declarations, news, and developments]
  http://www.un.org/terrorism/
• World Fact Book, Central Intelligence Agency (CIA)

Reference Documents
• “1999 International Narcotics Control Strategy Report” (Bureau for International Narcotics and Law Enforcement Affairs, U.S. Department of State, March 2000) [Go to the section on Country Reports]
• Patterns of Global Terrorism 2003 (U.S. Department of State, April 2004)
  http://www.state.gov/s/ct/rls/pgtrpt/2003/
Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations, and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialized in asset investigation, and cooperative investigations with appropriate competent authorities in other countries.

**Interpretative Note to Recommendation 27**

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures, the use of such procedures as controlled deliveries and undercover operations are precluded.
Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human, and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.
Appendix D: FATF Recommendation 28

When conducting investigations of money laundering and underlying predicate offenses, competent authorities should be able to obtain documents and information for use in those investigations, in prosecutions, and in related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.
Countries should establish an FIU that serves as a national center for the receiving (and, as permitted, requesting), analysis, and dissemination of STRs and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative, and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

**Interpretative Note to Recommendation 26**

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose and its Principles for Information Exchange between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs and the mechanisms for exchanging information between FIUs.
Appendix F: FATF Special Recommendation IX

Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering or that are falsely declared or disclosed.

Countries should ensure that effective, proportionate, and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would allow for the confiscation of such currency or instruments.

Interpretive Note to Special Recommendation IX: Cash couriers

Objectives

1. FATF Special Recommendation IX was developed with the objective of ensuring that terrorists and other criminals cannot finance their activities or launder the proceeds of their crimes through the physical cross-border transportation of currency and bearer negotiable instruments. Specifically, it aims to ensure that countries have measures (i) to detect the physical cross-border transportation of currency and bearer negotiable instruments; (ii) to stop or restrain currency and bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering; (iii) to stop or restrain currency or bearer negotiable instruments that are falsely declared or disclosed; (iv) to apply appropriate sanctions for making a false declaration or disclosure; and (v) to enable confiscation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering. Countries should implement Special Recommendation IX subject to strict safeguards to ensure proper use of information and without restricting either: (i) trade payments between countries for goods and services; or (ii) the freedom of capital movements in any way.
DEFINITIONS

2. For the purposes of Special Recommendation IX and this Interpretative Note, the following definitions apply.

3. The term *bearer negotiable instruments* includes monetary instruments in bearer form, such as traveler’s checks; negotiable instruments (including checks, promissory notes, and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including checks, promissory notes, and money orders) signed, but with the payee’s name omitted.¹

4. The term *currency* refers to banknotes and coins that are in circulation as a medium of exchange.

5. The term *physical cross-border transportation* refers to any in-bound or out-bound physical transportation of currency or bearer negotiable instruments from one country to another country. The term includes the following modes of transportation: (i) physical transportation by a natural person, or in that person’s accompanying luggage or vehicle; (ii) shipment of currency through containerised cargo; or (iii) the mailing of currency or bearer negotiable instruments by a natural or legal person.

6. The term *false declaration* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data that is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required.

7. The term *false disclosure* refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required.

8. When the term related to terrorist financing or money laundering is used to describe currency or bearer negotiable instruments, it refers to currency or bearer negotiable instruments that are: (i) the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts, or terrorist organizations; or (ii) laundered, proceeds from money laundering or predicate offenses, or instrumentalities used in or intended for use in the commission of these offenses.

¹ For the purposes of this Interpretative Note, gold, precious metals, and precious stones are not included despite their high liquidity and use in certain situations as a means of exchange or transmitting value. These items may be otherwise covered under customs laws and regulations. If a country discovers an unusual cross-border movement of gold, precious metals, or precious stones, it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which these items originated and/or to which they are destined, and should cooperate with a view toward establishing the source, destination, and purpose of the movement of such items and toward the taking of appropriate action.
THE TYPES OF SYSTEMS THAT MAY BE IMPLEMENTED TO ADDRESS THE ISSUE OF CASH COURIERS

9. Countries may meet their obligations under Special Recommendation IX and this Interpretative Note by implementing one of the following types of systems; however, countries do not have to use the same type of system for incoming and outgoing cross-border transportation of currency or bearer negotiable instruments:

   a. Declaration system: The key characteristics of a declaration system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments, which are of a value exceeding a preset, maximum threshold of EUR/USD 15,000, are required to submit a truthful declaration to the designated competent authorities. Countries that implement a declaration system should ensure that the preset threshold is sufficiently low to meet the objectives of Special Recommendation IX.

   b. Disclosure system: The key characteristics of a disclosure system are as follows. All persons making a physical cross-border transportation of currency or bearer negotiable instruments are required to make a truthful disclosure to the designated competent authorities upon request. Countries that implement a disclosure system should ensure that the designated competent authorities can make their inquiries on a targeted basis, based on intelligence or suspicion, or on a random basis.

ADDITIONAL ELEMENTS APPLICABLE TO BOTH SYSTEMS

10. Whichever system is implemented, countries should ensure that their system incorporates the following elements:

   a. The declaration/disclosure system should apply to both incoming and outgoing transportation of currency and bearer negotiable instruments.

   b. Upon discovery of a false declaration/disclosure of currency or bearer negotiable instruments or a failure to declare/disclose them, designated competent authorities should have the authority to request and obtain further information from the carrier with regard to the origin of the currency or bearer negotiable instruments and their intended use.

   c. Information obtained through the declaration/disclosure process should be available to the FIU either through a system whereby the FIU is notified about suspicious cross-border transportation incidents or by making the declaration/disclosure information directly available to the FIU in some other way.

   d. At the domestic level, countries should ensure that there is adequate coordination among customs, immigration, and other related authorities on issues related to the implementation of Special Recommendation IX.

   e. In the following two cases, competent authorities should be able to stop or restrain cash or bearer negotiable instruments for a reasonable time in order to ascertain whether evidence of money laundering
or terrorist financing may be found: (i) where there is a suspicion of money laundering or terrorist financing; or (ii) where there is a false declaration or false disclosure.

f. The declaration/disclosure system should allow for the greatest possible measure of international cooperation and assistance in accordance with Special Recommendation V and Recommendations 35 to 40. To facilitate such cooperation, in instances when: (i) a declaration or disclosure that exceeds the maximum threshold of EUR/USD 15,000 is made; (ii) where there is a false declaration or false disclosure; or (iii) where there is a suspicion of money laundering or terrorist financing, this information shall be retained for use by the appropriate authorities. At a minimum, this information will cover: (i) the amount of currency or bearer negotiable instruments declared/disclosed or otherwise detected; and (ii) the identification data of the bearer(s).

**Sanctions**

11. Persons who make a false declaration or disclosure should be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative. Persons who are carrying out a physical cross-border transportation of currency or bearer negotiable instruments that are related to terrorist financing or money laundering should also be subject to effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, and should be subject to measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or bearer negotiable instruments.
Answers
Module 7 Answers

Answer 1
The funds used for money laundering purposes are acquired through illicit ways (drug trafficking and other criminal activities), but financing of terrorism can be done with both legal and illegal funds.

Answer 2
a)

Answer 3
Examples are any of the following:

a) Suspicious Transactions Reports (STRs)
b) Currency Transactions Reports (CTRs)
c) Unusual Transaction Reports

Answer 4
Any two of the following:

a) FIU referral
b) Open criminal investigation
c) Informant
d) Closed criminal case

Answer 5
d)

Answer 6
a) FATF Recommendation 16 requires casinos to report STRs to the FIU.

Answer 7
c) Local law and practice may affect the initiation of money laundering cases. Unless prohibited by local law, an investigator may use information obtained from another case, opened or closed, to open or conduct a money laundering investigation. Local law must be followed.

Answer 8
To an investigator (or analyst, auditor, or bank examiner) “follow the money,” means to gather information about the movement of money within a criminal organization or as ordered or performed by a criminal. In following the money,
investigators uncover evidence of the financial activity surrounding criminal activity; they also develop leads to money laundering activities. Following the money can yield information on assets purchased with the proceeds of crime or terrorist financing. Those assets can be seized by the government if allowed by law. The FATF and other international organizations require countries to enact laws to allow seizure, freezing, and forfeiture or confiscation of assets associated with terrorist financing and money laundering.

Following the money means tracing the flow of money from the criminal activity to the parties involved in the crime. Investigators document the receipt and disbursement of money from the criminal activity by analyzing documents and records, interviewing witnesses and defendants, and questioning informants.

To follow the money during an interview, ask questions of the witness about payments and collections. Who paid you? To whom did you give the money? Did you ever deliver money to a bank, attorney, or accountant? Did you ever count the money? Were you conducting the transaction on another’s behalf? What other transactions are related to this transaction? Who was the ultimate beneficiary? Ask who, what, where, when, and how.

**Answer 9**

c) Local law and practice may affect how money laundering cases are opened. Local law may also address when and how informant information is used. Unless prohibited by local law, an investigator may use information obtained from an informant to open a money laundering investigation. However, the investigator should verify, if possible, the informant’s information. The investigator must also assess the credibility and reliability of the informant. Local law and policy must be followed.

**Answer 10**

Yes, customs, immigration, state security agencies, and police agencies can detect and deter money laundering and terrorist financing by developing compliance programs and other strategies to address these crimes—particularly when money laundering or terrorist financing occurs at borders and ports of entry.

**Answer 11**

It is a good idea for customs to form an anti-money laundering and financing of terrorism unit to work at ports of entry, particularly airports, that are gateways to “money centers”—that is, cities where currency is most likely to be smuggled. These AML/CFT units should develop expertise in currency smuggling techniques, which are very similar to drug smuggling techniques, and develop the means to identify and seize smuggled currency.
Answer 12

The work plan should specify:

- Witnesses to contact
- Financial records to obtain, domestically and internationally
- Surveillance requirements and expected results of surveillance activity
- Any other special investigative techniques that may be needed
- Evidence of criminal activity and of the proceeds of crime
- Analysis and summaries of evidence

Answer 13

When interviewing someone about money laundering activity (or terrorist financing) ask as many questions as you can about who handled, what was the amount involved, when did the transactions take place, and how the money moved was, where was it deposited, by whom, when, and so on.

Answer 14

If permitted by local law, search warrants may be used to gather evidence in a money laundering investigation. Very valuable evidence can be collected through the use of search warrants executed at residences or businesses used by criminals or criminal organizations. These locations often contain banking documents, travel documents, and miscellaneous records that can prove acts of money laundering or establish the movement of money. Local law must be followed.

Answer 15

Surveillance of people and places can yield valuable leads and evidence in a money laundering investigation. For example, surveillance of the suspect in a money laundering investigation (and of suspect’s employees) can identify banks and remittance agents used, attorneys and accountants consulted, locations where money is stored, vehicles used to transport money, flights used to ship money, and so on. If a bank or other financial institution is suspected of being used for money laundering, surveillance of the bank can identify the individuals using the bank for that purpose.

Surveillance of flights from “money centers” can yield leads to individuals who may be involved in cross-border currency smuggling.

Answer 16

To the extent permitted by local law, collecting trash from a suspect’s residence or business (after it has been put out for disposal) can yield valuable investigative leads and evidence of money laundering activity. Trash may contain discarded documents, bank records, or other items that can indicate money laundering activity.
Physical items that could indicate money laundering are bank wire transfer records; receipts for mailings to offshore banks, attorneys, or accountants; receipts for money orders, cashier’s checks, or travelers’ checks in large amounts; and airline ticket receipts for flights to or from offshore or money centers.

**Answer 17**

Domestic and foreign bank records are often the most valuable documents in every investigation of money laundering or terrorist financing. The documents provide primary pieces of evidence, such as evidence of introduction of the proceeds of crime into the banking system and of the movement of those proceeds between banks and often forms the heart of a money laundering or financing of terrorism investigation.

**Answer 18**

At times during a money laundering or financing of terrorism investigation, forensic analysis of evidence is needed. Fingerprint analysis and handwriting analysis is often needed to determine who prepared or handled a document. Was it an employee of the money launderer, a banker, or an accountant?

Ink analysis or paper analysis sometimes is needed to date a document or to determine the country in which it was prepared. Investigators look for documents that may yield evidence when subjected to forensic analysis.

**Answer 19**

Any four of the following:

- List of witnesses to be interviewed and deposed
- Domestic bank and business records needed
- Need for search warrants, and the points in the investigation when they will be required
- Need for surveillance, and the schedule for carrying it out
- Need for foreign bank or business records

**Answer 20**

Any three of the following:

- Evidence that are the proceeds of crime
- Evidence of money movement to hide or disguise illegal funds
- Witness testimony
- Bank or business documents
**Answer 21**
Any four of the following:

- Subpoena or court order to obtain bank or business records
- Witness interviews
- Surveillance
- Search warrant
- Undercover operation
- Controlled delivery

**Answer 22**
Any two of the following:

- Letters rogatory
- Treaties providing for mutual legal assistance
- Memorandums of understanding
- Cooperation between FIUs
- INTERPOL requests
Money laundering and the financing of terrorism are global problems that not only threaten a country's security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The Combating Money Laundering and the Financing of Terrorism training program was developed by the World Bank's Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide's modules are:

Module 1: Effects on Economic Development and International Standards
Module 2: Legal Requirements to Meet International Standards
Module 3a: Regulatory and Institutional Requirements for AML/CFT
Module 3b: Compliance Requirements for Financial Institutions
Module 4: Building an Effective Financial Intelligence Unit
Module 5: Domestic (Inter-Agency) and International Cooperation
Module 6: Combating the Financing of Terrorism
Module 7: Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.
Money laundering and the financing of terrorism are global problems that not only threaten a country’s security, but also compromise the stability, transparency, and efficiency of its financial system, consequently undermining its economic prosperity. The annual global estimate for money laundering is more than $1 trillion, valued in U.S. dollars. Efforts to counter these activities are known as anti-money laundering and combating the financing of terrorism (AML/CFT) programs.

The *Combating Money Laundering and the Financing of Terrorism* training program was developed by the World Bank’s Financial Market Integrity Unit, with support from the governments of Sweden, Japan, Denmark, and Canada. The program will help countries build and strengthen their AML/CFT efforts by training all relevant staff in both the public and private sectors, such as staff in financial intelligence units, financial supervisory authorities, law enforcement agencies, and financial institutions.

The training guide’s modules are:

**Module 1:** Effects on Economic Development and International Standards
**Module 2:** Legal Requirements to Meet International Standards
**Module 3a:** Regulatory and Institutional Requirements for AML/CFT
**Module 3b:** Compliance Requirements for Financial Institutions
**Module 4:** Building an Effective Financial Intelligence Unit
**Module 5:** Domestic (Inter-Agency) and International Cooperation
**Module 6:** Combating the Financing of Terrorism
**Module 7:** Investigating Money Laundering and Terrorist Financing

The modules cover all the Financial Action Task Force on Anti-Money Laundering’s Forty Recommendations and Nine Special Recommendations, with the original texts. Each module is targeted at a specific group of professionals in a jurisdiction’s AML/CFT regime, although they may also benefit from gaining wider knowledge through the other modules included in this program. Each module provides questions at the beginning and end to assess how much has been learned. The training guide contains numerous case studies, discussions and analyses of hypothetical and actual examples of money laundering schemes, and best practices in investigation and enforcement, which will help readers fully understand the implementation of successful AML/CFT programs.