INTERNATIONAL COMPLIANCE ASSOCIATION

ICA/MoEc Certificate in AML/CFT – Designated Non-Financial Businesses and Professions

Edition 1.0 (2024)

Editions
First Edition, Sep 2024 – ICA/MoEc Certificate in AML/CFT – Designated Non-Financial Businesses and Professions

Published by:
International Compliance Association
Fort Dunlop
6th Floor
Fort Parkway
Birmingham
ENGLAND
B24 9FD
www.int-comp.org

Syllabus

Unit 1: Understanding Money Laundering, Terrorist Financing, Global Standards and Obligations

Learning Objectives

The purpose of this unit is to:

- explain what money laundering is
- outline the methods used by money launderers
- discuss why it is important for designated non-financial businesses and professions (DNFBPs) to avoid involvement in money laundering, and
- define terrorist financing and explain the similarities and differences between money laundering and terrorist financing.

What is a DNFBP?

Before we begin to look at money laundering, it is firstly important to understand what a DNFBP is, what activities are involved and who this course applies to. In order to do so, we will use the Financial Action Task Force (FATF) definition of DNFBPs.

Designated non-financial businesses and professions *means*:

a) 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 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 AML/CFT measures.

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 or performing the equivalent function for another form of legal arrangement;
- acting as (or arranging for another person to act as) a nominee shareholder for another person.

Source: www.fatf-gafi.org/en/pages/fatf-glossary.html#accordion-a13085a728-item-121a8a2b0f

DNFBPs in the UAE

In the UAE, the following categories are considered DNFBPs:

1– Brokers and real estate agents when they conclude operations for the benefit of their Customers with respect to the purchase and sale of real estate.

2 – Dealers in precious metals and precious stones in carrying out any single cash transaction or several transactions that appear to be interrelated or equal to more than AED 55,000.

3 – Lawyers, notaries, and other independent legal professionals and independent accountants, when preparing, conducting or executing financial transactions for their Customers in respect of the following activities: (a) Purchase and sale of real estate. (b) Management of funds owned by the Customer. (c) Management of bank accounts, saving accounts or securities accounts. (d) Organising contributions for the establishment, operation

or management of companies. (e) Creating, operating or managing legal persons or Legal Arrangements. (f) Selling and buying commercial entities.

4 – Providers of corporate services and trusts upon performing or executing a transaction on the behalf of their Customers in respect of the following activities: (a) Acting as an agent in the creation or establishment of legal persons; (b) Working as or equipping another person to serve as director or secretary of a company, as a partner or in a similar position in a legal person. (c) Providing a registered office, work address, residence, correspondence address or administrative address of a legal person or Legal Arrangement. (d) Performing work or equipping another person to act as a trustee for a direct Trust or to perform a similar function in favour of another form of Legal Arrangement. (e) Working or equipping another person to act as a nominal shareholder in favour of another person.

Source: rulebook.centralbank.ae/en/rulebook/111-glossary-terms

DNFBPs are subject to specific anti money laundering (AML) and counter financing of terrorism (CFT) regulations under UAE law. These regulations align with the FATF Recommendations to ensure DNFBPs are not exploited for illicit financial activities.

What is money laundering?

Let's begin by taking a look at some definitions of money laundering.

Most people have an idea of what money laundering is. When asked, people tend to describe it in one of the following ways:

- 'turning dirty money into clean money'
- 'turning money from the illegitimate economy into money in the legitimate economy'
- 'washing drug money', or
- 'disguising criminal money'.

All of these descriptions are generally correct, but they fail to explain the real nature of money laundering and the extent to which it threatens the global financial services industry.

The actual definition of money laundering as per (Article 2) of the UAE AML Law 20 of 2018 is as follows:

Definition: Money laundering

Any person, having the knowledge that the funds are the proceeds of a felony or a misdemeanour, and who wilfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:

a– Transferring or converting proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source.

b– Concealing or disguising the true nature, source or location of the proceeds, or the method involving the disposition, movement or ownership of the Proceeds or rights related thereto.

c– Acquiring, possessing or using proceeds upon receipt.

d– Assisting the perpetrator of the predicate offense to escape punishment.

Source: rulebook.centralbank.ae/en/rulebook/article-2-4

Over time, criminals and terrorists have become more aware of the controls employed by financial institutions and DNFBPs to prevent money laundering, and have sought new or different methods to launder their money or fund their terrorist activities, making such laundering and activities increasingly difficult to detect and prevent.

You might think that decent and honest firms are rarely affected by money laundering – but nothing could be further from the truth. Today, businesses, organisations and professionals from a wide variety of sectors can easily become caught up in money laundering. Reputational damage is the result for both people and firms, as well as criminal prosecution, regulatory censure and in some cases civil proceedings in the form of actions for recovery of assets.

Definition: Anti money laundering (AML)

Countries around the world have legislation in place to tackle money laundering. The sum of this legislation and preventive efforts is referred to AML.

Many countries also possess legislation on terrorist financing, which we will discuss later in the course.

Definition: Counter-financing of terrorism (CFT)

Measures to stop the flow of funds to support terrorists and terrorist organisations financially and materially; this area has received a lot more focus since the terror attacks of 11 September 2001. These efforts are referred to as counter financing of terrorism (CFT) or counter-terrorist financing (CTF).

While **money laundering** and **terrorist financing** are often grouped together, and while there are many similarities, they are quite different, which we will explore in more detail as we progress.

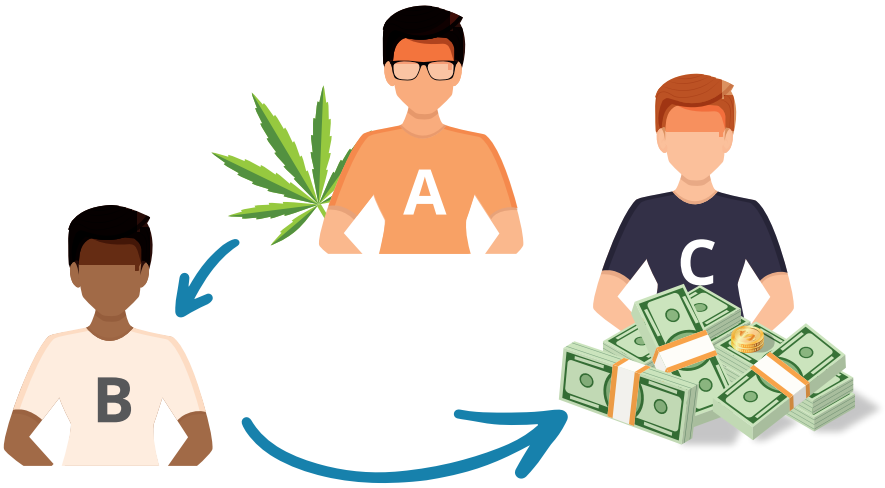
Understanding international money laundering and terrorist financing trends and the risks that flow from these transactions is more important today than ever before. Money laundering and terrorist financing mitigation is an essential prerequisite of good governance and business survival.

Question

So, what really is money laundering?

Quite simply, money laundering occurs every time **any transaction** takes place or **any relationship** is formed that **involves any form of property or benefit** that has come **from any crime**.

The problem is enormous. Consider the following diagram.



A is a drug dealer. He sells $100 of illegal drugs to B. In anticipation of a police investigation into the drug deal, A gives C the money and asks him to hide it for him until 'the coast is clear'. C takes the money and hides it under his mattress.

Is C Laundering A's money? The answer, of course, is **yes**. C has entered into an arrangement with A which involves A's proceeds of crime.

Key learning point

Criminal offences of money laundering are only committed when both the act of money laundering takes place and the person or business that handles the property has the required state of mind, i.e., knows or suspects or has reasonable grounds to suspect, that the property derives from crime (the required state of mind can vary by offence and jurisdiction).

Many businesses have a higher threshold or expectation that they suspect money laundering is taking place – banks are an obvious example of a type of entity with higher expectations placed on them.

Why must you avoid committing the criminal offence of money laundering?

i. **It is morally and ethically wrong to** provide services and products in a way that would **facilitate the laundering of criminal property**.

ii. While criminal liability may not result from relationships about which you have no knowledge or suspicion, **reputational damage** may be incurred

by yourself, by your organisation and by your jurisdiction in the event that a case of financial crime is discovered. Even innocent handling of criminal property is usually enough to generate very damaging media coverage.

iii. Generally, regulated firms have a **regulatory obligation to take measures to protect against exposure to the risk of money laundering**, terrorist financing and other types of financial crime. Any innocent involvement in a relationship which transpires to have featured money laundering or terrorist financing activity may lead to regulatory action being taken against the business and/or its employees, whose fitness and properness may also be questioned.

Offences of money laundering

The offence of money laundering occurs whenever a person or business assists anyone to launder the proceeds of crime while knowing or suspecting or having reasonable grounds to suspect that the property is the proceeds of crime.

We will now look at knowledge, suspicion and reasonable grounds for suspicion.

Knowledge

Question

What constitutes knowledge?

At first sight the answer to this question seems obvious – a person either knows something or they don't. Unfortunately, the truth is more complicated. There are several types of knowledge, including:

- **actual subjective knowledge** – you definitely know some fact(s), e.g., you know the money comes from drug dealing
- **wilfully shutting your eyes to the obvious (or 'wilful blindness')** – this is where you don't ask questions because you think they may reveal information that will mean you have to make a report; here you could be seen as having

'known' but turned a 'blind eye' – for example you think the money comes from a crime but you don't make any further enquiries; and

- **wilfully and recklessly failing to make such enquiries** as a reasonable and honest person would make.

There are dangers in attempting to define what is meant by suspicion, not least because it is by definition subjective and personal to individuals.

Consider

That which seems suspicious to one person may appear innocuous to another.

Definition: Suspicion

The courts have attempted to define suspicion in the following ways:

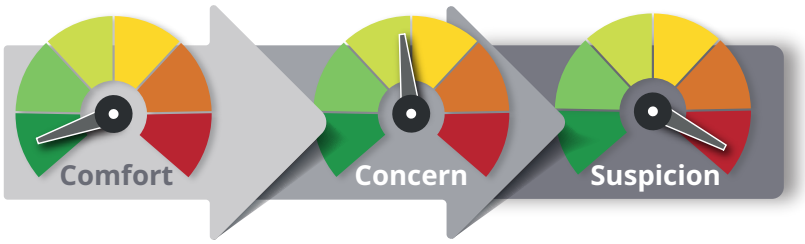
'A degree of satisfaction and not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not'; and

'Although the creation of suspicion requires a lesser factual basis than the creation of a belief, it must nonetheless be built upon some foundation'.[1]

Suspicion falls short of proof based on firm evidence but it seems clear that there must be a factual basis upon which it can be founded. Typically, the formulation of a suspicion is generally a gradual process – it rarely happens instantly or because of one event.

Businesses and professionals must remain vigilant and attentive to any unusual or suspicious activities, ensuring that their suspicions are based on observable facts and behaviours.

The formulation of suspicions generally follows the following pattern:



1. JMLSG, Prevention of money laundering/combating terrorist financing.

An event will happen within a normal client relationship which triggers a concern in the mind of an employee.

Once concerned the employee should:

i. analyse the available customer due diligence (CDD) and business information

ii. discuss concerns with colleagues and managers, and

iii. make discreet enquiries of clients – this is not 'tipping off', although client enquiries must be handled carefully.

Following this process there will either be a return to feeling comfortable with the client if concerns are allayed, or concerns will remain or shift to being suspicions.

If the employee remains concerned, then further enquiries should be made or the matter should be referred to a manager.

Important

Employees who develop suspicions of potential money laundering activities are required to promptly report their concerns to the money laundering reporting officer (MLRO). If the employee holds the position of MLRO within the entity, they must directly report their suspicions to the financial intelligence unit (FIU) without delay.

Question

What does it mean to have **reasonable grounds to suspect**? (sometimes referred to as the **objective test of suspicion**).

Think about

This test requires a prosecutor **to prove not** that a person **actually suspected** that property had derived from crime (i.e., a subjective test of suspicion) but that a person ***should*** **have suspected**, taking into account all the relevant information (the objective test of suspicion).

Offences of money laundering in the UAE

In the UAE, money laundering offences are outlined in the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations.
(source: www.moec.gov.ae/en/federal-decree-law-no-20-of-2018-on-anti-money-laundering-and-combating-the-financing-of-terrorism-and-illegal-organisations)

Article (2) of the Law outlines:

1. *Any person, having the knowledge that the funds are the proceeds of a felony or a misdemeanour, and who wilfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:*
    - a- *Transferring or converting proceeds or conducting any transaction with the aim of concealing or disguising their Illegal source.*
    - b- *Concealing or disguising the true nature, source or location of the proceeds, or the method involving the disposition, movement or ownership of the Proceeds or rights related thereto.*
    - c- *Acquiring, possessing or using proceeds upon receipt.*
    - d- *Assisting the perpetrator of the predicate offense to escape punishment.*
2. *The crime of Money Laundering is considered as an independent crime. The punishment of the perpetrator for the predicate offence shall not prevent his punishment for the crime of Money Laundering.*
3. *Proving the illicit source of the proceeds should not constitute a prerequisite to sentencing the perpetrator of the predicate offence.*

Why is money laundered?

The primary objective of the money launderer is to enjoy the benefits of their crimes. While some of the proceeds will be used to maintain the criminal activity or organisation and to finance more criminal activity, the ultimate aim is, of course, **profit**.

Consider

When examining the vulnerabilities of different products and services, it is essential that AML staff bear in mind the overriding objective of the money laundering process – namely, to disguise the source of property so that it cannot be linked to the original crime, what is known as the 'predicate' offence, and to conceal the dirty money as clean money to integrate it into the financial system.

In order to fulfil this primary objective, a launderer may first seek to achieve a number of secondary laundering objectives including:

- concealing the fact that they own the property
- concealing the fact that they may manage and control the property
- placing as much distance as possible between themselves and the property, both physically and 'on paper', and
- concealing the fact that the property is derived from criminal activity.

At the same time, however, the launderer will want to retain an element of control over the assets.

Note

In many cases the 'property' that results from a crime can prove to be very useful evidence in the prosecution of a criminal for the predicate (original) criminal offence which generated it. If it can be shown that the criminal owns the property, the prosecution's job is made easier.

Definition

In the UAE, a predicate offence is defined as:

'any act constituting an offence or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries.'

For example, fraud could be a predicate offence to money laundering if a monetary benefit was obtained from the fraud.

Law enforcement agencies across the world are more frequently investigating those suspected of criminality by examining their source of wealth – in other words, they try to discover how someone accumulated their total wealth (assets or money, for example) in the first place (for example, through inheritance, business ownership, investment income). It is interesting to note that such inquiries are similar to those carried out by staff within the regulated sectors, e.g., banks at account opening. The above money laundering process, if carried out effectively, breaks the 'reverse' link to predicate crimes and frustrates such investigations.

Think about

The key money laundering objectives are:

i. to disguise the source of criminal property

ii. to conceal/distance ownership of criminal property while avoiding detection for underlying crimes, and

iii. to control and therefore benefit from the proceeds of crime securely.

How is money laundered?

Having identified in broad terms what money laundering is, you must also understand the money laundering process itself, in its broadest sense. A whole range of professionals are usually required to assist in the laundering of the proceeds of crime. These professionals may include:

- bankers and other types of financial institutions
- trustees
- lawyers
- accountants
- brokers
- corporate service providers (CSPs)
- real estate agents/professionals, and
- dealers in precious metals and stones (DPMS).

Some professionals knowingly offer laundering assistance, whilst others provide their services without due regard for what they may be facilitating.

Note

The majority of professionals who help in the money laundering process do so inadvertently.

Money laundering may take a variety of forms. It's important to recognise that money laundering covers the proceeds of crime in all its various guises. The proceeds may be in the form of cash, but this cash could be paid into a bank account and its nature converted into funds held on account. Equally, it could be exchanged for high-value goods including, but not limited to, precious stones, luxury watches and/or jewellery, precious metals, gold bars, and high-value motor vehicles and real estate which then themselves become the proceeds of crime. When it comes to money laundering, there are an almost infinite number of methods using a range of financial services and products. Even so, it is commonly accepted that the money laundering process comprises three main stages of which you may have probably heard.

- **Placement:** where cash from criminal activity is placed into the financial system
- **Layering:** which usually involves a series of transactions designed to hide the source and ownership of the funds and confuse the authorities
- **Integration:** where laundered funds are reintroduced into the legitimate economy, appearing to have come from a legitimate source

We will now look at each of these three traditional stages in more detail.

Placement

Those involved in organised crime, such as drug trafficking, illegal gambling and prostitution, often acquire large amounts of money in the form of cash, usually in small denomination bank notes. Those wishing to finance terrorism might also wish to do so with cash, and terrorist organisations themselves are often in possession of large sums of cash.

When criminals are in physical possession of cash that can directly link them to underlying criminal activity, they are at their most vulnerable, particularly as the cash may be contaminated with drugs, security dye or 'smart water'. They need to get the cash into the financial system, in order to commence the laundering process of making their ill-gotten gains appear to be clean.

Example 1

DNFBPs can be used in the placement stage of money laundering through various methods, one of which is through real estate transactions.

For example, a money launderer may approach a real estate agent (a type of DNFBP) to purchase a high-value property. The money launderer pays the agent in cash, which is the illicit funds they want to launder. This cash is then deposited into the agent's trust account.

The real estate agent, either knowingly or unknowingly, becomes a part of the money laundering scheme by accepting large cash payments and depositing them into their business account. This activity places the illicit funds into the financial system, which is the first stage of money laundering, known as the 'placement' stage.

The launderer then sells the property, and the funds received from the sale appear to be legitimate earnings from a real estate transaction, thus successfully laundering the illicit funds. This is a basic example, and actual money laundering schemes can be much more complex and involve multiple DNFBPs and transactions.

Example 2

Saeed, a drug trafficker, has accumulated a large amount of cash from his illegal activities. He needs to launder this money to make it appear legitimate and hide its criminal origins. He decides to use a precious metals and stones dealer for this purpose.

Saeed visits a dealer and buys a large quantity of diamonds and gold using his illegal cash. The dealer, either knowingly or unknowingly, does not report this suspicious large cash transaction to the authorities.

Saeed now has a significant amount of precious metals and stones which are easier to transport, store and sell than large amounts of cash. The transaction is also hard

to trace since precious metals and stones do not have serial numbers like banknotes.

This is the placement stage of the money laundering cycle, where the 'dirty' money is first introduced into the financial system. Through the purchase of precious metals and stones, Saeed has effectively converted his illicit cash into assets that can later be sold to generate 'clean' money.

Example 3

An individual involved in illicit activities has accumulated a large amount of cash and needs to launder it to disguise its illegal origins. To do this, they approach a corrupt or unwitting accountant.

The individual asks the accountant to create a shell company, which exists only on paper and which has no real business operations or assets. The individual then deposits their illicit funds into the bank account of this shell company.

The accountant, using their knowledge and skills, helps the individual create false invoices and financial statements to make it seem as if the shell company is engaged in legitimate business transactions, thus justifying the funds deposited into its account.

This is the placement stage of the money laundering cycle, where the 'dirty' money is introduced into the financial system. By using a shell company and an accountant to create the illusion of legitimate business activity, the individual is able to convert their illicit cash into seemingly legitimate funds.

Example 4

A criminal owns a significant amount of illegally obtained money. To launder this money, he decides to use a company service provider, XYZ Services.

1. The criminal creates a shell company through XYZ Services, which offers services like forming corporations or LLCs, providing a registered office or agent, and other related services.
2. The criminal then appoints a nominee director and shareholders provided by XYZ Services to hide his association with the shell company.

3. Now, the criminal deposits his illegal money into the bank account of the shell company. This is the placement stage of money laundering – the process of introducing 'dirty' money into the financial system.
4. Since the shell company appears to be a legitimate business, the bank accepts the deposit without suspicion.
5. The criminal can now use the funds in the shell company's bank account to carry out legal transactions, thereby disguising the illegal origins of the money.

Key learning point

The most obvious way to place the proceeds of crime into the financial system is simply to deposit the cash into a bank account – or through buying assets with cash, selling those assets and depositing the funds in a bank account.

In well-regulated jurisdictions with modern AML legislation in place, this activity is now quite rare (there are, however, always a few less scrupulous people around who will still take 'dirty' cash into the system). In most countries around the world, all cash transactions over a determined figure (e.g., $10,000 in the US, £10,000 in the UK, €10,000 in European countries and similar/equivalent amounts in other countries), and for DNFBPs in the UAE AED55,000 or above, including deposits and withdrawals, **must** be reported by financial services providers to the regulatory authorities.

Important note: over time, more innovative and less obvious methods of placing cash into the financial system have been developed.

Money launderers are often creative in placing their ill-gotten gains into the financial system. One favoured method of theirs is the division of large amounts of cash into a number of small transaction amounts, each below the reporting threshold of, say, AED55,000. This is sometimes referred to as 'smurfing', or 'structured deposits'. This is followed by:

- making several **deposits** into single or multiple accounts on **successive days**

- making deposits into a number of accounts opened using false identities at **different branches of the same bank**
- using **different banks** and then **consolidating** the accounts
- depositing cash into accounts of third parties such as lawyers, real estate agents and brokers
- depositing cash with **the help of corrupt staff** who themselves manipulate the deposits to make them appear as if they are below the reporting threshold, and
- buying assets (e.g., real estate) in cash, selling those assets, and depositing the profit into a bank account.

The aim is to avoid detection of larger transactions by any monitoring systems and thresholds set by the bank.

Example: Real estate agents

Criminals often target real estate companies to buy properties with illicitly acquired funds. They may employ 'smurfs' to secure a short-term mortgage and then launder these ill-gotten funds through monthly payments. Furthermore, real estate is appealing to foreign investors who want to invest unlawfully obtained money into overseas properties. This adds an extra layer of complexity for law enforcement agencies in tracking fund transfers and identifying the individuals involved in these illegal operations.

Use of monetary instruments

Launderers have traditionally been known to use monetary instruments such as:

- money orders and bank drafts
- postal orders
- stored value cards (also known as prepaid or gift cards), and
- traveller's cheques.

More recently, launderers have turned to using online payment systems, mobile phone banking, prepaid cards

and virtual currencies to support their activity with a view to distancing themselves from face-to-face interactions with bank staff and adding complexity to the transactions in an effort to blur the trail.

In these cases, because of the relatively small amounts of cash involved in each deposit, warning signals are not raised. This converts the 'dirty' cash into an apparently low-risk item of relatively low value which can then be deposited elsewhere.

Intermingling, or co-mingling

Money launderers often try to conceal criminally derived cash by mixing it with legitimately generated cash.

They do this by using the services of legitimate business enterprises. The genuine cash takings of the businesses may have the 'dirty' cash added to them before they are deposited into the financial system, thereby disguising them as part of the genuine turnover/income of the business.

Key learning point

Businesses which generate large quantities of cash, such as retail outlets, tanning salons, nail and beauty bars, restaurants and bureaux de change, are popular for this type of activity.

Examples

Certain television series, such as the award-winning *Breaking Bad*, and more recently *Ozark*, are among the most-watched cable shows on US television and have raised awareness of the potential money laundering opportunities of cash-based businesses. In these instances, the use of a car wash company (*Breaking Bad*) or a lake-side bar/restaurant business and a strip club (*Ozark*), among others, were the 'front' companies.

Such businesses are able to absorb additional amounts of extra cash without arousing the suspicions of bankers or auditors. Generally, the legitimate business owner takes a percentage of the money for the 'laundering' service they are providing. Often it is businesses that are in financial difficulty that are most vulnerable to approaches from criminals to undertake intermingling.

Alternatively, money launderers set up their own legitimate businesses just to provide this as a route into the system, but this is expensive to do, and it should not be forgotten that firms will be monitoring the business profile and the expected/actual account transaction activity.

A cheaper, although riskier, alternative is for a launderer to establish what is known as a 'shell company'.

Definition: Shell company

This is a company that is incorporated on paper, but which does not own any physical assets and does not trade.

Example

The launderer opens an account in the name of the shell company and deposits criminally derived cash into it, presenting the money as the profits of the trading that has been performed by the shell company.

Another type of structure you will probably be familiar with is an offshore company. The terms 'shell company' and 'offshore company' are often used interchangeably but there are some key differences. As noted above, shell companies often do not own any physical assets or trade and are usually established for questionable purposes. A shell company, meanwhile, might be incorporated in any country, including the same country in which the criminals operate – in other words, not necessarily offshore.

An offshore company is simply one that is incorporated in another jurisdiction; it may be a shell company, but not necessarily, and it may be perfectly legitimate. The term 'offshore company' is often associated with tax avoidance and tax evasion. The well-documented *Panama*, *Paradise* and *Pandora Papers* leaks have raised public awareness of the use of offshore companies, in particular their use for questionable purposes by politically exposed persons (PEPs) and other wealthy individuals wishing to avoid scrutiny of their assets, and potentially avoid paying taxes.

It should be made clear that just because an individual and/or company has appeared in such leaks, it does not automatically mean that they have undertaken illegal activity.

If you are dealing with an entity established either as a shell company or offshore, your best defence and protection is to make sure that you carry out effective CDD, understand who your customer is, what activity the business undertakes, the expected volumes of money, and whether these volumes make sense for the type and size of business.

Shell companies are today coming under much greater scrutiny, and many firms will not open accounts for businesses established as shell companies.

Asset purchases

Launderers may use the cash proceeds of their criminal activities to buy assets, rather than placing the cash directly into the banking system.

Virtually any asset will work for this purpose, but popular items include:

- real estate
- branded goods
- prepaid store cards
- gold and precious metals
- art
- motor cars
- antiques, and
- virtual assets.

These items can then be sold and converted back into 'clean' cash, and will appear legitimate. In the case of movables, they can be transported to other countries to be converted back into local currency that is then deposited into local bank accounts. This adds physical distance from the crime and confusion to the trail for investigators.

Example

In an attempt to stop this sort of activity, some businesses are formally regulated (this includes banks, of course, but also jewellers and casinos in some countries, for example) and must submit what is often known as a large cash transaction report to the authorities if they receive cash in excess of,

say AED55,000 for dealers in precious metals and stones, or real estate agents in the UAE. In some countries, even unregulated companies are subject to a similar reporting requirement that obliges all businesses to file a report with the authorities for all goods and services purchased with cash in excess of $10,000 (or other similar thresholds).

Layering

Once cash has been successfully placed into the financial system, launderers can use a very large number of transactions and transfers designed to disguise the paper trail and the source of the property. This process can be as simple or as complicated as the situation demands, ranging from the low-level use of friends' or family members' bank accounts, up to the creation of a complex web of offshore entities with associated accounts.

The main objective of the layering stage is to confuse and delay any criminal investigation and to place as much distance as possible between the source of their illegal gains and the present status of the money or assets, as well as distancing the people involved from each other.

Often, at a very early point in the layering process, funds are placed outside the country where the money was first deposited. This puts the money outside the reach of the local law enforcement agencies based in the country where the underlying crime was committed. Later, the launderer may use any financial service or product to try to form as many 'layers' as possible.

In many cases, even when the proceeds of a crime are initially generated in electronic form (such as the theft of funds from a bank account), criminals choose to withdraw the funds from a bank account in cash, transport it to another country, and pay it into another account in order to break an audit trail. Virtual currencies are also being used much more in recent years to move the funds and contribute to the 'confusion'.

Example 1

Suppose a money launderer, who has already successfully placed illicit funds into the financial system through a series of transactions, now approaches a law firm for the purchase of a business. The launderer instructs the law firm to set up multiple shell companies in various jurisdictions and to use these shell companies to purchase the business, using the already placed illicit funds.

The law firm, either knowingly or unknowingly, assists the launderer in creating a complex web of transactions between these shell companies, transferring funds back and forth, buying and selling parts of the business and other assets, and creating a complex trail of transactions that are difficult to trace back to their original illicit source.

Each transaction adds a layer of complexity and moves the illicit funds further away from their source, making it more difficult for authorities to trace the funds back to their origin. This is the 'layering' stage of money laundering. The launderer could then sell the business, making the funds appear as legitimate profits from a business sale.

Example 2

An individual involved in illegal activities has already introduced their illicit money into the financial system in the placement stage. Now, they need to further disguise the origin of the money in the layering stage.

The individual goes to a dealer in precious metals and stones and purchases a large quantity of gold and diamonds with the funds they have placed into the system. They then sell these assets to another dealer, or maybe even several dealers, and have the proceeds deposited into a different bank account.

They repeat this process multiple times, buying and selling precious metals and stones with different dealers and depositing the funds into various accounts. They may also use different currencies and conduct these

transactions in different countries to make the trail even harder to follow.

This is the layering stage of money laundering, where the individual creates a complex network of transactions to obscure the source of the funds. By buying and selling precious metals and stones with different dealers, they are creating layers of transactions that make it difficult for authorities to trace the money back to its illegal origins.

Example 3

Similarly to the previous example, a money launderer can use real estate as a part of the layering process.

The individual contacts a real estate agent and purchases a property using the laundered money. Once the transaction is completed, the property is officially under the individual's name or a shell company's name.

After a short while, the individual then sells the property. The money received from the sale is then deposited into a different bank account or invested in another property.

The individual repeats this process, buying and selling properties through different real estate agents, each time using different bank accounts for transactions. The constant movement of funds through these transactions creates layers that make it difficult for the authorities to trace the original source of the illicit money.

This is the layering stage of money laundering, where convoluted transactions are made to obscure the trail back to the original illegal activity. By using real estate transactions, the individual has created a complex network of transactions, making it challenging for authorities to trace back the money to its illegal origins.

Integration

Integration is the final stage of the process, when criminally derived property that has been placed and layered (and so 'cleaned') is returned to the legitimate economy. At this stage the funds appear to have come from a legitimate source, but it should be remembered that the property will technically still be the proceeds of crime.

Examples: Reintegration methods

Examples of reintegration methods include the following.

Loan agreements – here money can be transferred from other accounts, sometimes based overseas, controlled by the launderer and made to appear as if the overseas company is making a loan.

Sham transactions – these are payments made from accounts controlled by the launderer that are made to look like the proceeds of a transaction for goods or services that never existed. The company may appear in its correspondence to be distributing the proceeds of a real estate deal, or a royalty. Alternatively, the company may appear to be purchasing goods or services from the launderer, shown on sham invoices at inflated prices.

Inheritance – funds held in another country on behalf of the launderer can be transferred to their home country and be said to represent a gift or inheritance.

Redemption of life policy or similar investment – this method involves placing funds with an insurance company (such as a lump sum investment or single-premium annuity) and sometime later encashing the policy (or borrowing against it) so that a cheque from the insurance company is obtained, thereby appearing to be from a legitimate source.

Sale of assets – when an asset originally purchased with illegitimate funds – say a yacht – is sold to a legitimate buyer. The funds received will be authentic and legitimate (e.g., a cheque from the buyer). This is a good example where the financial institution which receives the cheque needs to go beyond the determination of the legality of the cheque or the sale and ask more about how the person originally acquired the asset in the first place.

Example 1

DNFBPs can be involved in the integration stage of money laundering. Let's use the example of a luxury car dealership or an art dealer.

After successfully placing and layering illicit funds through a series of complex transactions and corporate structures, a money launderer might approach a luxury

car dealership or an art dealer. They would use the laundered money, which now appears as legitimate funds, to purchase a luxury car or a piece of valuable art.

The car dealership or art dealer, either knowingly or unknowingly, participates in the money laundering scheme by accepting these funds as payment. The launderer now owns a high-value asset that they purchased with funds that appear to be legitimate.

If questioned, the launderer can claim that the luxury car or art piece was purchased with the profits of a legitimate business transaction or investment. The illicit funds have now been fully integrated into the legitimate economy, which is the final 'integration' stage of money laundering.

The launderer could later sell the luxury car or art piece, further legitimising the previously illicit funds. The funds are now difficult, if not impossible, to link back to their original illicit source.

Example 2

Company service providers can be involved in the integration stage of money laundering. Let's use the example of a shell company or a complex business structure.

After successfully placing and layering illicit funds through a series of complex transactions, a money launderer might approach a company service provider. They would use the laundered money, which now seems like legitimate funds, to invest in or buy assets through the shell company or complex business structure.

The company service provider, either knowingly or unknowingly, participates in the money laundering scheme by assisting in these transactions. The launderer now owns high-value assets or investments made with funds that appear to be legitimate.

If questioned, the launderer can claim that the assets or investments were purchased with the profits of a legitimate business transaction. The illicit funds have now been fully integrated into the legitimate economy, which is the final 'integration' stage of money laundering.

The launderer could later sell the assets or use the profits from the investments, further legitimising the previously illicit funds. The funds are now difficult, if not impossible, to link back to their original illicit source.

Example 3

Real estate agents can be involved in the integration stage of money laundering. Let's use the example of a property purchase or property investment.

After successfully placing and layering illicit funds through a series of complex transactions, a money launderer might approach a real estate agent. They would use the laundered money, which now appears as legitimate funds, to purchase property or make an investment in real estate.

The real estate agent, either knowingly or unknowingly, participates in the money laundering scheme by facilitating the property transaction. The launderer now owns a high-value property that was purchased with funds that appear to be legitimate.

If questioned, the launderer can claim that the property was purchased with the profits of a legitimate business transaction or investment. The illicit funds have now been fully integrated into the legitimate economy, which is the final 'integration' stage of money laundering.

The launderer could later sell the property or earn income from it (for example, by renting it out), further legitimising the previously illicit funds. The funds are now difficult, if not impossible, to link back to their original illicit source.

Limitations of the three-stage interpretation of money laundering

The three-stage model is a convenient way of describing money laundering activity, but it does not always reflect the reality and can be seen as a little simplistic.

Key learning point

Money laundering does not always occur in a manner that fits into the three-stage model.

The three-stage model of money laundering assumes that all crime generates cash, which is then deposited in some way into the financial system. This is not true. There are a number of crimes, including almost all financial crimes and frauds, which result directly in benefits that are already within the financial system. For crimes of this

type, placement is irrelevant. Additionally, the modern assessment of money laundering recognises that the majority of money laundering involves assets such as real estate, luxury goods and investments, which are abused and manipulated through weaknesses in our financial system.

Another common myth encouraged by the three-stage model is that money laundering is always a set process and that it is possible to identify when it is happening at each step of the way. This is untrue. The line between the 'layering' and 'integration' stages of the process can be virtually impossible to separate, and the way laundered funds are 're-integrated' into the system often involves the completion of further 'layers'.

Even in relationships where there is no obvious process by which money is received and then paid away, money laundering can still in fact be occurring. Consider the following example.

Example

Mr Sami is a dealer who, having received inside information, sells stock prematurely in order to avoid a loss. The benefit from his crime is the amount that represents the loss that is avoided.

Unless you **appreciate the limitations of the three-stage money laundering model** there is a **danger** that you will **fail to identify money laundering activity**, simply because **what you see may not fit with what you expect** money laundering to look like.

Important

It is crucial that you keep an open mind about the types of client and relationship that pose the risk of money laundering.

The reality is that it is **not necessary to actively manage** the entire laundering process, or any particular stage of it, **in order to commit a money laundering offence**. All that is required is a **contribution to the process by dealing in some way** with another person's benefit from crime, however innocent this activity was.

What crimes generate property that can be laundered?

Many crimes generate property that can be laundered, but the criminal offence of money laundering generally only occurs when a person handles property that has been generated by certain types of crime. It is also worth noting that money laundering itself is a crime whether it is connected to the predicate offences or not.

The underlying crimes are often referred to as 'predicate offences'. The list of predicate offences differs from one country to another – for example, in most countries now, tax evasion is on the list, but it is not necessarily so in all countries. This is important, especially when the laundering takes place in several countries. As mentioned previously, in the UAE a predicate offence is 'any act constituting an offence or misdemeanour under the applicable laws of the State whether this act is committed inside or outside the State when such act is punishable in both countries'. When trying to prosecute a case, it is necessary to prove a crime was committed in the countries in question. Some countries define predicate offences by the type of criminality and its punishment (for example 'any criminal offence punishable by a sentence of more than 12 months' imprisonment'), while others might specifically list the offences themselves (e.g., drug trafficking, fraud, tax evasion, bribery, etc.). The issue becomes complex, as mentioned above, when several countries are involved in the process.

Different jurisdictions have different tests of underlying criminality for money laundering purposes. The tests can be:

i. '**single criminality**', which looks solely at the underlying conduct with reference to the law of the jurisdiction where the money laundering occurs, and

ii. '**dual criminality**', which requires the underlying conduct to be unlawful both in the country where the original crime takes place and with reference to the laws of the jurisdiction in which the money laundering takes place.

The types and seriousness of unlawful predicate acts that must be considered in a jurisdiction can also differ according to the minimum level of punishment applied in that jurisdiction.

FATF has outlined 21 predicate offence examples:

1. terrorism, including terrorist financing
2. illicit arms trafficking
3. participation in an organised criminal group and racketeering
4. trafficking in human beings and migrant smuggling
5. sexual exploitation, including sexual exploitation of children
6. tax crimes (related to direct taxes and indirect taxes)
7. illicit trafficking in stolen and other goods
8. corruption and bribery
9. forgery
10. counterfeiting currency
11. insider trading and market manipulation
12. environmental crime
13. murder, grievous bodily injury
14. kidnapping, illegal restraint and hostage-taking
15. robbery or theft
16. smuggling; (including in relation to customs and excise duties and taxes)
17. illicit trafficking in narcotic drugs and psychotropic substances
18. extortion
19. fraud
20. piracy
21. counterfeiting and piracy of products

The level of inclusiveness of different types of unlawful predicate acts can also vary depending upon the exclusion of specific types of criminal conduct.

Search

A useful source of information on this point, along with most other AML/CFT subject areas, is FATF's 'Mutual Evaluation Report' for your jurisdiction, which can be found at www.fatf-gafi.org/countries/

It is important for you to understand that you should report any knowledge or suspicion of criminality that comes to you during the course of your trade, profession or your employment of another person, to your MLRO.

Important

It is the responsibility of the MLRO/nominated officer to decide whether your knowledge or suspicion relates to a crime that will need to be reported to the authorities under the laws of your jurisdiction.

Even if what you have reported to your MLRO is not something that needs to be reported to the authorities, it will be valuable in helping your organisation to manage the risk of doing business with that particular client, taking into consideration to not tip off the client. We will discuss tipping off in more detail as we progress.

What forms of property can be laundered?

There is a common misconception that the only form of property that can be laundered is cash. The term 'money laundering' encourages this view. In fact, **any form of property can be laundered**.

The nature of property resulting from a crime can change. It may start as money in a bank account and then turn into, for example, units in an investment fund, property settled into a trust, virtual assets such as non-fungible tokens (NFTs) or cryptocurrencies, or a yacht.

The legal definition of property can be very wide. It may include all forms of property such as:

- **real** (e.g., land) or personal (cars, jewellery),
- **things in action** (contractual rights)
- **other intangible property** (intellectual property rights such as trademark ownership)

When we talk about money laundering, we are not simply talking about money in the form of cash or deposits in bank accounts; we are concerned about the laundering of criminally derived property in whatever form that property may be.

Terrorist financing

Definition: Terrorist financing

The provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organisations or to commit acts of terrorism.

Traditionally, AML efforts have concentrated on identifying the proceeds of different forms of underlying criminal conduct. Terrorist financing is another type of criminal activity which involves money and is a very serious threat to financial services businesses and DNFBPs.

To better understand terrorist financing, it is useful to compare it to money laundering to reveal some of their shared features, but also key differences.

Simplistically, the similarities and differences are often categorised according to:

i. the source of funds,

ii. the destination of the funds, and

iii. the purpose of the activity.

Let's look at each in more detail.

i. Source

With money laundering, there has to have been an original crime which generated the money – e.g., a drug deal, tax evasion, human trafficking, a bribe or a fraud, etc. With terrorist financing, although illegally earned money is often used, it does not have to be the case. The source of the funds may be legitimate – someone may wish to send their legally earned money from their salary to a terrorist organisation. The money was legitimately earned; it is the funding that is illegal.

ii. Destination of the funds

With money laundering, the money generated from the illegal activities serves to profit the people involved in the activity itself. In this sense, money laundering is often said to be 'circular', although this is slightly misleading as the funds also end up with perfectly legitimate recipients who may have no idea of the illegal origin of the funds – for example if you bought a car with drug money. With terrorist financing, the recipient is, by definition,

a terrorist or a terrorist organisation. Consequently, terrorist financing is said to be 'linear' – i.e., it is sent by one person (who is not necessarily involved in terrorism), to a terrorist or a terrorist organisation.

iii. Purpose of the activity

While criminals will use illegally earned money to fund more illegal activity, generally, the main purpose is to generate profit.

The aim of terrorist financing, again, by definition, is to support terrorists and terrorist organisations and fund their activities, purchase weapons and so on.

Examples

Below are examples of similarities and differences between money laundering and terrorist financing, including some of the methods used.

- Even in cases where the benefit of underlying criminality is being laundered, the laundered proceeds will eventually go to fund future or prospective criminal acts.
- The destination of money used to support terrorism has to be disguised, in the same way that the source of laundered funds must also be disguised. The same methods may be used for both.
- Even where the source of funding for terrorist activity is lawful, terrorists will nevertheless attempt to disguise it in order to preserve future funding. A classic example is the collection of charity donations for an organisation supporting terrorism.
- Both money laundering and terrorist financing require the assistance of the financial sector.
- Terrorist groups have shown a willingness to use emerging technologies and complex structures to fund attacks. The attacks in Mumbai in 2008 utilised VOIP (Voice Over-Internet Protocol), prepaid or value-stored cards and pre-loaded mobile phones to provide funds and information to assist the logistics of the attacks. Terrorists in the Gaza Strip

have used virtual currencies to fund operations.[2]

- Several high-profile attacks, including the Bali Bombings, bypassed the financial system entirely, using cash smugglers to courier funds across national borders to the terrorist cells.

Terrorist financing poses several unique difficulties to law enforcement and financial services firms in the above examples when the financial system is not even used, or when small sums of money are involved.

Case studies

Terrorist attacks, like the November 2015 Paris Attacks and the 2019 Sri Lanka Easter Attacks, have revealed that relatively small amounts of funds are required to perpetrate atrocities (the French government has indicated that the November 2015 bombings and mass shootings cost no more than $10,000). Other examples include simply using or renting a car and driving into crowds, or going on a shooting or stabbing rampage, at minimal cost.

Terrorist organisations vary in size, structure, operational reach and capabilities; examples of the largest being ISIS and Al-Qaeda. Despite differences among terrorist groups, as well as between individual terrorists and supporters, there is always a common need for financing to transform plots into terrorist acts.

In contrast to large terrorist organisations, small cells and individual terrorists face only minor financial needs since the cost of terrorist attacks is often minimal.

Consider

Electronic and online payments are emerging as a significant resource for terrorists; as with other criminal activities, the use of virtual currencies is also on the increase.

2. Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle and Julia Solomon-Strauss, Terrorist Use of Virtual Currencies: Containing the Potential Threat, Centre for a New American Security, 3 May 2017: www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies – accessed December 2021.

Question

Terrorist financing is often seen as money laundering in reverse.

Why? Because it is typically the case that terrorists collect money from perfectly legitimate sources (a charity used as a front for terrorist organisations, for instance) – clean money, which is then subsequently used for criminal purposes (e.g., financing the materials for a bomb).

Many of the techniques used to disguise the destination of terrorist funds are identical to those used to disguise the source of the proceeds of crime. The difficulty comes in protecting businesses against property that may have derived from a lawful source but that may be destined to fund future acts of terrorism. You must be alert to the possibility that property you handle may, at some future point in time, be used to fund an act of terror or terrorist organisation.

Terrorist financing offences

In the UAE, the offences of terrorist financing are outlined in the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations.

Article (3) of the Law outlines the following:

Without prejudice to the provisions of Federal Law No. (3) of 1987 referred to, and Federal Law No. (7) of 2014 referred to herein:

1- *Is guilty of the crime of financing terrorism whoever intentionally commits any of the following:*

a- Any of the acts specified in Clause (1) of Article (2) of the present Decree-Law, if he is aware that the proceeds are wholly or partly owned by a terrorist organisation or terrorist person or intended to finance a terrorist organisation, a terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin.

b- Providing, collecting, preparing or obtaining Proceeds or facilitating their obtainment by others with intent to use them, or while knowing that such proceeds will be used in whole or in part for the commitment of a terrorist offense, or if he has committed such acts on

behalf of a terrorist organisation or a terrorist person while aware of their true background or purpose.

2- *Is guilty of financing illegal organisations crime whoever intentionally commits any of the following:*

a- Any of the acts specified in Clause (1) of Article (2) of this Decree-Law, if he is aware that the proceeds are wholly or partly owned by an illegal organisation or by any person belonging to an illegal organisation or intended to finance such illegal organisation or any person belonging to it, even if without the intention to conceal or disguise their illicit origin.

b- Providing, collecting, preparing, obtaining Proceeds or facilitating their obtainment by others with intent to use such proceeds, or while knowing that such proceeds will be used in whole or in part for the benefit of an Illegal organisation or of any of its members, with knowledge of its true identity or purpose.

Proliferation financing

What is proliferation?

In international relations, the term 'proliferation' commonly refers to the illicit spread or possession of weapons of mass destruction (WMD). These include nuclear, chemical, radiological or biological weapons, and their related means of delivery, such as ballistic missiles.

Precise definitions of WMDs and proliferation vary from one jurisdiction to another, and sometimes within countries themselves.

Example

In the US alone, research in 2012 revealed that the US legal code contained five different definitions of WMDs; 21 US states had adopted their own definitions, and US government agencies had used at least 14 alternative definitions since the 1960s.

The UNRCPD defines WMDs in the following way:

Weapons of mass destruction (WMDs) constitute a class of weaponry with the potential to:

- *Produce in a single moment an enormous destructive effect capable to kill millions of civilians, jeopardize the*

natural environment, and fundamentally alter the lives of future generations through their catastrophic effects;

- *Cause death or serious injury of people through toxic or poisonous chemicals;*
- *Disseminate disease-causing organisms or toxins to harm or kill humans, animals or plants;*
- *Deliver nuclear explosive devices, chemical, biological or toxin agents to use them for hostile purposes or in armed conflict.*

While the types of weapons noted above are almost universally considered to be WMDs, depending on the context, so too may other sensitive technologies – those related to selected cyber or space-based military capabilities, for example.

One of the most prominent proliferation risks relates to the nuclear weapon and ballistic missile programme of the Democratic People's Republic of Korea (DPRK, or North Korea). The country's programme is subject to United Nations Security Council (UNSC) sanctions. These include measures that are intended to directly constrain their WMD programmes (such as a prohibition on WMD-related and dual-use items, which could be used in support of WMD programmes), as well as more general measures that are intended to apply pressure to the country's leader to curtail their WMD programmes (such as a ban on luxury goods, or a travel ban on government officials).

Notwithstanding the UNSC's focus on the DPRK, other proliferation risks exist. Syria, for instance, is reported to have used chemical weapons, such as sarin, chlorine gas, and sulphur mustard, on multiple occasions.

What is proliferation financing?

Let's now establish a precise definition of proliferation financing.

Definition: FATF

FATF defines proliferation financing as:

... the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use

goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

Legal frameworks

In 2008, FATF's mandate was widened to add responsibility for countering proliferation financing to its existing remit relating to money laundering and terrorist financing. FATF Recommendation 7 requires countries implement targeted financial sanctions to comply with UNSC Resolutions [UNSCRs] relating to WMD proliferation. FATF Recommendation 1 was amended in October 2020 to introduce a requirement for countries and financial institutions to identify, assess, understand and mitigate their proliferation financing risk. FATF also assesses countries' effectiveness in countering proliferation financing during its periodic Mutual Evaluation Reports, with Immediate Outcome 11 being 'persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs'.

In the UAE

In the UAE, as per Cabinet Decision 74, 'all current and future UN Security Council resolutions relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, including but not limited to Resolutions 1267 (1999), 1988 (2011), 1989 (2011), 1718 (2006), 2231 (2015) and any successor resolutions.'

Here is an example of how proliferation financing can take place.

Example: DPRK

The activities of DPRK state-owned Foreign Trade Bank (FTB) highlights this risk. FTB, despite its designated status, has operated multiple cover branches in several jurisdictions and was the centrepiece of efforts to launder money through the United States (U.S.) financial system in order to acquire components for the DPRK's weapons programmes. FTB maintained correspondent bank accounts and representative offices abroad that created and staffed front companies to conduct transactions. In June 2020, U.S. authorities seized millions of dollars held in correspondent accounts in the

names of front companies that were ultimately controlled by FTB. The companies involved operated in Asia, Middle East, and Europe.

Source: FATF Draft Guidance on Proliferation Financing Risk (www.fatf-gafi.org/en/publications/fatfgeneral/documents/public-consultation-proliferation-financing-risk.html)

www.moec.gov.ae/en/financial-crimes-legislations

Economic consequences of ML, TF and PF

Money laundering, as well as terrorist financing and proliferation financing, can have a damaging effect on our financial sector and global economy.

The International Monetary Fund (IMF) provide a fantastic summary of why we should be concerned about money laundering:

These crimes can make countries less stable, which in turn, can weaken law and order, governance, regulatory effectiveness, foreign investments, and international capital flows.

Money laundering and terrorism financing activity in one country can have serious adverse effects across borders and even globally. Countries with weak or ineffective controls are especially attractive for money launderers and financiers of terrorism. These criminals seek to conceal their criminal activities by exploiting the complexity of the global financial system, the differences between national laws, and the speed at which money can cross borders.

Source: www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing

On a business level, there are many cases of enforcement actions and fines levied on financial institutions and DNFBPs for having inadequate AML programmes, CDD measures according to the risk profile of clients, training, and investigative tools and systems to monitor transactions and to identify and report suspicious activity.

Case studies

The following is a sample only and you will undoubtedly know of many more cases, as they occur fairly regularly.

1) In November 2023, Binance, operator of the world's largest cryptocurrency exchange, was fined $4 billion due to various violations including

breaches of the Bank Secrecy Act and failing to maintain an effective AML programme. (Select this link for source).

2) DNB Bank in Norway was fined 400 million Norwegian Kroner (approximately $45.5 million) in December 2021 (Select this link for source).

3) In July 2023, Crown Resorts was fined $450 million from the Australian Transaction Reports and Analysis Centre (AUSTRAC) for breaches of money laundering laws. (Select this link for source).

4) Goldman Sachs was fined by a variety of regulators in the UK, the US and Singapore, after settling charges for its involvement in the Malaysian 1MDB scandal. Offences related to 'serious lapses and deficiencies in its management supervisory, risk, compliance and anti-money laundering controls' and involvement in bribery. The fines, settlements and payments, including to the Malaysian government, add up to $2.9 billion.[3]

   Significant also in this case is an example of increased action taken against individuals in firms, as opposed to only fining the institutions themselves. In this case, two Goldman Sachs executives were charged for their roles in the scandal.

5) The MoE revealed fines worth around AED100 million were imposed on around 300 DNFBPs operating in the country's DNFBP sector in the year of 2023.

6) In Malta, Insignia, a firm branded as a 'luxury lifestyle management group' was fined €373,670 in November 2020 by Malta's Financial Intelligence Analysis Unit, over a number of AML compliance breaches. The company, which caters to high-net-worth and ultra-high-net-worth individuals, had failed to raise a suspicious account with the authorities, in particular, relating to a high-risk Russian client.[4]

3. Manesh Samtani, 'Goldman Resolves Remaining 1MDB Charges for $2.9bn', Regulation Asia, 23 October 2020: www.regulationasia.com/goldman-resolves-remaining-1mdb-charges-for-2-9bn/ – accessed December 2021.
4. FIAU Malta, Administrative Measure Publication Notice, 3 December 2020: fiaumalta.org/wp-content/uploads/2020/12/Publication-Notice-03.12.2020.pdf – accessed December 2021.

Whilst less common, there are other examples of personal liability.

In February 2020, it was reported that Wells Fargo's former Chief Executive John Stumpf was fined $17.5 million by the Office of the Comptroller of the Currency for his role in the scandal relating to opening accounts on behalf of customers who had not requested them. The bank itself has been fined over $3 billion since the saga first came to light in 2016, and repercussions and lawsuits are still ongoing.[5]

In December 2020, it was reported that Ralph Hamers, the former ING CEO, was personally prosecuted in a major money laundering case for which the Dutch bank has already paid a €775 million fine in a settlement agreement with the Public Prosecutor in 2018.[6]

The international standards related to ML/TF/PF

There are a number of international initiatives and bodies that help to shape the AML regulatory landscape. Here, we shall take a look through some of these.

United Nations Office on Drugs and Crime (UNODC)

The UNODC was set up by the United Nations in 1997 to implement the United Nations International Drug Control Programme (UNDCP) and the Crime Prevention and Criminal Justice Programme (CPCJP), both of which were established by Resolutions of the UN General Assembly in 1991. Until 1 October 2002 the UNODC was called the Office for Drug Control and Crime Prevention.

Its headquarters are in Vienna and it has 22 field offices as well as a representative office in New York. It is funded by voluntary contributions, mainly from governments, for 90% of its budget.

The UNODC's overall aims are to assist UN member states in the struggle against illicit drugs, crime and terrorism. It does this in three main ways:

5. Pete Williams, 'Wells Fargo to pay $3 billion over fake account scandal', NBC News, 21 February 2020: www.nbcnews.com/news/all/wells-fargo-pay-3-billion-over-fake-account-scandal-n1140541 – accessed December 2021.
6. NL Times, 'Former ING CEO personally prosecuted in major money laundering case', 9 December 2020: nltimes.nl/2020/12/09/former-ing-ceo-personally-prosecuted-major-money-laundering-case – accessed December 2021.

i. through research and analytical work

ii. by helping countries in implementing treaties and drafting domestic legislation, and

iii. by field-based or on-the-ground assistance, which includes training judicial officials.

The UNODC has a series of 'Global Programmes' and a terrorism branch, which carries out the above tasks within each area. The most relevant to this course is the **Global Programme Against Money Laundering** (GPML). The GPML helps member states to:

- introduce legislation against money laundering and to develop and maintain strategies to combat money laundering
- encourage AML policy development
- raise public awareness about money laundering, and
- coordinate joint AML initiatives by the UN with other international organisations.

Financial Action Task Force (FATF)

Recognised as the worldwide leading standard setter for AML and CFT, **FATF** is an inter-governmental body established in 1989 with the objective of setting standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related financial risks.

FATF is globally recognised for its **40 Recommendations** which provide a comprehensive framework of measures intended to help countries deter and detect money laundering, financing of terrorism and the proliferation of WMDs. Recommendations 22 and 23 relate directly to DNFBPs, whilst professionals in these sectors should also take careful consideration of Recommendations 4, 10 and 11. FATF currently comprises 39 member jurisdictions and nine **FATF-Style Regional Bodies** (FSRBs). It also has a number of associate members and groups around the world representing most major financial centres in all parts of the globe. Over 200 jurisdictions around the world have committed to the FATF Recommendations through the global network of FSRBs and FATF memberships.

Through mutual evaluations, FATF monitors the progress of its members in implementing necessary laws and measures, reviews money laundering and terrorist

financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. Working in collaboration with other international stakeholders, FATF identifies national-level vulnerabilities with the aim of protecting the international financial system from misuse.

As well as performing mutual evaluation visits to member countries to monitor compliance with the 40 Recommendations, FATF and the nine FSRBs perform research into the methods used by money launderers and terrorist financiers. The results of this activity cover a range of risks and involve research and input from law enforcement agencies, academics and a diverse range of industry sectors.

FATF has issued guidance on a wide range of topics, including but not limited to:

FATF Guidance for a Risk Based Approach for the Accountants

FATF Guidance on the Risk-Based Approach for Dealers in Precious Metals and Stones

FATF Guidance on the Risk-Based Approach for Trust and Company Service Providers (TCSPs)

FATF Guidance on the Risk-Based Approach for Casinos

Risk-based Approach Guidance for the Real Estate Sector
FATF/Egmont Trade-based Money Laundering: Trends and Developments Money laundering and terrorist financing through trade in diamonds

FATF Guidance on Counter Proliferation Financing – The implementation of Financial Provisions of Unites Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction

FATF Guidance on Digital ID

Guidance – Private Sector Information Sharing

Guidance for a Risk Based Approach for Legal Professionals

The Application of Group-Wide Programmes by Non-Financial Business and Professions

Guidance on Counter Proliferation Financing Risk Assessment and Mitigation

Guidance on Proliferation Financing Risk Assessment and Mitigation

Terrorist Financing Risk Assessment Guidance

Search

A list of all FATF publications can be found on the FAFT publications page at this link.

High-risk and other monitored jurisdictions

FATF identifies jurisdictions with weak measures to combat money laundering and terrorist financing in two FATF public documents that are issued three times a year.[7] These documents are:

i. *High-Risk Jurisdictions subject to a Call for Action* (known as the FATF black list), and

ii. *Jurisdictions under Increased Monitoring* (known as the FATF grey list)

Forthcoming assessments will cover not only how well the legislative structure of each jurisdiction meets the Recommendations but, and probably more importantly, how well these are being implemented in each jurisdiction.

MENAFATF

MENAFATF is a FATF-style regional body. Originally established through the governments of 14 countries, MENAFATF now consists of 21 members, who endeavour to achieve the following objectives:

- to adopt and implement the FATF 40 Recommendations on combating money laundering and financing of terrorism and proliferation;
- to implement the relevant UN treaties and agreements and UNSCRs;
- to co-operate among each other to raise compliance with these standards within the MENA region and to cooperate with other international and regional organizations, institutions and agencies to improve compliance worldwide;
- to work jointly to identify issues of regional nature related to money laundering and terrorist financing, and to share relevant experiences and to develop solutions for dealing with them; and

7. FATF, 'Topic: High-risk and other monitored jurisdictions': www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/) – accessed February 2024.

- to take measures throughout the region to effectively combat money laundering and terrorist financing in a way that does not contradict with the cultural values, constitutional frameworks and legal systems in the member countries.

The MENAFATF is voluntary and co-operative in nature and independent from any other international body or organisation; it was established by agreement between the governments of its members and is not based on an international treaty. It sets its own work, regulations, rules and procedures and co-operates with other international bodies, notably FATF, to achieve its objectives. (www.menafatf.org/about)

AML/CFT legislation and guidelines in the UAE

As noted, the primary AML/CFT legislation in the UAE is the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations. The Law was issued to 'develop the legislative and legal structure of the nation to ensure compliance with international standards on anti-money laundering and countering the financing of terrorism.'

The Law aims to:

1. combat money-laundering practices
2. establish a legal framework that supports the authorities concerned with AML and crimes related to money laundering, and
3. counter the financing of terrorist operations and suspicious organisations.

To achieve these aims, the Law details:

- the offences of money laundering and terrorist financing
- the punishments for committing these offences
- reporting requirements for financial institutions and non-financial businesses and professions
- the requirements for financial institutions and DNFBPs relating to identifying risks and applying a risk-based approach, conducting necessary due diligence,

the development of policies, controls and procedures, and maintaining records and documents, and

- the responsibility of the FIU.

We will look at each of these in more detail as we progress through this course, however, you can familiarise yourself with the Law now by selecting this link.

There are a number of laws, bylaws, decrees, and guidelines that professionals within DNFBPs need to familiarise themselves with in relation to AML and CFT. These include:

- Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (Select this link to read more).
- Federal Decree Law No (26) of 2021 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (Select this link to read more).
- Cabinet Decision No (10) of 2019 Concerning the Implementing Regulation of Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (Select this link to read more).
- Cabinet Decision No (24) of 2022 Amending some provision of Cabinet Resolution No (10) of 2019 On the Executive Regulations of Federal Decree Law No (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations
- Cabinet Decision No. 74/2020 Concerning the UAE List of Terrorists and the Implementation of UN Security Council Decisions Relating to Preventing and Countering Financing Terrorism and Leveraging Non-Proliferation of Weapons of Mass Destruction, and the Relevant Resolutions (Select this link to read more).
- Cabinet Decision No (109) of 2023 regarding regulating the procedures of the beneficial owner (Select this link to read more).
- Cabinet Decision No. 132/2023 On the Administrative Penalties to Be Imposed on the Violators of Cabinet Decision No. 109/2023 Concerning the Regulation of Beneficial Ownership Procedures Type (Select this link to read more).

- Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations: Guidelines for Designated Non-Financial Businesses and Professions (Select this link to read more).

We will explore and refer to these more as we progress through this course, but it is worth familiarising yourself with them now.

Self-assessment questions

Congratulations, you have reached the end of Unit 1. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, **continue** or alternatively, you can work through the section again if you wish.

1. What is the difference between money laundering and terrorist financing?
    a) Money laundering involves disguising the source of funds, while terrorist financing involves disguising the destination of funds
    b) Money laundering involves legal funds, while terrorist financing involves illegal funds
    c) Money laundering is a global issue, while terrorist financing is a national issue
    d) Money laundering involves large sums of money, while terrorist financing involves small sums of money
2. What role does the Financial Action Task Force (FATF) play in combating money laundering and terrorist financing?
    a) It sets global standards for anti money laundering and counter-terrorist financing policies
    b) It conducts investigations into money laundering and terrorist financing activities
    c) It imposes sanctions on countries that fail to implement anti money laundering and counter-terrorist financing measures
    d) It provides financial assistance to countries to help them implement anti money laundering and counter-terrorist financing measures
3. One of the traditional stages of money laundering is known as 'layering'. To what does this refer?
    a) Disguising the origin of initial deposits through multiple transfers (correct)
    b) Depositing of funds into multiple bank accounts.
    c) Purchasing of property with the proceeds of money laundering.
    d) Transferring money acquired illegally on behalf of others.

Correct answers 1a, 2a, 3a

Unit 2: Identifying and Assessing ML/TF/PF Risks

Learning Objectives

The purpose of this learning material is to:

- share money laundering and terrorist financing and proliferation risks for DNFPBs
- explore self-risk assessments, including identifying and assessing risks
- determine how to apply a risk-based approach, and
- explore emerging technologies and new payment methods.

Understanding risks

Now that you fully appreciate what money laundering and terrorist financing are, you can see the size of the problem and the threat they pose to the financial services industry and DNFPBs.

A study by the UNODC suggests that the total annual amount of money laundered globally is equivalent to anything from 2 to 5% of global GDP, or $800 billion to $2 trillion, of which illicit drugs account for a fifth of all crime proceeds; human trafficking, illegal trade, bribery and many other crimes are included in this figure. However, because of the obviously clandestine nature of money laundering, it is difficult to obtain an accurate figure. Suffice it to say, it is a massive problem, let alone the actual underlying crimes which generated the proceeds in the first place. The UNODC also observed that less than 1% of global illicit financial flows are currently seized and frozen.[8]

A wide range of products and services are offered by both the financial services industry and DNFPBs, all designed in different ways to attract, manage, protect, preserve or enhance property that belongs to other people.

As we have seen, if that property derives from crime, then the provision of the service or product may constitute

8. UNODC, *The Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism 2011 to 2017*: www.unodc.org/documents/evaluation/indepth-evaluations/2017/GLOU40_GPML_Mid-Term_In-Depth_Evaluation_Final_Report_October_2017.pdf – accessed December 2021.

an act of money laundering and, if it is done by a person knowing or suspecting or having reasonable grounds to suspect criminality, the offence of money laundering will usually be committed.

Key learning point

Every DNFBP is at risk of being exposed to property derived from crime or terrorism.

DNFBPs include a wide range of sectors, each of which pose their own set of risks. These sectors are at risk to money laundering and terrorist financing activities as a result of the typically large nature of transactions, and the amount of money involved. They are often exploited as a means of layering illicit funds or as a method of integrating these funds into the legitimate economy. A self-risk assessment (SRA) of DNFBPs in the UAE has identified some specific details and threats relating to each of the different sectors, which we will take a look at shortly – before we do, let's gain a better understanding of national/self-risk assessments, entity wide risk assessments, and customer risk assessments

National risk assessments (NRAs)

A national risk assessment is a comprehensive evaluation carried out by a country to identify, analyse, and understand potential threats and vulnerabilities it faces from money laundering, terrorism financing and proliferation financing. The assessment is used to develop strategies and policies to mitigate these risks, prioritise resources, and enhance the country's resilience. It includes a systematic process of gathering and analysing information, evaluating potential impacts, and providing recommendations for action. It is an essential part of national security and emergency planning.

Sectoral risk assessment (SRA)

The sectoral risk assessment is another tool that countries use to reach a more detailed understanding of the identified risks in a particular sector/subject; this assessment is usually done by the competent authorities and can include more factors/sub-sectors than a national risk assessment to build a detailed understanding of the related risks.

Entity wide risk-assessment

An entity-wide risk assessment is a systematic examination carried out by an entity to identify, evaluate, and manage all potential money laundering and terrorist financing risks that could impact its operations, objectives or value. The assessment helps in formulating risk management strategies, prioritising resources, and enhancing the organisation's resilience. It involves collecting and analysing data, evaluating potential impacts, and recommending appropriate measures. It forms a crucial part of corporate governance and strategic planning, ensuring the organisation's sustainability and success in a volatile business environment. However, this assessment needs to be in line with the finding of the national/sectoral risk assessment.

Customer risk assessment (CRA)

An AML customer risk assessment is a vital process carried out by firms to evaluate the potential risks associated with their customers. It involves identifying, assessing, and understanding the potential money laundering or terrorist financing risks a customer may pose. It includes considerations like the customer's occupation, geographical location, transaction patterns, and the nature of the customer relationship. The assessment helps in implementing effective AML controls, tailoring CDD measures, and complying with regulatory requirements. It is a critical component of an institution's AML programme, designed to safeguard the institution from being misused for illicit activities. We will look into the customer risk assessment process later in this course.

The outcome of your CRA, which could be descriptive (i.e., High, Medium and Low) or numerical (i.e., 1 to 10), will determine the level of CDD you must perform and the frequency of reviews that you must undertake in relation to that customer. For example, where a customer poses higher risk and is rated high risk from a money laundering or terrorist financing perspective, you will be required to conduct enhanced CDD.

Self-risk assessment – Identifying, assessing the risks

AML self-risk assessments are a crucial part of a firm's AML/CFT/proliferation financing compliance programme. They involve the systematic identification and evaluation of the risks that the firm might face in terms of money laundering and terrorist financing.

The purpose of an AML self-risk assessment is to enable a firm to understand its unique risk exposure and design effective AML/CFT/proliferation financing policies and procedures accordingly. It is a proactive approach that helps in understanding the potential risks and vulnerabilities, and to devise strategies to mitigate those risks.

This risk-based approach is a key principle of many global AML standards, including those established by FATF.

In conducting an AML/CFT/proliferation financing self-risk assessment, a firm should identify, assess and understand the inherent money laundering and terrorist financing risks (i.e., the risks to which a DNFBP is exposed if there were no control measures in place to mitigate them) across all business lines and processes. Several risk factors should be considered during this process; let's take a look at each of these.

As per FATF, DNFBPs should:
Money laundering/terrorist financing risk assessment (Recommendation 1. Criteria 10)

- take appropriate steps to identify, assess, and understand their ML/TF risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels)[9]. This includes being required to:

  (a) document their risk assessments;

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

  (c) keep these assessments up to date; and

9. The nature and extent of any assessment of ML/TF risks should be appropriate to the nature and size of the business. Competent authorities or SRBs may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood, and that individual financial institutions and DNFBPs understand their ML/TF risks

(d) have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs.

Money laundering/terrorist financing risk mitigation (Recommendation 1. Criteria 11)

- should:

(a) have policies, controls and procedures, which are approved by senior management, to enable them to manage and mitigate the risks that have been identified (either by the country or by the financial institution or DNFBP);

(b) monitor the implementation of those controls and to enhance them if necessary; and

(c) take enhanced measures to manage and mitigate the risks where higher risks are identified.

Proliferation financing risk assessment and mitigation (Recommendation 1. Criteria 13)

(a) identify and assess, their proliferation financing risks[10]. This includes being required to:

(i) document their proliferation financing risk assessments;

(ii) keep these assessments up to date; and

(iii) have appropriate mechanisms to provide proliferation financing risk assessment information to competent authorities and SRBs;

(b) have policies, controls and procedures, which are approved by senior management and consistent with national requirements and guidance from competent authorities and SRBs, to enable them to manage and mitigate the proliferation financing risks that have been identified (either by the country or by the financial institution or DNFBP);

(c) monitor the implementation of those controls and to enhance them if necessary;

(d) take commensurate measures to manage and mitigate the risks where higher proliferation financing risks are identified, (i.e., introducing

10 Financial institutions and DNFBPs processes to identify, assess, monitor, manage and mitigate PF risks may be done within the framework of their existing targeted financial sanctions and/or compliance programmes

enhanced controls aimed at detecting possible breaches, non-implementation or evasion of targeted financial sanctions under Recommendation 7); and

(e) where the proliferation financing risks are lower, ensure that measures to manage and mitigate the risks are commensurate with the level of risk, while still ensuring full implementation of the targeted financial sanctions as required by Recommendation 7.

When must a CRA be completed?

- Prior to establishing a business relationship with a customer, and at regular intervals throughout the business relationship, depending on the risk rating of your customer.
- Whenever there is a change in the customer's circumstances or the nature of the business relationship. For example, change in ownership, nature of the products or services being offered, or transaction patterns (i.e., unusually complex transaction).
- Whenever the NRA or the SRA has been updated and raised a new concern about a certain type of activities, channels, ... that could affect the used risk factors.

Moreover, Article (16) of the Feder Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations details requirements for financial institutions and DNFBPs regarding identifying and assessing money laundering and terrorist financing risks. Article (16) outlines that:

1- Financial institutions and designated nonfinancial businesses and professions shall:

a) Identify the crime risks within its scope of work as well as continuously assess, document, and update such assessment based on the various risk factors established in the Implementing Regulation of this Decree-Law and maintain a risk identification and assessment analysis with its supporting data to be provided to the Supervisory Authority upon request.

b) Take the necessary due diligence measures and procedures and define their scope, taking into account the various risk factors and the results of the national risk assessment and retain the

records received during the implementation of this process. The Implementing Regulation of the present Decree-Law shall specify the cases in which such procedures and measures are applied, and the conditions for deferring the completion of customer or real beneficiary identity verification.

c) *Refrain from opening or conducting any financial or commercial transaction under an anonymous or fictitious name or by pseudonym or number, and maintaining a relationship or providing any services to it.*

d) *Develop internal policies, controls and procedures approved by senior management to enable them to manage the risks identified and mitigate them, and to review and update them continuously, and apply this to all subsidiaries and affiliates in which they hold a majority stake; the Implementing Regulations of this Decree-Law shall specify what should be included in said policies, controls and procedures.*

e) *Prompt application of the directives when issued by the competent authorities in the state for implementing the decisions issued by the UN Security Council under Chapter (7) of UN Convention for the Prohibition and Suppression of the Financing of Terrorism and Proliferation of weapons of mass destruction, and other related directives.*

f) *Maintain all records, documents, and data for all transactions, whether local or international, and make this information available to the competent authorities promptly upon request, as stipulated in the Implementing Regulation of this Decree-Law.*

g) *Any other obligations stipulated in the Implementing Regulation of this Decree-Law.*

The main risk factors

Nature and scale of the business

The nature, scale, diversity and complexity of its business. Businesses that offer a wider range of products or services, or operate in multiple jurisdictions, may face a higher risk of being exploited for money laundering purposes. Firms should understand the risks that are deemed highest and lowest in the sector in which they operate.

Customer risk

This involves understanding the types of customers with which the firm deals, the level of transparency or beneficial ownership, and the regularity or duration of their business relationships. Certain types of customers, such as PEPs, may present a higher risk due to their position and the potential for corruption.

Geographical risk

The firm will assess its geographical risk, based on the locations where it does business. Certain jurisdictions may present a higher risk due to factors such as weak AML laws or high levels of corruption or organised crime.

Delivery channels

The firm will consider its product, service, transaction, and delivery channel risk. Certain products or services, transactions, or delivery channels may inherently pose a higher risk of money laundering. For example, products or services that involve high-value transactions, or that allow for anonymity, could be more susceptible to money laundering. For example, in the UAE, dealers in precious metals and stones have obligations to responsibly source gold as per the Due Diligence Regulations for Responsible Sourcing of Gold (Select this link). The Regulations aim to inform Regulated Entities of the measures to be adopted in relation to responsible sourcing of gold from Conflict-Affected and High-Risk Areas (CAHRAs) as part of their overall AML/CFT controls framework.

In the UAE, in accordance with Section 2 of the Cabinet Decision No (10) of 2019, DNFBPs are required to identify, assess and understand their crime risks in relation to their business nature and size, and comply with the following:

(a) Considering all the relevant risk factors such as customers, countries or geographic areas, and products, services, transactions and delivery channels, before determining the level of overall risk and the appropriate level of mitigation to be applied.

(b) Documenting risk assessment operations, keeping them up to date on on-going bases and making them available upon request.

To identify their risks, businesses should ask themselves some key questions.

- What are we, who are we and what do we do?
- What is our target market?
- Are we growing/diversifying or relatively static?
- How and where do we carry on our business activities?
- Are we a complex/diverse or simple business?
- Do we have multiple or single premises?
- Do we rely on any third party to process our business transactions or act on our behalf?
- Is our head office in another jurisdiction and, if so, is that jurisdiction assessed as 'high risk' for money laundering or terrorist financing?
- Do we have any branches or subsidiaries in other jurisdictions?

Using inherent risks as a foundation, the firm can establish the type and severity of risk mitigation controls to address these risks. The level of inherent money laundering and terrorist financing risks helps to form the types and quantities of AML/CFT resources and mitigation plans that DNFBPs need to implement. The assessment of inherent money laundering and terrorist financing risks and the effectiveness of risk reduction strategies will lead to a residual risk assessment – the remaining risks when effective control measures are in operation. If the residual risk exceeds the DNFBP's risk tolerance, further control measures will have to be implemented to ensure that the money laundering and terrorist financing risk level is acceptable to the DNFBP.

The results of the AML self-risk assessment should be documented and updated periodically, or when significant changes occur in the business. This will help the firm to remain informed about its risk exposure and ensure that its AML policies and procedures are up to date.

It is also important to note that an AML self-risk assessment is not a one-size-fits-all process. The assessment should be tailored to the specific circumstances of the organisation, considering factors such as its size, structure and business activities.

AML self-risk assessments are a cornerstone of effective AML compliance. By systematically identifying and assessing risk exposure, firms can ensure that they are well-prepared to prevent and detect money laundering and terrorist financing. The AML self-risk assessment is therefore not only a regulatory requirement, but also a crucial component of a firm's broader risk management strategy.

Reviewing and updating the self-risk assessment

DNFBPs should also update their money laundering and terrorist financing business risk assessment whenever they become aware of any internal or external events or developments which could affect their accuracy or effectiveness. Such developments may include, among other things, changes in business strategies or objectives, technological developments, legislative or regulatory developments, or the identification of material new money laundering and terrorist financing threats or risk factors. In this regard, DNFBPs should take into consideration the results of the most recent NRA or any sectoral risk assessment, as well as circulars, notifications and occasional published information from official sources, such as the supervisory authorities, other national competent authorities, or relevant international organisations, such as FATF, MENAFATF and other FSRBs, the Egmont Group, and others.

Reviewing and updating AML self-risk assessments is a continuous process that should be embedded within a firm's overall risk management strategy. To ensure that their assessments are up-to-date and reflect their current risk profile, firms should establish a regular review cycle. The frequency of these reviews may be determined by regulatory requirements such as laws and regulations updates/changes, or change in the national risk assessment, or to the firm's operational environment.

The review process typically involves reassessing the firm's inherent risks, which include customer, product, geographic, and delivery channel risks, among others. This should take into account any changes in the firm's business model, customer base, products or services, or operational locations.

Changes in the external environment should also be considered. For instance, the emergence of new money laundering techniques, changes in AML laws or regulations, or shifts in the political or economic climate of a country where the firm operates could all affect the firm's risk profile.

Moreover, the effectiveness of the firm's current AML controls should also be evaluated. This could involve testing the controls to ensure they are working as intended, reviewing internal or external audit findings, or analysing the firm's AML compliance data, such as the number of suspicious activity reports filed.

The results of the review should be documented and communicated to all relevant parties within the firm. This may include the firm's senior management, board of directors, AML compliance team and other employees.

Based on the review, the firm should update its AML policies, procedures, and controls as necessary to address any identified gaps or weaknesses. This could involve implementing new controls, enhancing existing ones or providing additional training to employees.

An NRA or SRA affects the institutional risk assessment by the weight they give to the risk factors that DNFBPs use if they have been determined as a risk area at a national level.

Applying a risk-based approach

Increasingly, regulators and international bodies such as FATF are promoting risk-based controls for AML. A risk-based approach means that firms ensure that their systems and controls are proportionate to their particular risks of money laundering.

It therefore has the benefit of allowing firms to be cost effective, proportionate and flexible in the way they manage their risks.

Think about

The risk-based approach requires DNFBPs to identify and assess money laundering risks and to take steps to mitigate and monitor those risks.

Organisations should be looking to apply simplified due diligence to lower-risk business, and ensure that they conduct enhanced due diligence for higher-risk categories of business.

The rationale for a risk-based approach is simple: firms have finite resources and those resources should be targeted at the higher-risk areas to ensure the maximum benefit.

The aim of the risk-based approach is to promote a move away from a 'one-size-fits-all' approach to AML procedures.

The use of a risk-based approach allows DNFBPs to allocate their resources more efficiently and effectively, within the scope of the national AML/CFT legislative and regulatory framework, by adopting and applying preventative measures that are targeted at and commensurate with the nature of risks they face. It is important to consider here how the majority of customers of DNFBPs are 'walk in customers', meaning transactions will be occasional or non-recurring, rather than regular and recurring transactions for customers with whom there is no ongoing account or business relationship. It is therefore essential that these types of customers and transactions are factored into the firms risk-based approach. Examples of such transactions include, but are not limited to:

- sale or purchase of goods such as precious stones, metals, coins or other valuable property to or from a customer
- accepting a deposit for a real-estate purchase from a prospective buyer, and
- drafting of a will, trust agreement, or other legal agreement for a walk-in customer.

In this circumstance, DNFBPs are required to identify the customer and verify the customer's identity as well as that of the beneficial owners, beneficiaries and controlling persons. Furthermore, DNFBPs are required to undertake appropriate risk-based CDD measures, which includes the determining the nature of the customer's business and the purpose for the transaction. We will discuss customer due diligence in more detail as we progress.

While there are limits to any risk-management approach, and no risk-based approach can be considered as completely failsafe, there may be occasions where a DNFBP has taken all reasonable measures to identify and mitigate

money laundering and terrorist financing risks, but it is still used for money laundering and terrorist financing in isolated instances. DNFBPs should nevertheless understand that a risk-based approach is not a justification for ignoring certain money laundering and terrorist financing risks, nor does it exempt them from taking reasonable and proportionate mitigation measures, even for risks that are assessed as low. Their statutory obligations require them to identify, assess and understand the level of (inherent) risks presented by their (types of) customers, products and services, transactions, geographic areas and delivery channels, and to be in a position to apply sufficient AML/CFT mitigation measures on a risk-appropriate basis at all times.

In response to these variations, a risk-based approach will enable senior managers of a firm to create their own approach to systems and controls in a less prescriptive manner. This approach will result in a more efficient set of procedures, focusing greater effort on higher-risk areas. A risk-based approach will inform every aspect of firms' AML systems and controls, but is of particular importance in respect of account opening procedures, CDD and monitoring.

From the following, select the relevant example relating to your industry.

Example case study: Applying a risk-based approach to AML for a luxury real estate agency

A luxury real estate agency based in the UAE, named xyzProperties, operates in several high-end markets around the world. Given the nature of their clientele and the high transaction values, xyzProperties is classified as a DNFBP and is therefore subject to AML regulations.

In order to comply with these regulations and to ensure it was not inadvertently facilitating illegal activities, xyzProperties must implement a risk-based approach to AML.

Firstly, the agency identifies and assesses the AML risks associated with their operations. This involves a detailed analysis of their client base, the countries they operate in, and the types of transactions they typically handle.

The agency finds that some of their operations in certain countries posed a higher risk due to the prevalence of corruption and financial crime.

Secondly, they implement strict CDD procedures to identify high-risk clients and adhere with the requirements outlined in Federal Decree-law No. (20) of 2018. This involves verifying the identity of all new clients and conducting ongoing monitoring of existing clients. High-risk clients, such as PEPs, are subject to enhanced due diligence.

Thirdly, xyzProperties develop an AML compliance programme tailored to the identified risks. This includes regular staff training on AML regulations and procedures, regular audits to ensure compliance, and the appointment of a dedicated MLRO.

Finally, the agency implements a robust reporting system to report any suspicious transactions to the relevant authorities. This system is designed to detect unusual or suspicious activity, such as unusually large transactions or transactions involving high-risk countries or individuals.

By implementing a risk-based approach to AML, xyzProperties is able to effectively manage its AML risks and ensure compliance with regulations. The agency also gains a better understanding of its clients and is able to protect its reputation by avoiding involvement in illegal activities.

This case study highlights the effectiveness of a risk-based approach to AML for DNFBPs. By identifying and assessing risks, implementing robust procedures, and maintaining ongoing monitoring and reporting, DNFBPs can effectively manage their AML obligations and protect their businesses from financial crime.

Example case study: Applying a risk-based approach to AML for dealers in precious metals and stones

A prominent dealer in precious metals and stones based in the UAE, named ABC Jewels, operates in high-end markets across the globe. Given the nature of their clientele and high transaction values, ABC Jewels is classified as a DNFBP and is therefore subject to AML regulations.

In order to comply with these regulations and to ensure it is not inadvertently facilitating illegal activities, ABC Jewels must implement a risk-based approach to AML.

Firstly, ABC Jewels identifies and assesses the AML risks associated with their operations. This involves a detailed analysis of their client base, the countries they operate in, and the types of transactions they typically handle. The dealer finds that some of their operations in certain countries posed a higher risk due to the prevalence of corruption and financial crime.

Secondly, they implement strict CDD procedures to identify high-risk clients and comply with the requirements outlined in Federal Decree-law No. (20) of 2018. This involves verifying the identity of all new clients and conducting ongoing monitoring of existing clients. High-risk clients, such as PEPs, are subject to enhanced due diligence EDD.

Thirdly, ABC Jewels develops an AML compliance programme tailored to the identified risks. This includes regular staff training on AML regulations and procedures, regular audits to ensure compliance, and the appointment of a dedicated MLRO.

Finally, the dealer implements a robust reporting system to report any suspicious transactions to the relevant authorities. This system is designed to detect unusual or suspicious activity, such as unusually large transactions or transactions involving high-risk countries or individuals.

By implementing a risk-based approach to AML, ABC Jewels is able to effectively manage its AML risks and ensure compliance with regulations. The dealer also gains a better understanding of its clients and can protect its reputation by avoiding involvement in illegal activities.

Example case study: Applying a Risk-Based Approach to AML for accountants

A prestigious accounting firm based in the UAE, named XYZ Accountants, operates in various high-end markets worldwide. Given the nature of their clientele and high transaction values, XYZ Accountants is classified as a DNFBP and is therefore subject to AML regulations.

To comply with these regulations and ensure it is not inadvertently facilitating illegal activities, XYZ Accountants must implement a risk-based approach to AML.

Firstly, XYZ Accountants identifies and assesses the AML risks associated with their operations. This involves a detailed analysis of their client base, the countries in which they operate, and the types of transactions they typically handle. The firm finds that some of their operations in certain countries pose a higher risk due to the prevalence of corruption and financial crime.

Secondly, they implement strict CDD procedures to identify high-risk clients and comply with the requirements outlined in Federal Decree-law No. (20) of 2018. This involves verifying the identity of all new clients and conducting ongoing monitoring of existing clients. High-risk clients, such as PEPs, are subject to enhanced due diligence.

Thirdly, XYZ Accountants develop an AML compliance programme tailored to the identified risks. This includes regular staff training on AML regulations and procedures, regular audits to ensure compliance, and the appointment of a dedicated MLRO.

Finally, the firm implements a robust reporting system to report any suspicious transactions to the relevant authorities. This system is designed to detect unusual or suspicious activity, such as unusually large transactions or transactions involving high-risk countries or individuals.

By implementing a risk-based approach to AML, XYZ Accountants is able to effectively manage its AML risks and ensure compliance with regulations. The firm also gains a better understanding of its clients and can protect its reputation by avoiding involvement in illegal activities.

Example case study: Applying a Risk-Based Approach to AML for company services providers

A reputable company service provider based in the UAE, named ABC Services, operates in various high-end markets worldwide. Given the nature of their clientele and high transaction values, ABC Services is classified as a DNFBP and is therefore subject to AML regulations.

To comply with these regulations and ensure it is not inadvertently facilitating illegal activities, ABC Services must implement a risk-based approach to AML.

Firstly, ABC Services identifies and assesses the AML risks associated with their operations. This involves a detailed analysis of their client base, the countries in which they operate, and the types of transactions they typically handle. The firm finds that some of their operations in certain countries pose a higher risk due to the prevalence of corruption and financial crime.

Secondly, they implement strict CDD procedures to identify high-risk clients and comply with the requirements outlined in Federal Decree-law No. (20) of 2018. This involves verifying the identity of all new clients and conducting ongoing monitoring of existing clients. High-risk clients, such as PEPs, are subject to enhanced due diligence.

Thirdly, ABC Services develops an AML compliance programme tailored to the identified risks. This includes regular staff training on AML regulations and procedures, regular audits to ensure compliance, and the appointment of a dedicated MLRO.

Finally, the company service provider implements a robust reporting system to report any suspicious transactions to the relevant authorities. This system is designed to detect unusual or suspicious activity, such as unusually large transactions or transactions involving high-risk countries or individuals.

By implementing a risk-based approach to AML, ABC Services is able to effectively manage its AML risks and ensure compliance with regulations. The firm also gains a better understanding of its clients and can protect its reputation by avoiding involvement in illegal activities.

Important

It is important to remember that a risk-based approach is not an opportunity to leave uncompleted all appropriate identification, verification and monitoring for each client.

A risk-based approach is a continuous process. It starts with an assessment of the risks, and moves on to mitigating the risks as far as possible, monitoring performance and keeping good records.

Risk assessment: the risk factors

The key risk factors to be considered when formulating a risk-based approach include:

- product types your organisation offers
- distribution channels used
- jurisdictions where you operate and where your clients are from
- customer types
- volumes and sizes of transactions
- if the transaction is conducted in cash or virtual currency, and
- the risk appetite of your organisation.

Let's now look at some examples for some of these risk factors.

Product/service/transaction type risk factors

This could include:

- a one-off transaction or repetitive transactions
- a product, service or transaction that might allow for anonymity or confusion of the true identity of any of the parties involved in the transaction
- providing nominee services
- operating a crypto exchange
- customer requesting to set up of a complex structure to hide the beneficial owner's identity
- cross-border transactions from high-risk jurisdictions, and
- new products and new business practices, including new delivery mechanisms or the use of new or developing technologies for a new or pre-existing product.

Distribution/delivery channel risk factors

This could include:

- new products and/or new business practices involving new delivery channels for new and existing products, with newly developed technology
- assessment of customer acquisition methods and/or relationship management with respect to the channel that the primary product/service is offered through
- the use of non-face-to-face channels (i.e., through electronic means), especially when the customer lacks safeguards for means of electronic identification, or
- the use of third-party business introducers, agents or distributors.

Jurisdiction risk factors

This could include:

- whether the customer's business presence and country of operations have effective AML/CFT systems in place
- a customer's primary business presence and country of operation's reputation in terms of the level and rates of corruption, terrorism, and money laundering, including whether said country is:
  - subject to sanctions, embargos or similar measures
  - involved in the funding or support for terrorism, and
  - characterized by the presence of terrorist organisations.

Customer risk factors

This could include:

- nature of the business relationship (one-off interaction/repetitive transactions)
- registered country and areas of operations
- the customer has nominee shareholders or shares in bearer form
- use of large amounts of cash in the customer's business model

- the complexity of the legal, ownership or-network structure of the customer
- the type of clients the customer serves (i.e., general consumers, high-net-worth individuals, PEPs, corporations), and
- the most recent results of the NRA.

Other risk factors

This could include:

- newness and/or innovation of product, service, or delivery channel, which may not have been established in the market yet, and
- assessment of operational processes with respect to cyber security, use of third parties and/or virtual assets.

Examples of customer risk factors for the real estate sector and company service providers

- Type, complexity, country of origin and transparency of the customer (whether the customer is an individual or legal person and part of a larger corporate group)
- Customer's country of origin (whether they are a UAE national, UAE resident or a foreign customer, and whether they are associated with a high-risk country)
- Channel by which the customer is introduced (e.g., referrals vs. walk-in customers, or customers sourced via the Internet)
- Type, size, complexity, transparency and geographic origins of financial instruments and/or arrangements associated with the transactions
- Unusual nature of the financial instruments or arrangements associated with the transaction, particularly compared with what is normal practice in the local market

Examples of customer risk factors for dealers in precious metals and stones

- Type, complexity and transparency of the customer (whether the customer is a natural

or legal person, part of a larger corporate group, and is associated with a PEP)

- Country of origin of the precious metals and stones including the assessment of the mining risk:
- is it a high-risk country, such as product or trading hub for precious metals and stones, which is subject to international financial sanctions?
- does it have a low score on Transparency International's Corruption Perceptions Index or other corruption indices? Is it a known location for the operation of criminal or terrorist organisations with poor oversight from the government? And,
- does it have appropriate regulations and controls? Is it considered to be a conflict-affected and high-risk area?
- Residence status of the customer (whether they are a UAE national, UAE resident or a foreign customer, and whether they are associated with a high-risk country)
- Channel by which the customer is introduced (e.g., referrals vs. walk-in, international vs. domestic, in-person or via the Internet or other media)
- Types of products, including quantity, level of purity, value and form (whether physical or virtual, raw/rough or processed/finished), portability and potential for anonymity
- Type, size, complexity, cost and transparency of the transaction (including whether the physical or virtual exchange of products is involved); this includes whether the means of payment appear to be consistent with the customer's known income and local market practices
- Unusual nature of the transaction as compared with what is normal practice in the local market; this may include requirements to speed up the transaction beyond what is customary, unusual delivery requirements, or unusual requests for secrecy

DNFBPs in the UAE should incorporate their analysis of proliferation financing risks into a written risk assessment to document their understanding and analysis of proliferation financing risk as a foundation of the risk-based approach. For most entities, it will be appropriate to incorporate their proliferation financing

risk analysis into the same risk assessment performed for other financial crimes (including money laundering and terrorist financing). However, private sector entities may decide to conduct a proliferation financing-specific risk assessment. The approach should be commensurate with an entity's nature, size of its business, and level of exposure to proliferation financing risks.

Using the threat/vulnerability/consequence construct described above, DNFBPs should evaluate their proliferation financing risks. Their risk assessments should generally include the following categories:

- **Geographic risk**: identify and assess the jurisdictions where the DNFBP has headquarters, branches, conducts business and has target markets. Countries known or suspected to have developed illicit WMD programmes are a major source of proliferation financing risk.
- **Customer risk**: evaluate the customer base to identify sources of proliferation financing risk. Customer risk may emanate from dimensions such as designated persons and entities, entities owned or controlled by designated persons, customer business types or activities and customer geographic factors.
- **Product and service risk**: assess the product and service offerings for indicators of proliferation financing risk. Products and services that may be used in any of the three proliferation financing stages (fundraising, disguising funds, or procurement of materials) pose elevated risk.

How DNFBPs are exposed to proliferation financing

All DNFBPs are exposed to proliferation financing risks when dealing directly or indirectly with designated persons identified by the UNSC for proliferation financing.

- **Real estate buying and selling brokerage:**
  - **Direct exposure**: Real estate brokers are generally involved in the buying and selling of properties and typically do not deal directly with trade finance or dual-use goods.
  - **Indirect exposure**: They might encounter clients who are involved in various industries, including those dealing with dual-use goods.

For example, a company involved in the proliferation of WMDs could potentially invest in real estate to launder money or hide assets.

  - **Dealers in precious metals and stones:**
  - **Direct exposure**: These dealers are primarily focused on the trade of valuable commodities like gold, silver and gemstones. Their direct dealings with dual-use goods are unlikely.
  - **Indirect exposure**: Precious metals and stones can be used to finance illicit activities, including the proliferation of WMDs. The high value and ease of transport of these commodities make them attractive for money laundering and other illegal activities.

- **Accountants and company service providers:**
  - **Direct exposure:** Accountants and company service providers assist clients with financial management, tax advice, company formation and other related services. They do not directly engage in trade finance or the handling of dual-use goods.
  - **Indirect exposure:** They may provide services to companies involved in various industries, including those that might deal with dual-use goods. For instance, they could help set up shell companies or manage finances for businesses that engage in illicit trade.

Risk mitigation

Once these risk factors have been assessed, controls should be designed and implemented to mitigate these risks. Remember, it is probably not possible to totally remove any risk. The aim is to mitigate the risks as far as possible.

Risk monitoring: review

On a continuous basis, these controls should be monitored to enable improvements to be made when required to ensure that they remain effective. This monitoring should include a regular risk-assessment to ensure that the risk profile is fully understood.

Recordkeeping

The risk-based approach requires a robust audit trail documenting risk assessments, control measures implemented and the management information produced from monitoring. Effective recordkeeping will provide assurance to regulators and equip senior management with a powerful management tool in developing systems and controls.

Applying risk mitigation measures

The application of risk mitigation methods begins with the findings from the AML self-risk assessment. Once a firm has identified its inherent risks, it can formulate and implement measures to mitigate these risks.

The first step in risk mitigation is designing control measures tailored to the identified risks. For instance, if a firm identifies high risk in dealing with certain types of customer, it might implement enhanced due diligence procedures for these customers. This could involve collecting additional information about the customer, conducting more frequent reviews of the customer's transactions, or seeking approval from senior management before establishing a business relationship with the customer.

Similarly, risk identification might focus on the nature of their clients, the services they offer, and the jurisdictions they operate in. For instance, a real estate agency dealing with high-value property transactions, particularly in regions with high levels of corruption or crime, could face a higher risk of money laundering.

The next step is implementing these control measures. This often involves changes to the firm's policies and procedures, and may require training for employees to ensure they understand the new controls. The firm should also establish mechanisms to monitor the effectiveness of the controls, such as regular audits or reviews.

After the controls have been implemented, the firm should continuously monitor and review their effectiveness. This involves collecting and analysing data related to the controls, such as the number of suspicious activity reports filed, the number of high-risk customers identified, or the number of transactions flagged for review. If the controls are not effective in mitigating the identified risks, the firm should revise them as necessary.

Finally, the firm should document all steps in the risk mitigation process. This not only helps demonstrate compliance with AML regulations, but also provides valuable information for future risk assessments and for improving the firm's overall AML strategy.

Emerging technologies and new payment methods

Emerging technologies and new payment methods pose unique challenges and opportunities for AML compliance, particularly for DNFBPs, and therefore should be taken into consideration for any risk assessments. Let's take a look at some of the main emerging technologies and new payment methods and how they impact DNFBPs.

1. One of the most significant emerging technologies in the financial sector is blockchain, which underpins cryptocurrencies. Cryptocurrencies, due to their decentralised nature and potential for anonymity, can pose significant AML risks. DNFBPs, like real estate agencies or law firms, might face challenges when clients wish to make large payments in cryptocurrency. It becomes essential for these businesses to have robust AML controls in place, such as understanding the provenance of the cryptocurrency and conducting enhanced due diligence on customers using such payment methods.
2. Similarly, other new payment methods, such as mobile money or peer-to-peer payment platforms, can also present AML risks. These payment methods often involve rapid, real-time transactions that can be difficult to monitor effectively for suspicious activity. DNFBPs must ensure their AML controls can keep pace with the speed and volume of these transactions.

On the other hand, emerging technologies can also provide new tools for AML compliance. For instance, machine learning and artificial intelligence can be used to analyse large volumes of transaction data more quickly and accurately than human analysts. This can help DNFBPs to identify suspicious patterns of activity and high-risk customers more effectively.

Biometric technology, such as fingerprint or facial recognition, can also enhance customer identification and verification procedures, making it more difficult for criminals to use false identities for money laundering.

DNFBPs need to stay up to date with these emerging technologies and new payment methods, understanding their potential risks and benefits. This will help them to adapt their AML self-risk assessments and risk mitigation measures accordingly. Regular training for employees, continuous monitoring and review of controls, and collaboration with regulatory authorities and other stakeholders can also help DNFBPs navigate these challenges and opportunities.

While emerging technologies and new payment methods pose new AML challenges for DNFBPs, they also offer opportunities for more effective AML compliance. By staying informed and adapting their AML strategies accordingly, DNFBPs can manage their risk exposure and contribute to the global fight against money laundering.

In the UAE

As part of their obligation to update their ML/FT risk assessments on an ongoing basis, the AML-CFT Decision specifically requires DNFBPs to "identify and assess the risks of money laundering and terrorism financing that may arise when developing new products and new professional practices, including means of providing new services and using new or underdevelopment techniques for both new and existing products."

DNFBPs must complete the assessment of such risks, and take the appropriate risk management measures, prior to launching new products and services, practices or techniques, or technologies. In general, they should integrate these ML/FT risk assessment and mitigation requirements into their new product, service, channel, or technology development processes.

For the purpose of assessing the ML/FT risks associated with new products, services, practices, techniques, or technologies, DNFBPs may consider utilising the same or similar risk assessment models or methodologies as those utilised for their ML/TF business risk assessments, updated as necessary for the particular circumstances. They should also document the new product, service, practice, technique, or technology risk assessments, in keeping with the nature and size of their businesses.

(Source: Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations. Select this link for more information)

Self-assessment questions

Congratulations, you have reached the end of Unit 2. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, continue or alternatively, you can work through the section again if you wish.

1. Which of the following is an essential aspect of a risk-based approach to AML compliance?
    a) Ignoring low-risk business areas
    b) Applying the same level of scrutiny to all clients
    c) Applying enhanced due diligence for higher-risk categories of business
    d) Avoiding business with politically exposed persons (PEPs) at all costs
2. In the context of an AML self-risk assessment, which of the following is NOT typically considered as a key risk area?
    a) Nature and scale of the business
    b) Customer risk
    c) Geographical risk
    d) Historical performance of the business
3. In the context of AML regulations in the UAE, which obligation is specifically highlighted for DNFBPs when developing new products and professional practices?
    a) Ensure customer convenience is addressed prior to security measures
    b) Potential risks associated with new technologies should be considered if cost effective
    c) Identification and assessment of the risks of money laundering and terrorism financing
    d) Products are launched as quickly as possible to ensure they are not outdated

Correct answers 1c, 2d, 3c

Unit 3: Customer Due Diligence and Enhanced Due Diligence Requirements

Learning Objectives

The purpose of this learning material is to:

- define what customer due diligence is
- explain when to apply CDD requirements
- determine what a PEP is and how to apply the correct CDD measures, and
- examine high-risk jurisdictions and the risks they pose.

What is CDD?

In simple terms, CDD is a risk assessment.

Definition: CDD

CDD is defined in the Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations as:

The process of identifying or verifying the information of a Client or Beneficial owner, whether a natural or legal person or a legal arrangement, and the nature of its activity and the purpose of the business relationship and the ownership structure and control over it for the purpose of this Decree-Law and its Implementing Regulation.

(source: www.moec.gov.ae/en/federal-decree-law-no-20-of-2018-on-anti-money-laundering-and-combating-the-financing-of-terrorism-and-illegal-organisations

Having sufficient information about a client and making use of that information underpins all other aspects of a firm's AML regime and is the most effective weapon against being used to launder the proceeds of crime. In addition to minimising the risk that your firm will be used for illicit activities, it provides protection against fraud, assists in enabling suspicious activity to be recognised and protects individual institutions from reputational and financial risks.

Important

The obligation to 'know your customer' also serves to protect genuine clients from being suspected of money laundering and helps to guard against their identities being stolen.

CDD should be part of a client profile that you maintain in order to potentially identify anything that appears out of line with previous expectations and could therefore be considered grounds for suspicion.

Note

Before we begin to look at CDD requirements in more detail, it is important to note that some DNFBPs may use outsourcing companies in order to fulfil some, or all, of their CDD/AML requirements. In these circumstances, it is stipulated in the AML-CFT Decision that DNFBPs shall:

'Ensure that the third party is regulated and supervised, and adheres to the CDD measures towards Customers and record-keeping provisions of the present Decision.'

When relying on third parties, DNFBPs must ensure a number of things, including:

- checking if the outsourcing partner has relevant resources and capabilities for AML
- ensuring the third party follows a customised approach for AML compliance as determined by the DNFBP
- ensuring the third party complies with data security and confidentiality requirements
- establishing clear lines of communication, and
- being involved in the AML compliance function as a controlling factor.

In addition to the above, when relying on foreign third parties for the undertaking of CDD measures, DNFBPs should take necessary steps to ensure that the AML/CFT regulatory and supervisory framework under which the third party operates is at least equivalent to that of the State. This means that DNFBPs should ensure that the third party is regulated, supervised for AML/CFT purposes, and adheres to the equivalent CDD and recordkeeping measures.

The practical application of CDD

As in all areas of firms' AML regimes, regulation allows and expects a risk-based approach to be applied to CDD. Regulators and industry guidance provide direction in this area by:

- setting out scenarios that could warrant an 'automatic' low-risk categorisation allowing for 'simplified due diligence'
- mandating certain circumstances as higher risk and requiring enhanced due diligence, e.g., PEP clients
- providing guidance on the 'ingredients' firms should take into account to assess the money laundering risk in all other circumstances, and
- providing some assistance on the actual requirements for CDD in the various risk categories.

It is worth restating the fundamental reasoning behind CDD.

CDD is the foundation of a good AML regime because it assists in the prevention and detection of criminal activity and those behind such activity. Hence, it is important that firms ensure they have:

- **identified the client** (including beneficial owners)
- **verified that identity**, and
- **recorded 'on file' sufficient additional information** (at least the reason for the relationship) and data on their clients to assist in the detection of potentially suspicious activity. The type of additional information may include the type of business they are engaged in, the industry, whether they are new or established, or in the case of an individual, the stage of life they are in, the counterparties they deal with (both the people they pay and those from whom they will get paid), the geographical area(s) in which they operate, and the expected turnover on the account(s) – money in and out, values, volumes and frequency.

It is also expected that this will be carried out in a risk-based fashion in order that firms can allocate resources to CDD appropriately.

Example

In some firms, applying appropriate CDD may be relatively straightforward, where the client base is small and the product offering and geographic footprint are limited. For others it presents a considerable challenge to differentiate the risk posed by the many types of potential client.

Key learning point

It goes without saying that CDD must be completed in all cases before any transactions are completed for any client.

Examples of typical scenarios and the level of CDD to be applied

The following examples set out some scenarios that pose particular risk situations that may require a different approach to CDD. Select the example relating to your industry.

Example 1: Real estate agency

A high-profile real estate agency is approached by a foreign client who wishes to purchase several high-value properties in a short span of time. The client wishes to make the payments in cryptocurrency. This scenario presents a risk due to the large transactions involved, the client's foreign status, and the use of cryptocurrency, which can be harder to trace than conventional currencies.

In this case, the real estate agency would need to apply enhanced due diligence procedures. This could include verifying the source of the client's wealth and funds, obtaining detailed information about the client's business and reasons for the property purchases, and understanding the provenance of the cryptocurrency. The agency might also need to consult with a legal or financial expert to ensure compliance with laws and regulations related to cryptocurrency transactions.

Example 2: Law firm

A law firm provides services to a client who is a PEP. The client requires assistance in setting up an elaborate network of companies and trusts across multiple jurisdictions. This scenario presents a risk due to the client's PEP status and the complexity and international nature of the requested services, which could potentially be used to obscure beneficial ownership or launder money.

In this case, the law firm would need to conduct enhanced due diligence. This might involve obtaining senior management approval for establishing the business relationship, taking reasonable measures to establish the source of wealth and source of funds that are involved in the business relationship or transactions, and conducting enhanced ongoing monitoring of the business relationship. The law firm might also need to seek additional information or assurances about the purpose and nature of the proposed network of companies and trusts.

Example 3: DPMS

A precious metals and stones dealer is approached by a client who wishes to purchase a significant quantity of gold bullion and diamonds. The client is a PEP and the transaction involves multiple jurisdictions. The client insists on paying in cash and requests the delivery of the purchased items to be made to a location in a country known for its high rates of corruption and financial crime. This scenario presents a risk due to the client's PEP status, the size of the transaction, the method of payment, and the destination of the goods, which could all potentially be used to facilitate money laundering or other illicit activities.

In this case, the dealer would need to conduct enhanced due diligence. This would involve obtaining senior management approval for the transaction, taking reasonable measures to establish the source of wealth and source of funds involved in the transaction, and conducting enhanced ongoing monitoring of the business relationship. The dealer might also need to seek additional information or assurances about the purpose and nature of the proposed transaction, and consider

refusing to proceed with the transaction if such assurances cannot be satisfactorily provided.

Example 4: CPS

A corporate service provider is approached by a local small low-risk business, that has been in operation for several years in the same town. The business is seeking assistance with routine financial management and tax filing services. Given the nature of the business, its local operations, and its long-standing presence in the community, the risk of money laundering or other illicit activities is very low.

In this case, the corporate service provider could conduct simplified due diligence. This would involve basic identity verification of the business owners, confirmation of the business's registration and operations, and a cursory review of its financial transactions. Given the lower risk profile of this client, the provider may not need to conduct extensive checks on the source of funds or ongoing monitoring of the business relationship. However, the provider should still be mindful of any unusual or suspicious activities and be prepared to escalate due diligence measures if necessary.

Example 5: Accountants

An accountancy firm is approached by a local restaurant chain looking for financial auditing services. The restaurant chain has several locations within the same city, a clear and transparent ownership structure, and an established reputation. The firm is aware, however, that the hospitality industry can sometimes be associated with cash-based transactions and therefore a slightly higher risk of money laundering.

In this case, the accountancy firm would conduct standard due diligence. This would involve verifying the identity of the restaurant chain's owners, understanding the nature of the business, and reviewing its financial statements and transactions. The firm would also assess the risk profile of the restaurant chain based on factors such as its size, location, customer base, and the nature of its transactions. Regular monitoring of the business relationship would be conducted to identify any unusual or suspicious activities. If any higher risk factors were

identified, the firm would be prepared to escalate to enhanced due diligence measures.

Important

It is important to note that any situation in which CDD measures cannot be performed, such as when the customers or beneficial owners refuse to provide CDD documentation, or provide documentation that is false, misleading, fraudulent or forged, the transaction should be rejected and a report should be submitted to the FIU via the GoAML portal. We will discuss this in more detail later on in this course.

When the CDD requirements apply for DNFBPs

When DNFBPs are required to comply with the CDD requirements set out in FATF's Recommendation 10 (CDD requirements):

(a) Casinos – when customers engage in financial transactions[93] equal to or above USD/EUR 3 000.

(b) Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate.[94]

(c) Dealers in precious metals and dealers in precious stones – when they engage in any cash transaction with a customer equal to or above USD/EUR 15,000.

(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;*
- *creating, operating 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 following activities:

- *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 performing the equivalent function for another form of legal arrangement;*
- *acting as (or arranging for another person to act as) a nominee shareholder for another person.*

CDD requirements for DNFBPs in the UAE are detailed in the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

Section 3 of the Cabinet Decision details the following CDD requirements.

Article (5)

1. Financial Institutions and DNFBPs are required to undertake CDD measures to verify the identity of the Customer and the Beneficial Owner before or during the establishment of the business relationship or opening an account, or before executing a transaction for a Customer with whom there is no business relationship. And in the cases where there is a low crime risk, it is permitted to complete verification of Customer identity after establishment of the business relationship, under the following conditions:

(a) The verification will be conducted in a timely manner as of the commencement of business relationship or the implementation of the transaction.

(b) The delay is necessary in order not to obstruct the natural course of business.

(c) The implementation of appropriate and effective measures to control the risks of the Crime.

2. *Financial Institutions and DNFBPs are required to take measures to manage the risks in regards to the circumstances where Customers are able to benefit from the business relationship prior to completion of the verification process.*

Article (6)

Financial Institutions and DNFBPs should, as the case may be, undertake CDD measures in the following cases:

1. *Establishing the business relationship;*
2. *Carrying out occasional transactions in favour of a Customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;*
3. *Carrying out occasional transactions in the form of Wire Transfers for amounts equal to or exceeding AED 3,500.*
4. *Where there is a suspicion of the Crime.*
5. *Where there are doubts about the veracity or adequacy of previously obtained Customer's identification data.*

Article (7)

Financial Institutions and DNFBPs should undertake CDD measures and ongoing supervision of business relationships, including:

1. *Audit transactions that are carried out throughout the period of the business relationship, to ensure that the transactions conducted are consistent with the information they have about Customer, their type of activity and the risks they pose, including – where necessary - the source of funds.*
2. *Ensure that the documents, data or information obtained under CDD Measures are up-to-date and appropriate by reviewing the records, particularly those of high-risk customer categories.*

Article (12)

Financial Institutions and DNFBPs should apply CDD measures to Customers and the ongoing business relationship on the effective date of the present Decision, within such times as deemed appropriate based on relative importance and risk priority. It should also ensure the sufficiency of data acquired,

in case CDD measures were applied before the effective date of the present Decision.

Article (13)

1. *Financial Institutions and DNFBPs shall be prohibited from establishing or maintaining a business relationship or executing any transaction should they be unable to undertake CDD measures towards the Customer and should consider reporting a suspicious transaction to the FIU.*
2. *Even if they suspect the commission of a Crime, financial institutions and DNFBPs should not apply CDD measures if they have reasonable grounds to believe that undertaking such measures would tip-off the Customer and they should report a Suspicious Transaction to the FIU along with the reasons having prevented them from undertaking such measures.*

Article (14)

Financial Institutions and DNFBP's shall commit to the following:

1. *Not to deal in any way with Shell Banks, whether to open bank accounts in their names, or to accept funds or deposits from them.*
2. *Not to create or keep records of bank accounts using pseudonyms, fictitious names or numbered accounts without the account holder's name.*

From the following, select the case study that relates to your industry.

Case Study: Application of CDD requirements for a real estate agency in the UAE

A large real estate agency in the UAE is approached by a foreign investor seeking to purchase several high-value properties. The investor is not a resident and doesn't have an established business relationship with the agency. According to the UAE's legal requirements, as a DNFBP, the agency is required to undertake CDD measures before executing the transaction or establishing a business relationship (Article 5 of section three of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations).

The agency must verify the identity of the investor (the customer) and the beneficial owner. However, given the high value of the transaction and the non-residential status of the investor, there's a potential risk of money laundering or other financial crimes. As such, the agency must implement CDD measures immediately, rather than after the establishment of the business relationship (Article 5).

The agency should carefully assess the source of the funds being used for the transaction, confirm the customer's identification data, and understand the nature of the customer's business and the reasons for the purchase of the properties (Articles 6 and 7). The agency should also ensure that the documents, data, or information obtained are up-to-date and appropriate (Article 7).

If there are any doubts about the veracity or adequacy of the customer's identification data, or if there's suspicion of crime, the agency should not proceed with the transaction until these issues are resolved (Articles 6 and 13). The agency should be prepared to report a suspicious transaction to the FIU if unable to undertake appropriate CDD measures (Article 13).

The agency is also prohibited from accepting funds or deposits from shell banks or creating records of bank accounts using pseudonyms, fictitious names, or numbered accounts without the account holder's name (Article 14).

Overall, the agency must carefully manage the risks and ensure compliance with the UAE's legal requirements for CDD. Failure to do so could potentially result in severe penalties.

Case Study: Application of CDD requirements for DPMS in the UAE

A prominent precious metals and stones dealer in the UAE is approached by a foreign national looking to buy a significant quantity of diamonds and gold. The buyer is not a resident of the UAE and has no prior relationship with the dealer. In line with the UAE's legal stipulations, the dealer, as a DNFBP, is obliged to carry out CDD measures before the transaction can take place or a business relationship is established as outlined in

Article 5 of section three of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

The dealer is required to verify the identity of the buyer and the beneficial owner. Given the high value of the transaction and the foreign nature of the buyer, there is a potential risk of money laundering or other financial crimes. Therefore, the dealer must implement CDD measures as soon as possible, rather than waiting until after the business relationship is established, as per Article 5.

The dealer must carefully evaluate the source of the funds used for the transaction, ascertain the buyer's identification data, and understand the buyer's business nature and reasons for the diamond and gold purchase (Articles 6 and 7). The dealer must also ensure the documents, data, or information collected are up-to-date and relevant (Article 7).

If there are any doubts regarding the accuracy or adequacy of the buyer's identification data, or if there's a suspicion of a crime, the dealer should halt the transaction until these issues are resolved (Articles 6 and 13). If the dealer cannot undertake appropriate CDD measures, they should be prepared to report a suspicious transaction to the FIU (Article 13).

The dealer is also forbidden from accepting funds or deposits from shell banks or creating records of bank accounts using pseudonyms, fictitious names, or numbered accounts without the account holder's name (Article 14).

Overall, the dealer must carefully manage the risks and ensure compliance with the UAE's legal requirements for CDD. Non-compliance could result in severe penalties.

Case Study: Application of CDD requirements for Accountants in the UAE

A highly regarded accounting firm in the UAE is approached by a foreign company seeking to engage their services for a large-scale audit. The company is not based in the UAE and has no pre-existing relationship with the accounting firm. As per the UAE's legal framework, the accounting firm, being a DNFBP, is mandated to conduct CDD measures before

proceeding with the engagement or establishing a business relationship (Article 5 of section three of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations).

The firm must verify the identity of the company and the beneficial owner. Given the significant scale of the proposed engagement and the foreign status of the company, there is potential risk for financial crimes such as money laundering. Therefore, CDD measures must be put into action immediately, rather than after the establishment of a business relationship, as outlined in Article 5.

The firm must meticulously investigate the source of funds used for the engagement, confirm the company's identification data, and understand the nature of the company's business and the reasons for the engagement (Articles 6 and 7). It's also crucial that the firm ensures that the documents, data, or information collected are up-to-date and appropriate (Article 7).

If there are any doubts about the authenticity or adequacy of the company's identification data, or if there's any suspicion of illegal activities, the firm should not proceed with the engagement until these issues are resolved (Article 6 and 13). If the firm is unable to undertake proper CDD measures, they should be prepared to report the suspicious activity to the FIU (Article 13).

The firm is also prohibited from accepting funds or deposits from shell banks or creating records of bank accounts using pseudonyms, fictitious names, or numbered accounts without the account holder's name (Article 14).

Overall, the accounting firm must effectively manage the risks and ensure strict compliance with UAE's legal requirements for CDD. Failure to do so could result in serious penalties.

Case Study: Application of CDD requirements for CPS in the UAE

A reputable company service provider in the UAE is contacted by a foreign corporation seeking to establish a local subsidiary. The corporation is not based in the UAE and has no prior relationship with the service provider. As per the UAE's legal provisions, the service provider, as a DNFBP, is required to conduct CDD measures before proceeding with the proposed business setup or establishing a business relationship (Article 5 of section three of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations).

The service provider must verify the identity of the corporation and the beneficial owner. Given the large scale of the proposed business setup and the foreign status of the corporation, there is a potential risk of money laundering or other financial crimes. As such, the service provider must implement CDD measures immediately, rather than after the establishment of the business relationship, as per Article 5.

The service provider must diligently assess the source of the funds used for the business setup, verify the corporation's identification data, and understand the nature of the corporation's business and the reasons for the setup (Articles 6 and 7). The service provider should also ensure that the documents, data, or information obtained are up-to-date and appropriate (Article 7).

If there are any doubts about the veracity or adequacy of the corporation's identification data, or if there's a suspicion of illicit activities, the service provider should not proceed with the business setup until these issues are resolved (Articles 6 and 13). If the service provider is unable to undertake appropriate CDD measures, they should be prepared to report a suspicious transaction to the FIU (Article 13).

The service provider is also prohibited from accepting funds or deposits from shell banks or creating records of bank accounts using pseudonyms, fictitious names, or numbered accounts without the account holder's name (Article 14).

Overall, the service provider must carefully manage the risks and ensure compliance with the UAE's legal requirements for CDD. Failure to do so could potentially result in severe penalties.

Identifying your customers

The first step in identifying a customer's identity is obtaining personal information. This includes:

- full name
- date of birth
- residential address, and
- contact details.

For corporate customers, this may also involve obtaining information about the company's structure, ownership and nature of business.

The second step is verification of the obtained information. This involves corroborating the customer's identity using reliable, independent source documents, data or information. This could be a government-issued ID for individuals or registration documents for companies. For online businesses, identity verification could involve two-factor authentication or biometric data.

An essential part of CDD is understanding the purpose and intended nature of the business relationship. This involves gathering information about the nature of the customer's business, their source of funds, and the expected pattern and level of transactions. This information helps in assessing the risk level of the customer and determining the level of monitoring required.

Identifying the identity of your customers is not a one-off process – it requires ongoing monitoring to ensure that the customer's activities remain consistent with their risk profile and to detect any potentially suspicious activity.

Let's look at the requirements for DNFBPs in the UAE.

Article (8)

1. *Financial Institutions and DNFBPs should identify the Customer's identity, whether the Customer is permanent or walk-in, and whether the Customer is a natural or legal person or legal arrangement, and verify the Customer's identity and the identity of the Beneficial Owner. This should be done using documents, data or any other identification information from a reliable and independent source as follows:*

(a) For Natural Persons:

The name, as in the identification card or travel document, nationality, address, place of birth, name and address of employer, attaching a copy of the original and valid identification card or travel document, and obtain approval from the senior management, if the Customer or the Beneficial Owner is a PEP.

(b) For Legal Persons and Legal Arrangements:

(1) The name, Legal Form and Memorandum of Association

(2) Headquarter office address or the principal place of business; if the legal person or arrangement is a foreigner, it must mention the name and address of its legal representative in the State and submit the necessary documents as a proof.

(3) Articles of Association or any similar documents, approved by the relevant authority within the State.

(4) Names of relevant persons holding senior management positions in the legal person or legal arrangement.

2. Financial institutions and DNFBP's are required to verify that any person purporting to act on behalf of the Customer is so authorised, and verify the identity of that person as prescribed in Clause (1), of this Article.

3. Financial institutions and DNFBP's are required to understand the intended purpose and nature of the business relationship, and obtain, when necessary, information related to this purpose.

4. Financial institutions and DNFBP's are required to understand the nature of the Customer's business as well as the Customer's ownership and control structure.

Identifying the beneficial ownership

Identifying the beneficial ownership of customers is a key component of the CDD process, especially for DNFBPs dealing with corporate clients. First, let's determine what a beneficial owner is.

Definition

The natural person who ultimately owns or exercises effective control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or legal arrangement.

The first step to identify the beneficial owner involves obtaining information about the ownership and control structure of the corporate customer. This could include details about shareholders, directors, trustees or any other individuals who have significant control over the company's activities.

Next, verification of this information is critical. This can be done through a review of documents such as articles of incorporation, a trade license, shareholder agreements or trust deeds. Companies may also be required to provide official ownership registries or similar documents.

Understanding the nature and purpose of the business relationship is also vital. This will help in establishing the legitimacy of the beneficial ownership structure. If the ownership structure is complex or opaque, it may be necessary to seek additional information or clarification.

For higher-risk scenarios, enhanced due diligence may be required. This could involve more in-depth investigation into the beneficial owners, including source of funds checks, background checks or cross-checking with third-party databases.

Ongoing monitoring is also crucial to ensure that the information about beneficial ownership remains accurate and up to date. Any changes in the ownership structure should be identified and verified promptly.

Let's look at the requirements for identifying beneficial ownership for DNFBPs in the UAE.

Article (9)

Financial Institutions and DNFBP's are required to take reasonable measures to identity the Beneficial Owners of legal persons and Legal Arrangements and verify it, by using information, data, or documents acquired from a reliable source, by the following:

1. *For Customers that are legal persons:*
   - (a) *Obtaining and verifying the identity of the natural person, who by himself or jointly with another person, has a controlling ownership interest in the legal person of 25% or more, and in case of failing or having doubt about the information acquired, the identity shall be verified by any other means.*
   - (b) *In the event of failing to identify the natural person exercising control as per paragraph (a) of this Clause, or the person(s) with the controlling ownership interest is not the Beneficial Owner, the identity shall be identified for the relevant natural person(s) holding the position of senior management officer, whether one or more persons.*
2. *For Customers that are Legal Arrangements:*

   Verifying the identity of the Settlor, the Trustee(s), or anyone holding a similar position, the identity of the beneficiaries or class of beneficiaries, the identity of any other natural person exercising ultimate effective control over the legal arrangement, and obtaining sufficient information regarding the Beneficial Owner to enable the verification of his/her identity at the time of payment, or at the time he/she intends to exercise his/her legally acquired rights.

Article (10)

Financial Institutions and DNFBPs shall be exempted from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner, if such information is obtainable from reliable sources where the Customer or the owner holding the controlling interest are as follow:

1. *A company listed on a regulated stock exchange subject to disclosure requirements through any means that require adequate transparency requirements for the Beneficial Owner.*
2. *A subsidiary whose majority shares or stocks are held by the shareholders of a holding company.*

Article (11)

1. *In addition to the CDD measures required for the Customer and the Beneficial Owner, Financial Institutions shall be required to conduct CDD measures and ongoing monitoring of the beneficiary of life insurance policies and funds generating transactions, including life insurance products relating to investments and family Takaful insurance, as soon as the beneficiary is identified or designated as follows:*
   - *(a) For the beneficiary identified by name, the name of the person, whether a natural person a legal person or a legal arrangement, shall be obtained.*
   - *(b) For a beneficiary designated by characteristics or by class– such as a family relation like parent or child, or by other means such as will or estate – it shall be required to obtain sufficient information concerning the beneficiary to ensure that the Financial Institution will be able to establish the identity of the beneficiary at the time of the pay-out*
2. *In all cases – the Financial Institutions should verify the identity of the beneficiary at the time of the payout as per the insurance policy or prior to exercising any rights related to the policy. If the Financial Institution identifies the beneficiary of the insurance policy to be a high-risk legal person or arrangement, then it should conduct enhanced CDD measures to identify the Beneficial Owner of that beneficiary, legal person, or legal arrangement.*

From the following, select the case study that relates to your industry.

Case study: Identifying a beneficial owner in a precious metals and stones dealer in the UAE

A prominent dealer in precious metals and stones in Dubai is approached by a foreign legal entity wishing to purchase a large quantity of diamonds. The entity is a recently established trust located in an offshore jurisdiction, thereby necessitating the application of CDD as per UAE's legal requirements (Article 9).

The dealer begins by verifying the trust's registration details and its trustees. However, the complex structure of the trust makes it difficult to identify the controlling parties or the beneficial owner.

In line with Article 9, the dealer takes reasonable measures to identify the beneficial owner. The dealer seeks additional information from the trust, including details about the settlor, trustees, beneficiaries, and any other person exercising ultimate control over the trust. The dealer also employs an independent due diligence service to verify the information.

The investigations reveal that the trust is controlled by a single individual, a known PEP, who is also the settlor and a beneficiary. The dealer also verifies this information using documents obtained from reliable sources.

Given the high-risk profile associated with the PEP status of the beneficial owner, the dealer decides to conduct enhanced due diligence. This includes understanding the source of wealth and funds, obtaining senior management approval for the transaction, and conducting enhanced ongoing monitoring of the business relationship as per UAE's legal requirements (Article 11).

However, if the corporate entity had been a company listed on a regulated stock exchange or a subsidiary whose majority shares are held by the shareholders of a holding company, then the dealer would have been exempt from identifying and verifying the identity of any shareholder, partner, or the beneficial owner (Article 10).

This case study highlights the importance of thorough application of CDD measures in identifying beneficial owners to help DNFBPs manage potential risks and ensure compliance with legal requirements.

Case study: Identifying a Beneficial Owner in real estate agents in the UAE

A renowned real estate agency in Dubai is approached by a foreign legal entity looking to acquire several high-value properties. The entity is a newly established trust located in an offshore jurisdiction, necessitating the application of CDD as per UAE's legal requirements (Article 9).

The agency starts by verifying the trust's registration details and its trustees.

However, the complex structure of the trust makes it challenging to identify the controlling parties or the beneficial owner.

In line with Article 9, the agency takes reasonable measures to identify the beneficial owner. The agency seeks additional information from the trust, including details about the settlor, trustees, beneficiaries, and any other person exercising ultimate control over the trust. The agency also employs an independent due diligence service to verify the information.

The investigations reveal that the trust is controlled by a single individual, a known PEP, who is also the settlor and a beneficiary. The agency also verifies this information using documents obtained from reliable sources.

Given the high-risk profile associated with the PEP status of the beneficial owner, the agency decides to conduct enhanced due diligence. This includes understanding the source of wealth and funds, obtaining senior management approval for the transaction, and conducting enhanced ongoing monitoring of the business relationship as per UAE's legal requirements (Article 11).

However, if the corporate entity had been a company listed on a regulated stock exchange or a subsidiary whose majority shares are held by the shareholders of a holding company, then the agency would have been exempt from identifying and verifying the identity of any shareholder, partner, or the beneficial owner (Article 10).

This case study highlights the importance of thorough application of CDD measures in identifying beneficial owners to help DNFBPs manage potential risks and ensure compliance with legal requirements.

Case study: Identifying a beneficial owner in accountants in the UAE

A prestigious accounting firm in the UAE is approached by a foreign legal entity seeking to engage their audit services. The entity is a newly formed trust located in an offshore jurisdiction, thereby making it necessary to apply CDD as per UAE's legal requirements (Article 9).

The firm starts by verifying the registration details of the trust and its trustees. However, due to the complex structure of the trust, it becomes difficult to identify the controlling parties or the beneficial owner.

As per Article 9, the firm takes reasonable measures to identify the beneficial owner. It seeks additional information from the trust, including details about the

settlor, trustees, beneficiaries, and any other person exercising ultimate control over the trust. The firm also employs an independent due diligence service to verify the information.

Through their investigations, it becomes evident that the trust is controlled by a single individual, a known PEP, who is also the settlor and a beneficiary. The firm also verifies this information using documents obtained from reliable and independent sources.

Given the high-risk profile associated with the PEP status of the beneficial owner, the firm decides to conduct enhanced due diligence. This includes understanding the source of wealth and funds, obtaining senior management approval for the transaction, and conducting enhanced ongoing monitoring of the business relationship as per UAE's legal requirements (Article 11).

However, if the corporate entity had been a company listed on a regulated stock exchange or a subsidiary whose majority shares are held by the shareholders of a holding company, then the firm would have been exempt from identifying and verifying the identity of any shareholder, partner, or the beneficial owner (Article 10).

This case study highlights the importance of thorough application of CDD measures in identifying beneficial owners to help DNFBPs such as accountants manage potential risks and ensure compliance with legal requirements.

Case Study: Identifying a beneficial owner in CPS in the UAE

A well-respected company service provider in the UAE is approached by a foreign legal entity looking to establish a subsidiary in the UAE. The entity is a newly formed trust located in an offshore jurisdiction, thereby necessitating the application of CDD as per UAE's legal requirements (Article 9).

The service provider begins by verifying the trust's registration details and its trustees. However, due to the complex structure of the trust, it becomes difficult to identify the controlling parties or the beneficial owner.

In accordance with Article 9, the service provider takes reasonable measures to identify the beneficial owner.

It seeks additional information from the trust, including details about the settlor, trustees, beneficiaries, and any other person exercising ultimate control over the trust. The service provider also engages an independent due diligence service to verify the information.

The investigations reveal that the trust is controlled by a single individual, a known PEP, who is also the settlor and a beneficiary. The service provider also verifies this information using documents obtained from reliable sources.

Given the high-risk profile associated with the PEP status of the beneficial owner, the service provider decides to conduct enhanced due diligence. This includes understanding the source of wealth and funds, obtaining senior management approval for the transaction, and conducting enhanced ongoing monitoring of the business relationship as per UAE's legal requirements (Article 11).

However, if the corporate entity had been a company listed on a regulated stock exchange or a subsidiary whose majority shares are held by the shareholders of a holding company, then the service provider would have been exempt from identifying and verifying the identity of any shareholder, partner, or the Beneficial Owner (Article 10).

This case study underscores the importance of thorough application of CDD measures in identifying beneficial owners to help DNFBPs like company service providers manage potential risks and ensure compliance with legal requirements.

Applying ongoing CDD

While 'ongoing' monitoring of a business relationship is a general regulatory requirement seen as applying to the transactions conducted over the accounts of a client, it is also – either by actual regulation or expectation – related to keeping the CDD data and information a firm retains on clients relevant and up to date. Again, this is accepted to be on a risk-sensitive basis.

Ensuring that customer information is relevant and up to date is also a requirement contained within data protection legislation and regulation. 'Ongoing' monitoring of client business relationships and scrutiny of transactions must be undertaken throughout the course of that relationship

to ensure that 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.

This does not mean reviewing each and every transaction. Firms are, instead, to adopt a risk-based programme of monitoring that will ensure that those relationships and transactions, which are identified as being higher risk, are reviewed more frequently than those that are identified as being a lower risk.

Think about

In practice, this means that some transactions and relationships may be reviewed as they are instructed or daily, weekly or monthly. Others will be reviewed retrospectively and as part of annual checks.

In order to conduct ongoing monitoring of higher-risk business and relationships, firms may use systemic screening tools to identify these risks and to route them for further consideration and approval. This form of automated screening may include the use of internal 'bad guys' lists to which the names and accounts of high-risk relationships are added to supplement other lists of sanctioned names, along with entities that are prescribed by laws and regulations. Alternatively, firms may implement enhanced due diligence checks during which transactions are manually reviewed together with the data that is held on record for each client profile.

There is generally no expectation for firms to re-verify the identity of a client (unless there are doubts or new information – e.g., the previous identity document used is missing or no record of it was retained or there is a new executive director or partner of a firm), however, legislation might state the need for the information to be 'up to date'.

This 'ongoing' monitoring has seen the emergence in many firms of periodic customer reviews which, in a risk sensitive environment, create their own challenges around the following questions.

Questions

- What should such a review comprise?
- When should it occur?
- Should it apply across all clients?

It is clearly common sense to be able to identify when a client's behaviour would make a firm reconsider the money laundering risk associated with them (e.g., they become a PEP or adverse media information emerges linking them to criminal conduct).

Occasional transactions

During the course of business, DNFBPs may be required to perform occasional or nonrecurring transactions for customers with whom there is no ongoing account or business relationship. Examples of such transactions include, but are not limited to:

- sale or purchase of goods such as precious stones, metals, coins or other valuable property to or from a customer
- accepting a deposit for a real-estate purchase from a prospective buyer, and
- drafting of a will, trust agreement, or other legal agreement for a walk-in customer.

On such occasions, DNFBPs are required to identify the customer and verify the customer's identity as well as that of the beneficial owners, beneficiaries and controlling persons. Furthermore, DNFBPs are required to undertake appropriate risk-based CDD measures, including among other things understanding the nature of the customer's business and the purpose of the transaction, in the cases specified in Article 6 of the AML-CFT Decision, such as:

- when carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED55,000 (or equivalent in any other currency), whether the transaction is carried out in a single transaction or in several transactions that appear to be linked
- when there is a money laundering or terrorist financing suspicion, and

- when there are doubts about the veracity or adequacy of identification data previously obtained with regard to the customer.

Simplified due diligence

As we have discussed international standards require that a risk-based approach is applied to CDD. Consequently, the measures should be applied on a risk-sensitive basis depending on the type of customer, business relationship or nature of the transactions or activity. Higher-risk categories should be subject to enhanced due diligence and lower-risk categories may be subject to simplified due diligence.

Most AML regulations now allow for a form of simplified due diligence in the lowest-risk situations. Customers considered to be of a low risk are typically subjected to simplified due diligence requirements, focusing primarily on the **customer identification** element of CDD.

Customer identification

Due diligence enquiries will usually be limited to verifying the customer's identity and the elements justifying the low-risk treatment of the customer, such as:

- evidence of domiciliation in, or citizenship of, a low-risk country
- absence of exposure to sanctions
- confirmation of non-high-risk business activities
- confidence that the customer is not a PEP, and
- proof of status as a public authority, publicly listed company or regulated institution (with equivalent status).

Other elements

As for the other elements:

- beneficial owners and controllers will either not be assessed or be assessed only if their ownership exceeds the higher 25% threshold
- the purpose of relationship will be assessed at a high level

- future due diligence will be performed at a lower intensity, for example periodic reviews will be carried out at longer intervals (three to five years) and transaction monitoring done on a less intensive basis than would be the case for standard CDD, and
- information provided by the customer in these areas may be considered sufficient – external verification will not be sought.

In order to apply simplified due diligence, firms must be satisfied that the relationship presents a lower degree of risk. Simplified due diligence is therefore not an exemption to carry out CDD checks and should never be applied when specific risk factors are known to exist.

Extract: Simplified CDD measures

The Interpretive Notes to Recommendation 10 of the FATF Recommendations clarify the requirements in the following terms.

The simplified measures should be commensurate with the lower risk factors (e.g. the simplified measures could relate only to customer acceptance measures or to aspects of ongoing monitoring). Examples of possible measures are:

Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold).

Reducing the frequency of customer identification updates.

Reducing the degree of ongoing monitoring and scrutinising transactions based on a reasonable monetary threshold.

Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transaction or business relationship established.[11]

From the following, select the example that relates to your industry.

11. FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, updated March 2022: www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF% – accessed December 2021.

Example: Real estate agency

A real estate agency in the UAE is approached by a local retail business seeking to lease a small storefront. The retail business is a well-known, family-run operation that has been serving the local community for several years.

Given the local nature of the business, its long-standing presence, and the relatively low value of the lease, the risk of money laundering or other illicit activities is considered very low. Therefore, in this situation, the real estate agency can apply simplified due diligence.

This would involve basic verification of the retail business' registration details and the identities of the business owners. The real estate agency would not need to conduct extensive checks on the source of funds or ongoing monitoring of the business relationship due to the low risk.

However, the agency should still remain vigilant for any unusual or suspicious activities and be prepared to escalate to standard or enhanced due diligence measures if necessary.

Example: DPMS

A dealer in precious metals and stones in the UAE is approached by a local jeweller looking to purchase a small quantity of gold for their family-run business. The jeweller has been a part of the local community for several years and is well-respected.

Given the local nature of the business, its long-standing reputation, and the relatively low value of the purchase, the risk of money laundering or other illegal activities is considered very low. Therefore, in this situation, the dealer can apply simplified due diligence.

This would involve basic verification of the jeweller's business registration details and the identities of the business owners. The dealer would not need to conduct extensive checks on the source of funds or ongoing monitoring of the business relationship due to the low risk.

However, the dealer should still remain alert for any unusual or suspicious activities and be prepared to escalate to standard or enhanced due diligence measures if necessary.

Example: Accountants

An accounting firm in the UAE is approached by a local restaurant looking for assistance with their yearly tax filing. The restaurant is a well-known, family-run establishment that has been serving the local community for many years.

Given the local nature of the business, its long-standing reputation, and the relatively low value of the engagement, the risk of money laundering or other illicit activities is considered very low. Therefore, in this situation, the accounting firm can apply simplified due diligence.

This would involve basic verification of the restaurant's business registration details and the identities of the business owners. The accounting firm would not need to conduct extensive checks on the source of funds or ongoing monitoring of the business relationship due to the low risk.

However, the accounting firm should still remain vigilant for any unusual or suspicious activities and be prepared to escalate to standard or enhanced due diligence measures if necessary.

Example: CPS

A company service provider (CSP) in the UAE is approached by a local family-run grocery store seeking assistance with business registration renewal. The grocery store is a well-known, community-oriented operation that has been serving local residents for many years.

Given the local nature of the business, its long-standing reputation, and the relatively low value of the service, the risk of money laundering or other illicit activities is considered very low. Therefore, in this situation, the CSP can apply simplified due diligence.

This would involve basic verification of the grocery store's business registration details and the identities of the business owners. The CSP would not need to conduct extensive checks on the source of funds or ongoing monitoring of the business relationship due to the low risk.

However, the CSP should still remain vigilant for any unusual or suspicious activities and be prepared to escalate to standard or enhanced due diligence measures if necessary.

Important

Specific examples of situations which allow simplified due diligence to be applied may be outlined in legislation. For any other situations, it is important to note that any decision to apply simplified due diligence must be carefully documented and be justifiable in the eyes of the regulators.

In the UAE

As part of the risk-based approach to CDD, in some circumstances and where there is no suspicion of money laundering or terrorist financing, DNFBPs are able to apply simplified due diligence. This is only permitted with regards to customers identified as low risk through an adequate risk analysis.

Simplified due diligence, as discussed, generally involves a more lenient approach to certain areas of the CDD process, including:

- reduced verification requirements with regards to customer or beneficial owner identification
- fewer and less detailed inquiries with regards to the purpose of the business relationship, the nature of the customer's business, the customer's source of funds, and the purpose of individual transactions, and
- more limited supervision and reduced ongoing monitoring of the business relationship, as well as reduced frequency of reviewing/updating CDD information.

Section 2, Article (4) of the Cabinet Decision No. (10) of 2019 states with regards to simplified due diligence:

In case the requirements stipulated in Clauses (1 and 2) are met, the Financial Institutions and DNFBPs shall be permitted to apply simplified CDD measures to manage and limit the identified low risks, unless there is suspicion of a committed Crime. The simplified CDD measures should be commensurate with the low risk factors.

These include the following, as examples:

(a) Verifying the identity of the Customer and Beneficial Owner after establishing the business relationship.

(b) Updating the Customer's data based on less frequent intervals.

(c) Reducing the rate of ongoing monitoring and transaction checks.

(d) Concluding the purpose and nature of the business relationship based on the type of transactions or the business relationship that has been established, without the need to gather information or performing specific procedure.

What is enhanced due diligence?

Where high-risk clients or countries are involved, regulations will normally require you to go further than the standard identification (e.g., passport and utility bill).

Consider

The emergence of websites supplying fake documents, such as bank statements and utility bills, presents new challenges for verification.

Additional checks may be appropriate for high-risk clients and additional information must be collected to get a full picture of the individual or entity.

Example

As an example, source of wealth descriptions that are not acceptable include: 'savings', 'profits from investments', 'inheritance', 'business dealing' or 'sale of business' as they are insufficient proof that wealth is legitimate and not the product of criminal activity.

Additional information must be gathered to demonstrate that adequate due diligence has been undertaken. Further steps must sometimes be taken to gain assurance that wealth has not been obtained from criminal activity. In a case where the source of wealth is obvious (e.g., a monthly salary that is credited to the account), there is no further corroboration required.

There could also be instances where more detailed corroboration is required, such as client interviews, background checks and documentary evidence – all of which are valid approaches to corroborating the source of wealth and funds. In considering exactly what steps are appropriate, it is worthwhile considering how well, with hindsight, the following questions could be answered.

Questions

- Are you convinced that the funds and wealth can be reasonably explained and established to be legitimate?
- Can you independently obtain the evidence of the client's source of wealth for higher-risk accounts and relationships?
- Are you able to establish the relationship between the client and the third party where accounts are funded by a third party?
- Do you continue asking for information, and persist in seeking clarity wherever the circumstances are unclear or account structures are complex?

There is a wide array of sound practices to enable one to answer these questions and satisfy oneself that a customer's source of wealth has been corroborated. These could include:

- in-depth interviewing
- collection of documentary information, or
- reference to publicly available information from reliable sources.

Note

It is important to remember that CDD and **enhanced due diligence** are not 'tick-box' exercises. Every case, particularly high-risk cases requiring enhanced due diligence, must be risk assessed on its own merits and appropriate identification and verification of information must be obtained.

Let's look at how enhanced due diligence is typically applied.

Customer identification and verification

In an enhanced due diligence context, the verification of customer information will be performed using sources independent from the customer including, where necessary, certification by third parties or the use of more than one source of information.

The business activities of the customer will be investigated in more detail and verified independently, possibly including on-site visits. The profile of a corporate customer will include a more granular assessment of its client base and geographical footprint.

It may also include queries confirming a customer's good standing, and assessment of its internal policies and control environment, financial position, etc.

The customer's source of wealth will be established at a detailed level and verified to a degree.

Beneficial owners and controllers

The ownership structure of a corporate customer will be more closely scrutinised, including by:

- investigation of owners with ownership only slightly below the beneficial ownership threshold
- verification of the individual identities of beneficial owners
- assessment of the source of wealth of beneficial owners
- reputation checks on beneficial owners and controllers (an adverse media check)
- profiling of intermediate owners (nature of their business, location, reputation, etc.)
- verifying the individual identities of controllers, and
- verifying the controller's authority to act on behalf of the customer (e.g., by requiring a Certificate of Incumbency).

The enhanced due diligence process should identify any owners and controllers who are subject to sanctions, are PEPs and/or are subject to adverse media.

Nature and purpose of relationship

The purpose of the relationship will be documented in more detail than for standard CDD, including an assessment of the source of funds for the relationship, which will usually also be externally verified to a degree.

The expected levels of activity (volumes, amounts, frequency of transactions) will be assessed in more detail to support a more granular monitoring of the customer's activities.

Ongoing due diligence

Enhanced monitoring will typically include:

- a higher frequency of period reviews of the relationship, commonly every year
- a higher intensity of transaction monitoring (lower detection thresholds), and
- the individual approval of new products and services.

In some more extreme cases, the firm's rules may require the case-by-case approval of transactions.

Approvals

Owing to the higher levels of risk involved, the enhanced due diligence process will include:

- processes for senior management to review and approve high-risk relationships and mitigating measures
- the possible examination of the relationship by a customer acceptance committee, and
- the independent review and approval of the relationship by the firm's AML compliance function.

Recordkeeping

It is important to record KYC/CDD information in the form of a structured KYC file for clear and easy access. Here, we discuss how this information is organised in practice.

Recordkeeping requirements

Firms have a regulatory obligation to maintain customer records and to keep them for a minimum period of time after the end the customer relationship. In its **Recommendation 11**, FATF prescribes a minimum retention period of five years after the business relationship is ended, or after the date of the occasional transaction. As per the FATF Recommendation, it is a requirement for DNFBPs in the UAE to maintain records for a minimum period of five years under the AML-CFT Law. These records can be either physical or digital.

Failure to keep adequate KYC records creates significant risks for firms including:

- potential regulatory sanctions due to the inability to evidence application of proper CDD controls, resulting in financial and reputational damage
- inability to produce adequate records in the event of an investigation or production order, resulting in possible regulatory or criminal liabilities
- operational inefficiencies and poor use of the relationship manager's time, and
- repeated unnecessary contacts affecting the customer experience and commercial reputation of the firm.

KYC templates

A 'KYC template' is an industry-recognised term designating the form in which KYC data is held on the customer relationship as a product of CDD. In most instances, KYC records are held in electronic form as part of a **KYC system**, allowing safer recordkeeping and immediate access to large amounts of customer data for reporting or planning purposes.

Each of the following points will help us learn more.

Data points

A KYC template consists of a set of data points capturing specific customer information and typically includes:

- data fields, often based on a set of valid values (e.g., names, countries, business activities)

- questions about the customer or the relationship (e.g., whether there are known reputation issues with the customer; identifying the main markets in which the customer operates)
- narratives such as a summary of risks associated with the relationship, background comments on specific issues, rationale for approving the relationship, and
- signatures evidencing the review and acceptance of the KYC file by the relevant parties, such as the KYC analyst, relationship manager or MLRO, and any conditions attached thereto.

CDD elements

The KYC template contains all elements of CDD organised in a logical manner and suited to the customer types and business of the firm. These include:

- the identity and profile of the customer
- the purpose, nature and context of the relationship
- the identity of beneficial owners and controllers
- the results of customer screening
- the risk rating and assessment, and
- the approvals of the relationship.

Account opening form

In some instances, the account opening form filled out by the customer may serve as the initial part of the KYC template, which is then supplemented by the firm's own records and enquires. An example of this may be found in the retail environment, where most customer data is provided at the onset by the customers themselves. In this case, the firm focuses its CDD checks on independently verifying the accuracy of the information provided by the customer.

Records of communication

Let's now look at the communications that are preferred to be recorded.

What communications should be recorded in the KYC file?

The KYC file will also contain the records of all communications and notes produced during the CDD process, where relevant. These include:

- communications with the customer, including relevant representations or consents
- information and comments received from the RM, including those that result from escalations performed during the CDD process
- opinions and directions received from the MLRO during the CDD process
- records of telephone conversations where information obtained orally needs to be recorded in the KYC file, for example consulting the MLRO on a minor exception, and
- any other information of relevance to the outcome of CDD.

Why is this important?

Keeping adequate records of this correspondence enables the KYC file to carry the 'full story' and to substantiate the context and rationale for why and how decisions were made about the acceptance of the customer relationship.

This is particularly important because:

- it enables the firm to produce meaningful explanations as to why the customer was accepted into the firm, in the event of an examination or law enforcement request
- it supports a more effective periodic review of the customer relationship by allowing everyone involved to understand the thought process applied to the relationship during the initial onboarding or the last review, and
- it serves as a record of the decision-making process that may be applied to other customer relationships, for example where adverse media is analysed for an entire group of companies.

Documentary evidence

Finally, the KYC file contains all the documents used during the CDD process to identify and verify customer information and includes:

- documentary evidence supporting the verification of customer information (e.g., personal IDs, extracts of company registrar, audited accounts, regulator's webpage, offering memorandum)
- records of the screening of the customer and related parties; where large numbers of screening records exist, such as adverse media screening, a separate screening report may be created – including searches made which did not generate a response – to ensure full clarity of the screening outcome, and
- mandatory documents or representations from the customer, such as the original account opening form, questionnaires, tax forms or board resolutions related to specific products or facilities.

Politically exposed persons (PEPs)

One of the most prominent risks to have been highlighted over the past decade has been the risk posed by corrupt public officials and their associates and family members. There have been a number of damaging high-profile money laundering scandals involving PEPs.

The danger posed to DNFPBs by PEPs is simply that the business may be exposed to property that has been generated by corruption. Let's first determine what a PEP is.

Definition

The AML-CFT Law and the AML-CFT Decision define PEPs as:

Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any

prominent function within such an organisation; and the definition also includes the following:

1. *Direct family members (Of the PEP, who are spouses, children, spouses of children, parents).*
2. *Associates known to be close to the PEP, which include:*
   - *(a) Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP.*
   - *(b) Individuals having individual ownership rights in a legal person or arrangement established in favour of the PEP.*

(source: the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.)

Important

Knowing whether or not a client is a PEP is an essential element of CDD for all relationships. Once a business has ascertained that an existing or prospective client is a PEP it must then take the necessary action to reduce the associated risks. It is a regulatory obligation to carry out EDD when PEPs are involved in the customer relationship.

The most important CDD elements in mitigating the risk posed by PEPs are:

i. geography

ii. source of wealth

iii. source of funds, and

iv. commercial rationale for the arrangement/ relationship.

Requirements for PEPs in the UAE

The requirements for DNFBPs in relation to PEPs is outlined in the Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations.

Section 4 article 15:

1. In addition to undertaking CDD measures required under Section 3, Part 1 of this Chapter, Financial Institutions and DNFBPs shall be required to carry out the following:

First: ***For Foreign PEPs:***

(a) Put in place suitable risk management systems to determine whether a Customer or the Beneficial Owner is considered a PEP.

(b) Obtain senior management approval before establishing a business relationship, or continuing an existing one, with a PEP.

(c) Take reasonable measures to establish the source of funds of Customers and Beneficial Owners identified as PEPs.

(d) Conduct enhanced ongoing monitoring over such relationship.

Second: For ***Domestic PEPs*** *and individuals previously entrusted with prominent functions at international organisations:*

a. Take sufficient measures to identify whether the Customer or the Beneficial Owner is considered one of those persons

b. Take the measures identified in Clauses (b), (c), and (d) under the first paragraph of this Article, when there is a high-risk business relationship accompanying such persons.

DNFBPs are required to put in place appropriate risk management systems to determine whether a customer, Beneficial Owner, beneficiary, or controlling person is a PEP. As well as undertaking standard CDD procedures, DNFBPs are also required to take reasonable measures to establish the source of funds and the source of wealth of customers and Beneficial Owners identified as PEPs. In this regard, and commensurate with the nature and size of their businesses, DNFBPs should take measures that include:

- *Implementing (automated) screening systems which screen customer and transaction information for matches with known PEPs;*
- *Incorporating thorough background searches into their CDD procedures, using tools such as:*
  - *Manual internet search protocols;*
  - *Public or private databases;*

- *Publicly accessible or subscription information aggregation services;*
- *Commercially available background investigation services.*

If a customer, Beneficial Owner, beneficiary, or controlling person is identified as a PEP, DNFBPs must take appropriate measures to establish the PEP's source of funds and source of wealth. In addition, they should also evaluate the legitimacy of the source of funds and source of wealth, including making reasonable investigations into the individual's professional and financial background. Furthermore, DNFBPs are also required to obtain senior management approval before establishing a business relationship with a PEP, or before continuing an existing one. In regard to the latter, senior management should be notified and their approval should be obtained for the continuance of a PEP relationship each time any of the following situations occur:

- *An existing customer, Beneficial Owner, beneficiary, or controlling person becomes, or is newly identified as, a PEP;*
- *An existing PEP Business Relationship is reviewed and the CDD information is updated, either on a periodic or an interim basis, according to the organisation's internal policies and procedures;*
- *A material transaction that appears unusual or illogical for the PEP Business Relationship is identified;*
- *The beneficiary or Beneficial Owner of a life insurance policy or family takaful insurance policy is identified as a PEP, and in case higher risks are identified, the overall Business Relationship should also be thoroughly examined and consideration given to filing an STR. Senior management should be informed before the payout of the policy proceeds.*

Those individuals identified as Domestic PEPs or individuals who were previously (but are no longer) entrusted with prominent functions at international organisations, the AML-CFT Decision states that DNFBPs should implement the measures previously described, apart from their PEP status, the business relationships associated with such persons could be classified as high-risk for any other reason.

Customers who are no longer entrusted with a prominent public function should be subject to an assessment of risk.

This risk-based approach requires that DNFBPs assess the ML/FT risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk.

Possible risk factors include:

- *the level of (informal) influence that the individual could still exercise;*
- *the seniority of the position that the individual held as a PEP; or*
- *whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).*

(source: Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations)

Important

It is important to note that if a PEP, whether domestic or foreign, refuses to provide CDD documentation, or provides documentation that is false, misleading, fraudulent or forged, you should not enter into a business relationship, and a report should be submitted to the FIU via the GoAML system.

High-profile cases and increasing scrutiny

Concerns over PEPs arose initially in the context of high-profile cases of corrupt heads of state and dictators who were syphoning off their country's resources for their personal benefit, and hiding their stolen wealth in Western private banks. Firms found dealing with such proceeds of crime expose themselves to considerable reputational, legal and financial risks.

As international efforts have been stepped up in the global fight against corruption in parallel with AML/CFT measures, the scrutiny over PEPs has become a key feature of CDD requirements across all regulated activities, and the definition of PEPs now includes domestic PEPs.

Example: Former Malaysian Prime Minister

Former Malaysian Prime Minister Najib Razak embezzled billions of dollars from a government-owned investment fund intended to be spent on boosting Malaysia's economic development. Instead, the stolen funds were spent on high-end overseas real estate, private jets and luxury goods.

Goldman Sachs, which helped raise $6.5 billion for the development fund, agreed a $3.9 billion settlement with the Malaysian government for the role it played.

Goldman Sachs suffered further reputational damage after 12 of its executives were charged by Malaysian authorities for their handling of the funds. AmBank, which held three accounts belonging to the ex-Prime Minister, was involved in the same scandal. AmBank agreed to pay a $700 million fine settlement for their failings.

The case demonstrates the importance of effective due diligence and risk management controls to prevent money being laundered, particularly regarding PEPs.

(Forbes, 2022)

High-risk countries/jurisdictions

High-risk countries or jurisdictions are those identified as posing a greater AML/CFT threat.

Extract FATF

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation. For all countries identified as high-risk, the FATF calls on all members and urges all jurisdictions to apply enhanced due diligence, and, in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country. This list is often externally referred to as the "black list".

(source: High-Risk Jurisdictions subject to a Call for Action – February 2024)

Financial institutions and DNFBPs are required under Decree Law No. 20 of 2018 on Anti-Money Laundering , and Combating the Financing of Terrorism and the Financing of illegal organizations to:

1. *implement enhanced customer due diligence (CDD) measures proportionate to the risk level that might arise from business relationships and transactions with natural or legal persons from High-Risk Countries*
2. *implement the countermeasures as defined by the Committee regarding High-Risk Countries.*

It is a requirement for all DNFBPs to verify and review the lists and information issued by FATF and the National Committee for Combating Money Laundering and the Financing of Terrorism and Illegal Organizations, as amended and current at that time, on a regular basis, and shall take such lists and information into account when establishing and implementing the required countermeasures and/or enhanced due diligence measures, as appropriate, and proportionate to the level of risks. DNFBPs are also required to re-evaluate the implementation of due diligence measures consistent with the degree of risks, in respect of countries whose names have been removed from those lists by FATF.

Counter measures for high-risk countries

DNFBPs must apply enhanced due diligence measures to all business relationships and transactions with jurisdictions on the Black List, including natural persons and legal entities and those acting on their behalf, in addition to the countermeasures listed below:

1. *Supervisory authorities shall prohibit the establishment of any branches or representative offices for FIs, DNFBPs, and Virtual Assets Service providers subject to its supervision within jurisdictions on the Black List.*
2. *All FIs, DNFBPs, and Virtual Assets Service providers and non profit organisations shall comply with their internal reporting mechanisms on monitoring transactions and activities pertaining to jurisdictions on the Black List, and submit suspicious transaction reporting to the FIU where relevant, using the existing template pertaining to jurisdictions on the Black List reports in GoAML (High Risk Jurisdiction and High Risk Jurisdiction Activity).*

3. *All supervisory authorities in the UAE shall impose increased monitoring and supervisory examination for financial groups with respect to any of their branches and subsidiaries located jurisdictions on the Black List.*
4. *All FIs, DNFBPs, and Virtual Assets Service providers and NPOs are prohibited from relying on third parties located in jurisdictions on the Black List to perform their due diligence procedures.*
5. *All supervisory authorities in the UAE shall remind all FIs, DNFBPs, and Virtual Assets Service providers of the requirement to implement targeted financial sanctions requirements in accordance with applicable UN Security Council Resolutions and CABINET DECISION NO. (74) of 2020, to protect financial and non-financial sectors in the UAE from ML, TF, and proliferation financing risks.*
6. *All supervisory authorities in the UAE must take legal action against FIs, DNFBPs, and Virtual Asset Service Providers, including their directors and senior management, in the event of failure to implement the measures stipulated in this decision.*

(source and a list of FATF high-risk jurisdictions)

Jurisdictions under increased monitoring

Jurisdictions under increased monitoring work actively with FATF to address strategic deficiencies in their regimes to counter money laundering, terrorism financing, and proliferation financing. When FATF places a jurisdiction under increased monitoring, it means the country has committed to resolving the identified strategic deficiencies swiftly within agreed timeframes and is subject to increased monitoring. This list is often externally referred to as the 'FATF grey list'.

DNFBPs in the UAE are required to regularly review the grey list and weaknesses identified in it, and take these into account when devising and applying risk-based compliance measures. Due diligence measures taken by DNFBPs should be proportionate to the risks posed from business relationships and transactions with natural or legal persons from such jurisdictions, and ultimately should be effective in minimising such risks. The measures taken may require the application of enhanced due diligence depending on the circumstances referred to in paragraph 20 to the interpretive note of Recommendation 10 as well as Article (4) of the 2019 Cabinet Decision.

A list of jurisdictions under increased monitoring by FATF can be found by selecting this link.

Counter-measures for countries under increased monitoring:

Financial institutions, DNFBPs, VASPs and non-profit organisations in the UAE shall on a regular basis review the grey list and weaknesses identified in it, and take them into account when devising and applying risk-based compliance measures.

Due diligence measures taken by FIs, DNFBPs, and VASPs providers and non-profit organisations shall in all cases be proportionate to the risks posed from business relationships and transactions with natural or legal persons from such jurisdictions and be effective to minimise such risks. The measures taken may require the application of enhanced due diligence depending on the circumstances referred to in paragraph 20 to the interpretive note of Recommendation 10 as well as Article (4) of the 2019 Cabinet Decision.

(www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2024.html)

KYC/CDD quick recap

The KYC/CDD process can be complex, and we have covered a lot in this unit. Let's quickly recap the key components of the KYC/CDD process.

1. *Gather and verify customer information – You must verify the identity of the customer and obtain an understanding of the intended nature of the proposed business relationship and the nature of a customer's business.*
2. *Risk rating – You must develop an adequate customer risk assessment framework to be able to assign risk ratings to your customers.*
3. *Customer due diligence – You must conduct adequate due diligence on your customers, which should include screening your customers for potential adverse media and against sanctions lists.*
4. *Onboarding – If concerns arise regarding your customer at the onboarding stage, such as refusing to provide adequate KYC information or necessary documentation, your compliance officer or MLRO must consider rejecting*

the application and recording the findings of the due diligence review.

5. *Enhanced due diligence – You must conduct Enhanced CDD on customers posing a higher risk of money laundering, which includes PEPs and PEP associates. Just because an individual is a PEP it does not automatically mean that the individual must be assigned a 'high risk' rating. However, you must conduct a thorough assessment to determine your customer's risk category.*
6. *Ongoing/periodic reviews – You must conduct periodic reviews of your customers throughout the relationship. The frequency of your periodic reviews depends on the risk rating assigned to your customer or any trigger event, as applicable.*
7. *SARs/STRs reporting – You must report an STR/SAR to the UAE FIU via the goAML system when you become suspicious of a transaction or an activity made by your customer.*

Source: www.adgm.com/documents/registration-authority/dnfbps/quick-guide-1-know-your-customer-kyc-20230920.pdf

End of Unit Learning Outcomes Summary Guide Animation

Self-assessment questions

Congratulations, you have reached the end of Unit 3. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, **continue** or alternatively, you can work through the section again if you wish.

1. What is the purpose of CDD in AML practices?
    a) To identify and assess the risks a business might face in terms of money laundering and terrorist financing
    b) To ensure the business complies with tax regulations
    c) To prevent fraudulent activities within the business
    d) To evaluate the creditworthiness of the customers
2. According to the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations, what does the term 'politically exposed persons (PEPs)' refer to?
    a) Individuals who are or have been entrusted with prominent public functions
    b) Individuals involved in political activism
    c) Individuals who are politically influential
    d) Individuals holding high-ranking positions in political parties
3. In the context of an AML self-risk assessment, which of the following is NOT a key component of enhanced due diligence?
    a) Customer identification and verification
    b) Nature and purpose of relationship
    c) Beneficial owners and controllers
    d) Transaction volume prediction

Correct answers 1a, 2a, 3d

Unit 4: Reporting Obligations

Learning Objectives

The purpose of this learning material is to:

- detail the role of transaction monitoring and investigations in an effective AML programme
- explain the process for reporting SARs and STRs
- examine the need for recordkeeping, and
- discuss the various red flags for DNFBPs.

Transaction monitoring and investigations

Transaction monitoring and investigations play a crucial role in the AML compliance programmes of DNFBPs. These practices are essential for detecting suspicious activities, identifying potential risks, and ensuring compliance with regulatory obligations.

Transaction monitoring involves the ongoing scrutiny of customer transactions to identify patterns or activities that may suggest money laundering or terrorist financing. It's not just about monitoring large transactions, but also understanding the normal transaction patterns for each customer to identify any deviations from the norm. Anomalies such as frequent high-value transactions, rapid movement of funds, or transactions with high-risk countries could all be potential red flags.

When suspicious activity is detected, it triggers an investigation process. Investigations involve a deep dive into the transactions in question to uncover the source of funds, the nature of the transaction and the parties involved. This could involve reviewing customer records, analysing transaction patterns and cross-checking information with external databases.

For DNFBPs, transaction monitoring and investigations can present unique challenges. These businesses may deal with complex transactions, high-value assets and a diverse range of clients, all of which can increase the risk of money laundering.

Therefore DNFBPs need to have robust systems in place for transaction monitoring and investigations. This includes trained personnel, effective risk assessment processes, and advanced technological tools. Automated systems can help in detecting suspicious patterns in large volumes of transactions, while machine learning algorithms can adapt and improve over time to recognise new patterns of illicit activity.

Transaction monitoring and investigation requirements in the UAE

DNFBPs are expected to conduct ongoing business monitoring and examinations of transactions in order to identify unusual or suspicious activity.

In 2022, the national Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee conducted a Suspicious Activity and Transaction Reporting Thematic Review, which outlined transaction monitoring and investigation expectations for DNFBPs. Let's explore some of the key expectations identified in the review.

Risk-based deployment of transaction monitoring controls

DNFBPs should maintain a transaction monitoring programme based on an underlying AML/CFT risk-based assessment. The programme should take into account the AML/CFT risks of the DNFBPs:

- customers
- prospective customers
- counterparties
- businesses
- products
- services
- delivery channels, and
- geographic markets.

Additionally, the components of the transaction monitoring programme should be able to prioritise high-risk alerts.

DFNBPs with a larger scale of operations are expected to have in place automated systems capable of handling the risks from an increased volume and variance of transactions. DFNBPs utilising automated systems should:

1. Perform a typology assessment to design appropriate rule- or scenario-based automated monitoring capabilities and processes. This should include risks outlined in the National Risk Assessment and other typology reports circulated by the supervisory authorities.
2. Employ quantifiable parameters that are tailored to the institution's risk profile and the specific product, service, and customer types involved in the transaction.
3. Implement risk-based customer and product segmentation, so that rule parameters and thresholds are appropriately calibrated to the type of activity subject to transaction monitoring.
4. Utilise statistical tools or methods such as above-the-line and below-the-line testing; this involves increasing and decreasing the pre-determined thresholds of transaction monitoring rules in a testing environment and measuring the resulting output to better fine-tune their calibrations and reduce the volume of false-positive alerts.
5. Where automated systems are employed, DNFBPs should perform pre-implementation testing of transaction monitoring systems using historical transaction data, as appropriate.
6. System testing should cover compatibility of the transaction monitoring and core (source) systems with each other and with the overall AML/CFT and sanctions compliance infrastructure. Such testing is to ensure that the system performs as intended.

Data identification and management

- DNFBPs should identify and document all data sources that serve as inputs to their transaction monitoring programme, including internal customer databases, core- system, or other transaction processing systems, and external sources such as SWIFT message data.
- Where automated transaction monitoring systems are used, DNFBPs should institute data extraction

and loading processes to ensure complete, accurate, and traceable data flows from their source to the transaction monitoring system.

- Both prior to initial deployment and at risk-based intervals thereafter, LFIs and DNFBPs should test and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data is flowing into the transaction monitoring system.
- Data testing and validation should typically occur every 12 to 18 months or earlier as deemed appropriate based on the outcomes the money laundering/terrorist financing risk assessment, risk appetite and any ad-hoc internal and external factor(s). Moreover, the frequency of such activities should be clearly documented.
- Such testing can include data integrity checks to ensure that data is being completely and accurately captured in source systems and transmitted to the transaction monitoring system, as well as to ensure the reconciliation of transaction codes across core systems and transaction monitoring system.
- DNFBPs should place appropriate detection controls, such as the analysis of trends observable through management information. They should also generate exception reports in order to identify abnormally functioning transaction monitoring rules or scenarios.

Alert review, case investigation and STR/SAR decision making

DNFBPs must ensure that an efficient alert management and disposition process is in place, whether automated or manual. This assists law enforcement in the identification and investigation of criminal activity, and satisfies regulatory expectations concerning timely suspicious activity reporting. The alert management and dispositioning process should be adequately staffed and should include a process for the expedited filing of urgent reports for select cases.

Firms must also ensure the following.

- DNFBP employees should review an alert and determine whether further investigation is warranted. The underlying basis for the determination should be documented in accordance with the DNFBP's investigation procedure.
- Where the facts available at the alert review stage are or may be sufficient enough to warrant a suspicious transaction report (STR) or suspicious activity report (SAR) filing without further investigation, or where the transaction may otherwise require immediate attention, employees should immediately escalate the alerted activity to the designated STR or SAR decisioning authority (i.e., the compliance officer or the MLRO in this case) for expedited review.
- For any alerted activity deemed to require further investigation, employees should conduct and complete (at least a preliminary) investigation of the alerted activity, document the results of any research or analysis performed, and make a recommendation as to whether an STR or SAR should be filed.
- Where a case investigator becomes aware of activity that requires immediate attention, employees should immediately escalate the activity to the designated STR or SAR decisioning authority (i.e., the compliance officer or the MLRO in this case) for expedited review. The compliance officer or MLRO must maintain records of decisions made.
- In the event of escalation for expedited review, the compliance officer or the MLRO should review the activity and make a determination as to whether or not it is suspicious within 24 hours from the time of escalation and should file an STR or SAR to the FIU accordingly. Where appropriate, the compliance officer or the MLRO should also escalate the activity for potential exit, account closure, and internal watchlist addition.
- DNFBPs needs to evaluate continuing the relationship (except in the cases related to narcotics/terrorism) with the customer by placing enhanced monitoring controls based on the nature of concern and their own risk appetite.

We shall explore some of the further triggers and requirements for suspicious activity reporting as we progress.

Reporting SAR and STR obligations

The duty to report suspicious activity and transactions, including possible terrorist financing activity, rests with every employee within the financial sector, the professions and a number of non-financial businesses.

Let's first take a look at the similarities and differences between SARs and STRs.

An SAR and an STR are both tools used in financial institutions and DNFBPs to report suspicious or potentially illegal activities.

The main difference between the two lies in their usage across different regions and jurisdictions. In the UAE, the term SAR is commonly used when financial institutions/DNFBPs identify and report any suspicious activity that might indicate money laundering, fraud or other financial crimes, such as the insistence on involving too many intermediaries, or refusal to provide KYC documents.

On the other hand, STR is the term more commonly used in international contexts, particularly by FATF. An STR is a report made by a financial institution/DNFBP about suspicious or potentially suspicious activity, including transactions that are inconsistent with a customer's known legitimate business or personal activities.

Despite the different terms, both SAR and STR serve the same fundamental purpose – to alert authorities about activities that could be related to financial crime.

SAR

- Relates to: suspicious activities or actions performed by the customer
- Scenarios: proposed customer activity or proposed but non-executed transactions
- Reporting requirement: a SAR should be submitted

Examples:

- insistence on involving multiple or too many intermediaries

- proposed customer is associated to a sanctioned individual
- insistence on secrecy lack of rationale
- transaction proposed on behalf of an undisclosed individual, and
- conducting business without the necessary license.

STR

- Relates to: suspicious flow of funds, transactions, deposits/withdrawals etc
- Scenarios: conducting a transaction, establishing a business relationships
- Reporting requirement: a STR should be submitted

Examples:

- multiple transactions conducted in a short period
- transaction not in line with customer profile
- last minute changes in transaction parameters, and
- customer insists on payment via virtual currencies.

What is suspicious activity?

Any possible suspicious activity must be reported as set out in your own organisation's policy and procedure on reporting.

Examples: Suspicious activity

Common examples of suspicious activity may include:

- a transaction that is unusually large given what we know about the client
- an activity or type of transaction that deviates from that normally seen on the client's account, or compared to similar profiles of other customers, or
- an inconsistency or discrepancies in the CDD provided.

The subjective test of suspicion

The Oxford English Dictionary defines suspicion as:

An act of suspecting, the imagining of something without evidence or on slender evidence, inkling, mistrust.

Suspicion has been defined as being beyond mere speculation and based on some foundation, i.e., 'a degree of satisfaction not necessarily amounting to belief but at least extending beyond speculation as to whether an event has occurred or not' and 'although the creation of suspicion requires a lesser factual basis than the creation of a belief, it should nonetheless be built upon some foundation'.

Suspicion is therefore normally described as personal and subjective, falling far short of proof based upon firm evidence. It is unique to the individual experiencing it and cannot be objectively prescribed. This is known as the subjective test of suspicion.

Many legal frameworks however define suspicion in an additional context – this is summarised in the next subsection.

Reasonable grounds to suspect: The objective test of suspicion

The requirement to report when there are reasonable grounds to suspect that a person is engaged in money laundering/terrorist financing introduces an objective test. The test would probably be met when there are facts or circumstances known to the employee concerned from which another person engaged in a similar business and in similar circumstances would have formed a suspicion that a person was engaged in money laundering or terrorist financing.

The concept of 'reasonable grounds to suspect' is likely to include not only negligence but also the concept of wilful blindness, i.e., the intentional and deliberate avoidance of the facts.

Example

Wilful blindness could involve proceeding with a transaction or institution while deliberately 'turning a blind eye' to the potentially illegal origin of the funds involved.

The introduction of the objective test has had an important impact upon internal procedures for recognising and reporting suspicions and upon training. Under the subjective test, a prosecutor has to prove that the individual/institution clearly knew or suspected. Under the objective test however, a prosecutor needs to satisfy a lower threshold by demonstrating only that an individual ought to have known or suspected. In order to avoid the increased risk posed by the objective test MLROs should carefully consider the extent of monitoring, the extent of enquiry and the extent of documentary records required.

To defend themselves against a charge that they failed to meet the objective test of suspicion, employees may need to demonstrate that they took all reasonable steps in the context of a risk- based approach, to know the customer and the rationale for the transaction, activity or instruction.

Reporting suspicion

Unusual behaviour or activity can arise at any time during a customer relationship. This gives rise to a legal as well as procedural requirement to report concerns – applying to all staff within the firm regardless of their role. For evidential reasons it is necessary for internal suspicion reports to be made in writing, as this will provide an employee with statutory protection, especially where the suspicion is set aside by the MLRO. If the report was made verbally, an employee would not be able to defend or rebut an allegation that they did not discharge their legal obligation by making a suspicion report. Written reports are also necessary to enable the data on internal reports to be collated when preparing reports to senior management.

Note

As we have discussed previously, in the UAE a SAR should be submitted when there are concerns over a customer's behaviour, actions or a proposed but non-executed transaction. If there are concerns over a transaction, an STR should be submitted.

Anonymity for staff in making an SAR is crucial to ensure that all suspicions are reported.

If staff fear that their names will be disclosed, then possible criminal activity may go unreported. It is therefore crucial

that the name of the member of staff who submitted the report is not included when the report is passed to the authorities. Only the nominated officer's or/MLRO's name should be given as the contact point on behalf of the reporting institution.

Reason for reporting

A very important feature of an effective internal reporting system is the requirement for employees to provide reasons for their suspicion. Standard internal report forms completed by employees should always include a section requiring staff to outline their reasons for making a report.

Contrast the two following scenarios.

Scenario One

A makes a report about X. The report is premised on A's suspicion that X is evading tax, but A provides no reasons for their suspicion.

Scenario Two

B makes a report about Y. The report is premised upon B's suspicion that Y is evading tax and that the money held by their employer is undeclared. B substantiates their suspicion with reference to:

- a conversation that they had with Y in which Y hinted that the revenue authorities were unaware of the money that had been deposited offshore and should remain so, and
- their belief that there was no legitimate commercial advantage to Y in holding the money offshore.

The advantages of the report in Scenario Two are obvious. Nevertheless, it is important to recognise that every suspicion report, however it is formed, has the potential to be valuable and that if sufficient information is not currently being provided, this can be addressed through effective training. All reports should be appropriately evaluated.

While it is impossible to list all the indicators of suspicion here, a few examples of potentially suspicious transaction types that DNFBPs should take into consideration and deem as potential reasons to report include:

- *transactions or series of transactions that appear to be unnecessarily complex, that make it difficult to identify the Beneficial Owner, or that do not appear to have an economic or commercial rationale numbers, sizes, or types of transactions that appear to be inconsistent with the customer's expected activity and/or previous activity*
- *transactions that appear to be exceptionally large in relation to a customer's declared income or turnover*
- *large unexplained cash amounts, especially when they are inconsistent with the nature of the customer's business*
- *loan repayments that appear to be inconsistent with a customer's declared income or turnover*
- *early repayment of a loan followed by an application for another loan*
- *third-party loan agreements, especially when there are amendments to or assignments of the loan agreement*
- *requests for third-party payments, including those involving transactions related to loans, investments, or insurance policies*
- *transactions involving high-risk countries, including those involving "own funds" transfers, particularly in circumstances in which there are no clear reasons for the specific transaction routing*
- *frequent or unexplained changes in ownership or management of Business Relationships*
- *illogical changes in business activities, especially where high-risk activities are involved*
- *situations in which CDD measures cannot be performed, such as when the customers or Beneficial Owners refuse to provide CDD documentation, or provide documentation that is false, misleading, fraudulent or forged.*

(Source: www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf/0557c726-d8a7-ea63-594b-10110e300dc8?t=1633853458984)

Reporting requirements in the UAE

The Central Bank of UAE (CBUAE) first established a specific unit dedicated to investigating illicit activity such as financial crimes, frauds and suspicious transactions in

1998. This unit acted as a unique institution that prevented money laundering and terrorist financing activities. In 2002, it was renamed the Anti-Money Laundering and Suspicious Cases Unit (AMLSCU), and in 2018, after the UAE government introduced the Federal Decree-Law No. 20 on AML/CFT, the unit was renamed the Financial Intelligence Unit. All suspicious activity is reported to the FIU through the 'goAML' portal. (source: www.uaefiu.gov.ae/en/)

Section 5 of the Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. 20 details STR requirements for DNFBPs, as detailed in the following.

Article (16)

Financial Institutions and DNFBPs shall put in place indicators that can be used to identify the suspicion on the occurrence of the Crime in order to report STRs, and shall update these indicators on an ongoing basis, as required, in accordance with the development and diversity of the methods used for committing such crimes, whilst complying with what the Supervisory Authorities or FIU may issue instructions in this regard.

Article (17)

1. *If Financial Institutions and DNFBPs have reasonable grounds to suspect that a Transaction, attempted Transaction, or funds constitute crime proceeds in whole or in part, or are related to the Crime or intended to be used in such activity, regardless of the amount, they shall adhere to the following without invoking bank secrecy or professional or contractual secrecy:*
    - *(a) Directly report STRs to the FIU without any delay, via the electronic system of the FIU or by any other means approved by the FIU*
    - *(b) Respond to all additional information requested by the FIU.*
2. *Lawyers, notary publics, other legal stakeholders and independent legal auditors shall be exempt from Clause (1) of this Article, if obtaining this information regarding such Transactions relates to the assessment of their Customers' legal position, or defending or representing them before judiciary authorities or in arbitration or mediation, or providing legal opinion with regards to legal proceedings, including providing consultation concerning the initiation or avoidance of*

such proceedings, whether the information was obtained before or during the legal proceedings, or after their completion, or in other circumstances where such Customers are subject to professional secrecy.

3. *Financial Institutions and DNFBPs, their board members, employees and authorised representatives shall not be legally liable for any administrative, civil or criminal liability for reporting when reporting to the Unit or providing information in good faith.*

In March 2021, The Ministry of Economy released a Circular (No. 5 2021) to DNFBPs outlining their requirements to register on the 'goAML' system. It states:

All Suspicious Transaction Reports ("STRs") are to be submitted to the FIU using the 'goAML' portal. Registration on the 'goAML' portal is mandatory for all Relevant Persons including Designated Non-Financial Businesses ("DNFBPs").

The full circular can be viewed by selecting this link.

Let's now take a look at some specific reporting requirements for different DNFBP sectors.

Dealers in precious metals and stones

Dealers in precious metals and stones must undertake the following procedures effective 12 June 2021:

1. *Transactions with resident individuals: Obtain identification documents (Emirates ID or Passport) for cash transactions equal to or exceeding AED 55,000 and register the information in the Financial Intelligence Unit's ("FIU") GoAML platform using the recently created 'Dealers in Precious Metals and Stones Report' (DPMSR).*
2. *Transactions with non-resident individuals: Obtain identification documents (ID or Passport) for cash transactions equal to or exceeding AED 55,000, and register the information in the FIU's GoAML platform using the newly created DPMSR.*
3. *Transactions with entities / companies: Obtain a copy of the trade license, and identification documents (Emirates ID or passport) of the person representing the company, in transactions equal to or exceeding AED 55,000 in cash or through wire transfer, and register the information in the FIU's GoAML using the newly created DPMSR.*
4. *Keep records of all documents and information related to the above transactions for a minimum period of 5 years.*

Real estate brokers and agents licensed in the UAE

The Ministry of Economy instructs all real estate brokers and agents to undertake the following procedures effective 1 July 2022:

1. *Purchase and sale transactions of Freehold real estate, according to the description and determination of the law of each emirate, in carrying out any single physical cash transaction or several transactions equal or exceeding AED 55,000 for the entire, or a portion, of the property value:*
    a. *Obtain and record identification documents (Emirates ID, or Passport copy).*
    b. *Obtain and record receipts, invoices, contracts and Purchase & Sale Agreement.*
    c. *Submit a 'Real Estate Transaction Report' ("REAR") via the Financial Intelligence Unit's ("FIU") goAML platform.*
2. *Purchase and sale transactions of Freehold real estate where the method of payment is a virtual asset for a portion or the entire property value:*
    a. *Obtain and record identification documents (Emirates ID, or Passport copy).*
    b. *Obtain and record receipts, invoices, contracts and Purchase & Sale Agreement.*
    c. *Submit a 'Real Estate Transaction Report' ("REAR") via the Financial Intelligence Unit's ("FIU") goAML platform.*
3. *Purchase and sale transactions of Freehold real estate where the funds used to carry out the transaction were converted from a virtual asset for a portion or the entire property value:*
    a. *Obtain and record identification documents (Emirates ID, Passport).*
    b. *Obtain and record receipts, invoices, contracts and Purchase & Sale Agreement.*
    c. *Submit a 'Real Estate Transaction Report' ("REAR") via the Financial Intelligence Unit's ("FIU") goAML platform.*

4. *If the buyer or seller are legal person(s), identification documents must include the following:*
    a. *Trade License;*
    b. *Articles of Association;*
    c. *Register of Beneficial Owners;*
    d. *Emirates ID or passport copy for all Beneficial Owners; and*
    e. *Emirates ID or passport copy for all shareholders/partners.*
5. *If the buyer or seller are natural person(s), identification documents must include the following:*
    a. *Valid Emirates ID or Passport copy.*
6. *Keep records of all documents and information related to the above transactions for minimum period of (5) years.*
7. *Note that submissions of REARs does not exempt you from your existing obligations to submit the following types of reports via goAML:*
    a. *Suspicious Transaction Report (STR);*
    b. *Suspicious Activity Report (SAR);*
    c. *Funds Freeze Report (FFR);*
    d. *Partial Name Match Report (PNMR);*
    e. *High Risk Country Report (HRC); and*
    f. *High Risk Country Activity Report (HRCA).*

When reporting an STR in the goAML system, the user is required to select the most appropriate reason for reporting available from the menu selection provided. More than one reason may also be provided, if deemed necessary. In order to select the appropriate indicator, click 'Add' to select the appropriate reason for the report. It is imperative that a minimum of one reason for reporting must be selected to avoid rejection of the report by the goAML system.

Timing of STRs

DNFBPs are obliged to report STRs to the FIU without delay. Since it is the responsibility of the designated AML/CFT compliance officer to "review, scrutinise and study records, receive data concerning suspicious transactions, and take decisions to either notify the FIU or maintain the transaction,"

it follows that the STRs should be immediately reported once the suspicious nature of the transaction becomes clear. This means that the internal reporting of suspicious transactions to the compliance officer should be done directly once the suspicion or reasonable grounds for suspicion are established, and immediately the designated AML/CFT compliance officer has confirmed that the transaction (whether pending, in progress, or past) is suspicious, it should be reported.

[DNFBPs should note that], *with the exception of any obligatory indicators for which immediate reporting to the FIU is required by the relevant Competent Authorities, some potentially suspicious transactions or indicators of suspicion may require a degree of internal investigation before a suspicion or reasonable grounds for suspicion are established and an internal STR is reported to the designated AML/CFT compliance officer. The DNFBP should however be able to demonstrate that this investigation is started immediately and has been ongoing continuously until the transaction is reported to the FIU.*

(www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf)

Sanctions against persons violating reporting obligations

The AML-CFT Law provides for the following sanctions against any DNFBPs, their managers or their employees, who fail to perform, whether purposely or through gross negligence, their statutory obligation to report a suspicion of money laundering or the financing of terrorism or of illegal organisations:

- *Imprisonment and fine of no less than AED100,000 and no more than AED1,000,000; or*
- *Any of these two sanctions. According to Article 15 of the AML-CFT Law, the requirement to report is in the case of suspicion or reasonable grounds to suspect a Crime. It should also be noted that the transactions or funds that are the subject of the suspicion may represent only part of the proceeds of the criminal offence, regardless of their value.*

Likewise, the AML-CFT Law provides for sanctions against anyone who warns or notifies a person of a suspicious

transaction report or reveals that a transaction is under review or investigation by the Competent Authorities, as follows:

- *Imprisonment for no less than six months and a penalty of no less than AED100,000 and no more than AED500,000; or*
- *Any of these two sanctions.*

(Source: www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf)

Tipping off

Let's begin by defining tipping off.

Definition: Tipping off

The offence of tipping off is committed by a person who discloses information that is likely to prejudice an actual or a proposed investigation. This can be either before or after an SAR/STR is made to law enforcement, and includes circumstances where the offender knows or suspects that there is either an investigation or a proposed investigation or that a disclosure has been made to law enforcement.

The offence is widely misunderstood. It is often mistakenly assumed that enquiries should not be made of clients at the time that a concern is first developed for fear that such enquiries might expose an employee to tipping the client off. **This is not the case**.

While enquiries must be handled with care, an employee will only be in danger of committing a tipping off offence if they either know that a report has been made or know that an investigation is underway or is planned, and they tell the client about this. This should never be the case at the stage before a suspicion is formulated.

Tipping off does, however, become a very real danger once an SAR/STR is made to law enforcement, after which all communications between a DNFBP, its employees and suspected clients must be handled with care. Again, it does not mean you cannot talk to the client, but conversations must not include the topic of the investigation or SAR. All employees should look for guidance from either the MLRO or from management on how to deal with suspect clients.

Tipping off in the UAE

The offence of tipping off in the UAE is detailed in Section 5 of the Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. 20. It states the following:

Article (18)

1. *Financial Institutions and DNFBPs, their managers, officials or staff, shall not disclose, directly or indirectly, to the Customer or any other person(s) that they have reported, or are intending to report a Suspicious Transaction, nor shall they disclose the information or data contained therein, or that an investigation is being conducted in that regard.*
2. *When lawyers, notaries, other independent legal professionals, and legal independent auditors attempt to discourage their Customers from committing a violation, they shall not be considered to have made a disclosure.*

Recordkeeping

Keeping accurate and comprehensive records of SARs/STRs is a regulatory requirement across the globe. The first requirement in recordkeeping is that the firm must retain a copy of any SAR/STR filed and the original or business record equivalent of any supporting documentation. This includes any documents that assisted in the identification of suspicious activity, such as:

- transaction records
- customer identification data, and
- the results of any analysis conducted.

The next requirement is the duration of storage. Typically, SARs/STRs and their supporting documentation must be retained for a minimum of five years from the date of filing. However, this can vary depending on the jurisdiction, so firms must be aware of the specific requirements in their region. In the UAE, DNFBPs are required to retain all records for a minimum of five years.

It is important that the records are stored and organised in a manner that allows them to be retrieved easily when requested by the appropriate authorities. This means that the firm needs to have a robust recordkeeping system in place that allows for prompt retrieval of SAR/STR records and supporting documentation.

The confidentiality of SAR/STR records is a paramount concern. Firms must ensure that these records are stored securely to prevent unauthorised access. Only authorised personnel should be allowed to access these records, and there should be strict controls and monitoring of access to such information.

In addition to these requirements, firms should also document their decision-making processes when deciding not to file an SAR/STR in response to a flagged suspicious transaction. This would serve as evidence that the institution has taken appropriate steps to investigate the transaction and determined that it was not necessary to file an SAR/STR.

The recordkeeping process is subject to regular audits and reviews by regulatory bodies. Non-compliance with recordkeeping requirements can result in heavy penalties and sanctions. Therefore, it is crucial for financial institutions to have a comprehensive and robust system for maintaining SAR/STR records.

Regulatory authorities, such as FATF have detailed guidelines concerning the recordkeeping requirements for SARs/STRs. These guidelines are designed to ensure that in the event of an investigation, all relevant information is readily available and can be accessed swiftly.

Recordkeeping requirements in the UAE

Recordkeeping requirements in the UAE are detailed in Section 11 of the Cabinet Decision No. (10) of 2019 concerning the implementing regulation of Decree Law No. 20. This states the following:

Article (24)

1. *Financial Institutions and DNFBPs shall maintain all records, documents, data and statistics for all financial transactions and local or international commercial and cash transactions for a period of no less than five years from the date of completion of the transaction or termination of the business relationship with the Customer.*
2. *Financial institutions and DNFBPs shall keep all records and documents obtained through CDD measures, ongoing monitoring, account files and business correspondence, and copies of personal identification documents, including STRs and results of any analysis performed , For a period of no less than five years from*

the date of termination of the business relationship or from the closing date of the account to Customers who maintain accounts with these institutions or after the completion of a casual transaction or from the date of completion of the inspection by the Supervisory authorities, or from the date of issuance of a final judgment of the competent judicial authorities, all depending on the circumstances.

3. *The records, documents and data kept shall be organised so as to permit data analysis and tracking of financial transactions.*
4. *Financial Institutions and DNFBPs shall make all Customer information regarding CDD towards Customers, ongoing monitoring and results of their analysis, records, files, documents, correspondence and forms available immediately to the relevant authorities upon request.*

Red flags

Detecting and combating money laundering and terrorist financing is a complex task that requires vigilance and understanding of potential warning signs, known as 'red flags.' These red flags are unusual or suspicious behaviours, patterns or activities that may indicate illicit activity. While the presence of a red flag doesn't confirm illicit activity, it does signal the need for further investigation. Let's now explore some potential red flags and risk indicators for money laundering and terrorist financing.

Risk indicators – money laundering

Some common examples of questions that might identify 'red flags' for money laundering includes the following.

- Does the type of transaction seem unusual for the customer? What about the currency?
- Does it seem that something is 'just not right' – the gut feeling or plausibility test?
- Is the amount of the transaction unusual for the type of customer?
- Does the source of funds add up to the type of customer they are?
- Is the customer making identical or similar transactions more frequently than normal?

It is very rare to identify money laundering activity through actual knowledge that property or funds come from a crime. This is because it is very rare that a firm will have direct knowledge of the underlying or predicate crime that created the criminal property. Criminals will generally not disclose that their wealth comes from drug dealing or fraud! Rather, they will adopt a cover story or provide false CDD information.

Let's discover situations in which money laundering is often otherwise identified.

- Where there is no legitimate commercial rationale for the relationship.
- Where the behaviour of the customer is suspicious, for example, where the customer pressures you to follow instructions without providing you with all the answers that you need.
- Where there is unusual or irregular activity when compared with:
    1. The historical pattern of relationship activity
    2. What is known about the personal and financial circumstances of the customer
    3. What is known about the commercial objectives of the relationship, i.e., the nature of the business and the purpose of the account.

Identifying money laundering activity is a challenge. You increase your chances of meeting the challenge by ensuring that you are well placed to identify unusual and potentially suspicious activity. You do this by knowing your customers.

Risk indicators – terrorist financing

A variety of activities should trigger red flags warning of terrorist financing potentially taking place. Indicators that warrant further investigation include the following.

- Individuals and businesses transferring funds to entities listed as terrorists or reported as having links to terrorism.
- International fund transfers to beneficiaries in a high-risk jurisdiction are potential indicators of terrorist financing.

- Transactions might be conducted by multiple customers to a single beneficiary in a high-risk jurisdiction or by a single customer to multiple beneficiaries all located in that jurisdiction.
- Multiple customers might be using the same address and telephone number to conduct activities.
- A customer could be found using incorrect spellings or variations of their name when transferring funds to high-risk jurisdictions, in order to circumvent name screening.
- Incomplete records or false documentation: this could be an attempt to hide the true origin of funds.
- Incomplete records or false documentation: this could be an attempt to hide the true origin of funds.

To be clear – identifying any of these activities does not necessarily mean that they are financing terrorism, but it is advisable for these instances to be investigated.

We will now focus on some examples of red flags specifically for some DNFBP sectors within the UAE.

Red flags for dealers in precious metals and stones

Whilst some of the red flags we are about to discuss may echo those we have previously mentioned, it is worth reviewing these as they are more specific to DNFBPs in the UAE as identified by the MoE.

Red flags for dealers in precious metals and stones includes.

1. **Large or frequent cash transactions**
   - Unusually large cash purchases or multiple cash transactions below the reporting threshold without a clear business purpose may indicate attempts to avoid detection or conceal the source of funds.
2. **Structuring or smurfing**
   - Transactions deliberately structured in amounts below the reporting threshold or split into smaller transactions to evade reporting requirements or mask the true nature of the activity.
3. **Rapid movement of funds**
   - Unexplained and swift movement of funds between accounts, particularly involving multiple

jurisdictions or high-risk countries, can be indicative of money laundering or illicit activities.

4. **Lack of business rationale**
   - Transactions lacking a legitimate business purpose, such as excessive or unexplained buying or selling of gold, raise suspicions and should be investigated further.
5. **Inconsistent customer behavior**
   - Customers displaying inconsistent behavior, such as frequent changes in personal details, business operations, or purchasing patterns, may be involved in illicit activities and require additional scrutiny.
6. **High-risk jurisdictions**
   - Transactions involving countries known for money laundering, terrorism financing, or weak AML/CFT controls in the gold sector should be closely monitored and subject to enhanced due diligence.
7. **False or forged documentation**
   - Presentation of counterfeit invoices, forged certificates, or fraudulent identification documents in gold transactions is a strong red flag indicating potential illicit activity.
8. **Shell companies or nominee directors**
   - Involvement of shell companies, front entities, or nominee directors without legitimate business activities, particularly in offshore or high-risk jurisdictions, raises suspicions of money laundering or illicit gold trading.
9. **Complex ownership structures or holding companies in tax havens**
   - Transactions involving companies with complex ownership structures, including the use of holding companies in tax havens or jurisdictions known for facilitating tax evasion, can indicate attempts to conceal the true ownership or origin of funds.
10. **Involvement of PEPs**
    - Transactions involving PEPs, their immediate family members, or close associates require enhanced due diligence due to the higher corruption and money laundering risks associated with such individuals.

11. **Unexplained price discrepancies**
    - Significant discrepancies between the market value and the declared or invoiced value of gold may indicate attempts to manipulate prices for illicit purposes or conceal the true value of transactions.
12. **Unusual trade patterns**
    - Unexplained or irregular trading patterns, sudden surges in trading volume or frequency, or unorthodox trade routes should be investigated further as they may indicate illicit gold trade or money laundering activities.
13. **Gold-to-gold transactions**
    - Unusual or frequent gold-to-gold transactions without a clear business purpose, particularly involving different jurisdictions or high-risk countries, may indicate attempts to obscure the origin or movement of funds.

Red flags for real estate brokers

The following are red flags for real estate brokers as outlined by the MoE.

Cash or third-party payments: cash payments or payments made by third parties not directly involved in the transaction, particularly when there is no clear legitimate reason, could be an indicator of illicit funds being introduced into the transaction.

Non-resident buyers or investors: transactions involving non-resident individuals or entities, especially from high-risk jurisdictions or those with a history of financial crime, may warrant closer scrutiny.

Unusual payment methods: payments made through unusual or non-traditional methods, such as cryptocurrencies, bearer instruments, or third-party payments, should be carefully examined.

Inconsistent transaction patterns: transactions that deviate significantly from a customer's normal behavior or established patterns, including sudden increases or decreases in activity, could indicate suspicious activity.

Lack of economic purpose: transactions lacking a legitimate economic purpose, such as buying properties without rental income potential or significant commercial use, may suggest money laundering.

Red flags for legal professionals

The following are red flags for legal professionals as outlined by FATF.

Red flags about the client

Red flag 1: The client is overly secret or evasive about:

- *who the client is*
- *who the beneficial owner is*
- *where the money is coming from*
- *why they are doing this transaction this way*
- *what the big picture is.*

Red flag 2: The client:

- *is using an agent or intermediary without good reason*
- *is actively avoiding personal contact without good reason*
- *is reluctant to provide or refuses to provide information, data and documents usually required in order to enable the transaction's execution*
- *holds or has previously held a public position (political or high-level professional appointment) or has professional or family ties to such an individual and is engaged in unusual private business given the frequency or characteristics involved*
- *provides false or counterfeited documentation*
- *is a business entity which cannot be found on the internet and/or uses an email address with an unusual domain part such as Hotmail, Gmail, Yahoo etc., especially if the client is otherwise secretive or avoids direct contact*
- *is known to have convictions for acquisitive crime, known to be currently under investigation for acquisitive crime or have known connections with criminals*
- *is or is related to or is a known associate of a person listed as being involved or suspected of involvement with terrorist or terrorist financing related activities*
- *shows an unusual familiarity with respect to the ordinary standards provided for by the law in the matter of satisfactory customer identification, data entries and suspicious transaction reports*

– that is – asks repeated questions on the procedures for applying the ordinary standards

Red flag 3: The parties:

- *the parties or their representatives (and, where applicable, the real owners or intermediary companies in the chain of ownership of legal entities), are native to, resident in or incorporated in a high-risk country*
- *the parties to the transaction are connected without an apparent business reason*
- *the ties between the parties of a family, employment, corporate or any other nature generate doubts as to the real nature or reason for the transaction*
- *there are multiple appearances of the same parties in transactions over a short period of time*
- *the age of the executing parties is unusual for the transaction, especially if they are under legal age, or the executing parties are incapacitated, and there is no logical explanation for their involvement*
- *there are attempts to disguise the real owner or parties to the transaction*
- *the person actually directing the operation is not one of the formal parties to the transaction or their representative*
- *the natural person acting as a director or representative does not appear a suitable representative.*

Red flags in the source of funds

Red Flag 4: The transaction involves a disproportional amount of private funding, bearer cheques or cash, especially if it is inconsistent with the socio-economic profile of the individual or the company's economic profile.

Red flag 5: The client or third party is contributing a significant sum in cash as collateral provided by the borrower/debtor rather than simply using those funds directly, without logical explanation.

Red flag 6: The source of funds is unusual:

- *third party funding either for the transaction or for fees/taxes involved with no apparent connection or legitimate explanation*

- *funds received from or sent to a foreign country when there is no apparent connection between the country and the client*
- *funds received from or sent to high-risk countries.*

Red flag 7: The client is using multiple bank accounts or foreign accounts without good reason.

Red flag 8: Private expenditure is funded by a company, business or government

Red flag 9: Selecting the method of payment has been deferred to a date very close to the time of notarisation, in a jurisdiction where the method of payment is usually included in the contract, particularly if no guarantee securing the payment is established, without a logical explanation.

Red flag 10: An unusually short repayment period has been set without logical explanation.

Red flag 11: Mortgages are repeatedly repaid significantly prior to the initially agreed maturity date, with no logical explanation.

Red flag 12: The asset is purchased with cash and then rapidly used as collateral for a loan.

Red flag 13: There is a request to change the payment procedures previously agreed upon without logical explanation, especially when payment instruments are suggested which are not appropriate for the common practice used for the ordered transaction.

Red Flag 14: Finance is provided by a lender, either a natural or legal person, other than a credit institution, with no logical explanation or economic justification.

Red Flag 15: The collateral being provided for the transaction is currently located in a high-risk country.

Red flag 16: There has been a significant increase in capital for a recently incorporated company or successive contributions over a short period of time to the same company, with no logical explanation.

Red flag 17: There has been an increase in capital from a foreign country, which either has no relationship to the company or is high risk.

Red flag 18: The company receives an injection of capital or assets in kind which is notably high in comparison with the business, size or market value of the company performing, with no logical explanation.

Red flag 19: There is an excessively high or low price attached to the securities transferred, with regard to any circumstance indicating such an excess (e.g. volume of revenue, trade or business, premises, size, knowledge of declaration of systematic losses or gains) or with regard to the sum declared in another operation.

Red flag 20: Large financial transactions, especially if requested by recently created companies, where these transactions are not justified by the corporate purpose, the activity of the client or the possible group of companies to which it belongs or other justifiable reasons.

Red flags in the choice of lawyer

Red flag 21: Instruction of a legal professional at a distance from the client or transaction without legitimate or economic reason.

Red flag 22: Instruction of a legal professional without experience in a particular specialty or without experience in providing services in complicated or especially large transactions.

Red flag 23: The client is prepared to pay substantially higher fees than usual, without legitimate reason.

Red flag 24: The client has changed advisor a number of times in a short space of time or engaged multiple legal advisers without legitimate reason.

Red flag 25: The required service was refused by another professional or the relationship with another professional was terminated.

Red flags in the nature of the retainer

Red flag 26: The transaction is unusual, e.g.:

- *the type of operation being notarised is clearly inconsistent with the size, age, or activity of the legal entity or natural person acting*
- *the transactions are unusual because of their size, nature, frequency, or manner of execution*
- *there are remarkable and highly significant differences between the declared price and the approximate actual values in accordance with any reference which could give an approximate idea of this value or in the judgement of the legal professional*

- *a non-profit organisation requests services for purposes or transactions not compatible with those declared or not typical for that body.*

Red flag 27: The client:

- *is involved in transactions which do not correspond to his normal professional or business activities*
- *shows he does not have a suitable knowledge of the nature, object or the purpose of the professional performance requested*
- *wishes to establish or take over a legal person or entity with a dubious description of the aim, or a description of the aim which is not related to his normal professional or commercial activities or his other activities, or with a description of the aim for which a license is required, while the customer does not have the intention to obtain such a licence*
- *frequently changes legal structures and/ or managers of legal persons*
- *asks for short-cuts or unexplained speed in completing a transaction o appears very disinterested in the outcome of the retainer*
- *requires introduction to financial institutions to help secure banking facilities*

Red flag 28: Creation of complicated ownership structures when there is no legitimate or economic reason.

Red flag 29: Involvement of structures with multiple countries where there is no apparent link to the client or transaction, or no other legitimate or economic reason.

Red flag 30: Incorporation and/or purchase of stock or securities of several companies, enterprises or legal entities within a short period of time with elements in common (one or several partners or shareholders, director, registered company office, corporate purpose etc.) with no logical explanation.

Red flag 31: There is an absence of documentation to support the client's story, previous transactions, or company activities.

Red flag 32: There are several elements in common between a number of transactions in a short period of time without logical explanations.

Red flag 33: Back to back (or ABC) property transactions, with rapidly increasing value or purchase price.

Red flag 34: Abandoned transactions with no concern for the fee level or after receipt of funds.

Red flag 35: There are unexplained changes in instructions, especially at the last minute.

Red flag 36: The retainer exclusively relates to keeping documents or other goods, holding large deposits of money or otherwise using the client account without the provision of legal services.

Red flag 37 There is a lack of sensible commercial/financial/tax or legal reason for the transaction.

Red flag 38 There is increased complexity in the transaction or the structures used for the transaction which results in higher taxes and fees than apparently necessary.

Red flag 39: A power of attorney is sought for the administration or disposal of assets under conditions which are unusual, where there is no logical explanation.

Red flag 40: Investment in immovable property, in the absence of any links with the place where the property is located and/or of any financial advantage from the investment.

Red flag 41: Litigation is settled too easily or quickly, with little/no involvement by the legal professional retained.

Red flag 42: Requests for payments to third parties without substantiating reason or corresponding transaction.

Red flags for CSP

The following are examples of red flags that CSPs should be aware of:

- Transfer of funds to/from third parties on the basis of fraudulent contracts, invoices, loans, or other payments, either with or without the use of the customer's own company or legal arrangement account as an intermediate step.
- Structuring of transactions, or the use of third-party names and/or involvement in transactions unrelated to the business relationship with the TCSP.
- Cancellation of transactions before completion, including those in which funds are instructed to be returned to third parties unrelated to the underlying transaction.

- Business relationships with legal entities that are complex in structure and lack transparency.
- Clients that conceal the true beneficial ownership details through nominee agreements.
- Clients who hide their true identities by giving incorrect details or fake identity documents.
- Clients that use the services of a CPS to create complex company structures that are used to conceal illicit activity or transactions as part of the layering process of money laundering.
- Clients attempting to bribe the CPS into conducting illicit activity for them.
- Clients who are based in or operate in high-risk jurisdictions, or those with high levels of corruption, subject to sanctions or have a weak AML/CFT regime.
- Clients that have either a high number of cash transactions, a significant debt amount, are PEPs or have association with PEPs, unusually high level of assets, have funds that are disproportionate to their status or have frequently changed their organisational structure.

Many of the red flags that we have discussed in the previous two examples can also be related to other DNFBP sectors. It is important to regularly review industry guidelines and updates to familiarise yourself with current red flags.

Self-assessment questions

Congratulations, you have reached the end of Unit 4. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, **continue** or alternatively, you can work through the section again if you wish.

1. What is the purpose of transaction monitoring in AML compliance programmes?

    a) To exclusively focus on transactions exceeding a specified high-value threshold

    b) To identify patterns or activities that may suggest money laundering or terrorist financing

    c) To audit customer records for any discrepancies, ignoring transaction patterns

    d) To verify the validity of transactions by cross-checking information with external databases, disregarding internal data patterns.

2. What should DFNBPs have in place for transaction monitoring and investigations?

    a) Trained personnel, effective risk assessment processes, and advanced technological tools

    b) Automated systems only aimed at freeing up personnel for the investigation

    c) Strict transaction limits that shouldn't be exceeded under any circumstances

    d) Manual monitoring only so staff can verify and investigate all transactions

3. Which three of the following are potential red flags in transaction monitoring?

    a) Frequent high-value transactions

    b) Rapid movement of funds

    c) Transactions with high-risk countries

    d) Routine, low-value transactions from a typically inactive account

Correct answers 1b, 2a, 3a,b,c

Unit 5: Implementing the Targeted Financial Sanctions

Learning Objectives

The purpose of this learning material is to:

- define what sanctions are
- determine which sanctions list you should use
- explain how to implement effective sanctions screening and reporting, and
- recognise sanctions evasion techniques and red flags.

What are sanctions?

Sanctions are restrictive measures imposed by national and international authorities that focus on:

- preventing terrorism
- conflict resolution
- non-proliferation of WMDs
- protection of civilians from harm (including protecting human rights)
- coercing a regime, or individuals within a regime, into changing their behaviour, by increasing the cost to such an extent that they decided to cease the offending behaviour, and
- signalling disapproval, stigmatising and potentially isolating a regime or individual.

Why are sanctions issued?

The UN Security Council creates restrictions in pursuit of the objectives outlined above. They are used to:

- change the behaviour of a targeted country, region or regime
- apply pressure on a targeted country, region or regime to comply with set objectives
- act as an enforcement tool when international peace and security have been threatened and diplomatic efforts have failed

- restrict the funding of individuals, entities or groups associated with criminal or terrorist activity, and
- restrict providing funds or financial services which are used, in whole or in part, in nuclear proliferation/manufacturing of WMDs.

Why are sanctions important?

Recent developments

Recent international political developments and military conflicts have brought the threat of terrorism to the forefront of domestic and international political agendas. It is critical that firms and compliance functions fulfil their legal and regulatory sanctions obligations, in support of the wider political aims of the international community.

Fighting financial crime

Financial institutions and DNFBPs act as a front-line defence against financial crime. It is also a regulatory requirement for financial institutions to combat money laundering, terrorist financing and sanctions breaches. Similarly, businesses operating in other industries are also required to implement robust compliance programmes to ensure that they are not exposed to sanctions risks. For example, oil and gas companies will consider prohibitions relating to petrochemicals, gold and precious metals.

By proper implementation of targeted financial sanctions against persons and entities designated by the UN Security Council and under applicable national or supra-national sanctions regimes, you will ensure that all designated persons and entities are identified and deprived of their resources and means to finance or support terrorist activities and organisations or proliferation activities.

This include, but not limited to, financial assets, economic resources (including oil and other natural resources), 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, and any

other assets which potentially may be used to obtain funds, goods or services.

What forms can sanctions take?

Sanctions can take numerous forms. The most relevant types of sanction for businesses are:

- targeted financial sanctions (e.g., asset freezes)
- trade sanctions, and
- non-financial sanctions.

What sanctions are applicable to DNFBPs in the UAE?

It is important to note that DNFBPs in the UAE are only required to implement targeted financial sanctions issued by the UN Security Council that's related to terrorist financing and proliferation financing and the UAE sanctions list. However, all regulated entities need to be aware about the other type of sanctions (such as OFAC, EU, HM Treasury, etc.) and how they could be vulnerable to their risks.

What are targeted financial sanctions?

The term targeted financial sanctions refers to both asset freezing and prohibitions aimed at preventing funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

Targeted financial sanctions are restrictive measures imposed by governments or the UN Security Council to restrict access to financial resources for specific individuals, entities or countries. These sanctions aim to achieve specific policy objectives, typically related to international security or human rights. Unlike comprehensive economic sanctions that affect an entire country, targeted financial sanctions focus on particular entities or individuals believed to be involved in illicit activities related to terrorism or nuclear proliferation.

Targeted financial sanctions can include freezing assets, limiting access to financial services, restricting trade and banning certain types of financial transactions. They serve as a non-violent means of exerting pressure, isolating the targeted subjects from the global financial system,

and disrupting their capacity to finance their activities. These sanctions can also discourage third parties from engaging in transactions with the targeted individuals or entities, further isolating them economically and financially.

While targeted financial sanctions aim to minimise harm to the general population, they may still have indirect effects on broader economic sectors or innocent parties associated with the targeted entities. Therefore, their implementation and impact are often a subject of careful monitoring and ongoing debate.

Financial Sanctions may be issued against a number of different actors as follows(e.g., individuals, corporate bodies, terrorist groups, and vessels) and activities/sectors and trade activities.

Actions related to implementing targeted financial sanctions :

The implementation of targeted financial sanctions includes both **asset freezing and prohibitions** to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities. Assets freezing is more related to financial institutions that hold accounts to their clients but for DNFBPs its more related to prohibitions rather than freezing, anyway they are required to freeze if any cases requiring that.

Asset freezing

The term freeze means to prohibit the transfer, conversion, disposition or movement of any funds or other assets that are owned or controlled by designated persons, groups or entities on the basis of, and for the duration of the validity of, an action initiated by the UN Security Council or in accordance with applicable Security Council resolutions by a competent authority or a court.

The obligation to freeze should extend to:

(i) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular terrorist act, plot or threat;

(ii) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities; and

(iii) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities, as well as

(iv) funds or other assets of persons and entities acting on behalf of, or at the direction of, designated persons or entities.

All natural and legal persons within the country must freeze, without delay and without prior notice, the funds or other assets of designated persons and entities. And once de-listed they have to unfreeze funds immediately. DNFBPs should report any action taken in implementing the targeted financial sanctions to the competent authority.

Note:

The term 'funds' refers to assets of every kind, whether corporeal or incorporeal, 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.

Prohibition to offer funds and services

This involves 'the prohibition to provide funds to, or render financial services or other services related to, any listed individual, group, or entity.'

All persons and entities within their jurisdiction 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 and entities; entities owned or controlled, directly or indirectly, by designated persons or entities; and persons and entities acting on behalf of, or at the direction of, designated persons or entities, unless licensed, authorised or otherwise notified in accordance with the relevant UN Security Council Resolutions (UNSCRs).

An example of this for DNFBPs could be the prohibition of any service, such as legal services to transfer asset ownership, the buying or selling of real estate, selling jewellery, precious metals, etc.

Implementing targeted financial sanctions without delay

All reporting entities are required to implement the targeted financial sanctions without delay.

The phrase without delay means, ideally, within a matter of hours of a designation by the UNSC (within 24 hours) or its relevant Sanctions Committee (e.g. the 1267 Committee, the 1988 Committee, the 1718 Sanctions Committee). For the purposes of S/RES/1373(2001) (UAE Local Terrorist List), 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. In both cases, the phrase without delay should be interpreted in the context of the need to prevent the flight or dissipation of funds or other assets which are linked to terrorists, terrorist organisations, those who finance terrorism, and to the financing of proliferation of WMDs, and the need for global, concerted action to interdict and disrupt their flow swiftly.

Sanctions requirements for DNFBPs in the UAE

Before we go into further detail with regards to the requirements for DNFBPs, let's first understand the legal framework for implementing UN financial sanctions and local targeted financial sanctions measured.

Legal framework

The following are the main laws applicable to firms in the UAE:

Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations

Articles/text 16.1, 28

Cabinet Decision No. 10 of 2019 Concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.

Articles/text 11, 12, 44.7, 60

Cabinet Resolution No. 74 of 2020 concerning the Local Terrorist List of terrorists and implementation

of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction, and the relevant resolutions

The UNSC holds the capacity to take action in seeking to maintain or restore international peace and security under Chapter VII of the UN Charter, including by imposing sanctioning measures under Article 41, which encompass a broad range of enforcement options that do not involve the use of armed force. The UNSC has the authority to issue binding resolutions on UN member states.

The UAE, as a member of the UN, is committed to implementing the UNSCRs, including those related to UN sanctions regimes. Consequently, through the Cabinet Resolution No. 74 of 2020, the UAE implements UNSCRs on the suppression and combating of terrorism, terrorist financing and countering the financing of proliferation of WMDs, in particular, targeted financial sanctions regimes as defined by the UN.

Security Council sanctions have taken several different forms, in pursuit of a variety of goals. The measures have ranged from comprehensive economic and trade sanctions to more targeted measures such as arms embargoes, travel bans, and financial or commodity restrictions. The Security Council has applied sanctions to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote the non-proliferation of WMDs.

As stated above, the UN sanctions regimes include different measures that countries must apply; however the following explains only how to implement in the UAE the targeted financial sanctions related to the freezing measures and prohibition to provide funds and services in accordance with the following UNSCRs. Individuals and legal entities in the UAE should also refer to relevant rules, regulations, and guidance published by the Supervisory Authorities and the UN Security Council.

Articles/text all

Now that we have established the legal framework, let's explore the requirements in more detail.

All DNFBPs are required to comply with the following targeted financial sanctions obligations in accordance with

Cabinet Decision No. 74 of 2020 for UNSCRs 1718 (2006) and 2231 (2015). These requirements include:

1. *Implement screening procedures on all parties of a transaction or provided services as per the definition of a DNFBP in Article (3) of Cabinet Decision No (10) of 2019 concerning the Implementing Regulations to ensure they are not linked with persons or entities or organizations listed under UNSCR 1718 (2006) and 2231 (2015).*
2. *Implement Enhanced Due-Diligence (EDD) procedures on all transactions, including trade transactions, linked to North Korea and Iran.*
3. *Verification of cross-border transactions suspected of being related to unauthorized trading of Dual-Use Goods.*
4. *Report immediately (without delay) all confirmed or potential matches related to any individuals or entities designated pursuant to the above-mentioned UNSCRs. Reporting shall cover:*
    - *Any confirmed match by raising a Funds Freeze Report (FFR) via GoAML within 5 business days from implementing any freeze measures.*
    - *Any potential match by raising a Partial Name Match Report (PNMR) via GoAML within 5 business days from implementing any suspension measures.*
    - *Any suspicious transactions or activity that may be related to designated individuals or entities pursuant to the above-mentioned UNSCRs by raising an STR/ SAR via GoAML to the UAE Financial Intelligence Unit.*

In addition to the above, Article 21 of Cabinet Decision 74 outlines obligations of financial institutions and DNFBPs. This details the following.

For the purposes of implementing the present Decision, financial institutions and DNFBPs shall abide by the following:

1- *Register on the Office's website in order to receive notifications related to new listing, re-listing, updating, or de-listing decisions issued by the UN Security Council, the Sanctions Committee or the Cabinet.*

2- *Regularly screen their databases and transactions against names on lists issued by the UN Security Council, the Sanctions Committee or the Local Lists, and also immediately when notified of any changes to any of such lists, provided that such screening includes the following:*

a - Searching their customer databases.

b - Search for the names of parties to any transactions.

c - Search for the names of potential customers.

d - Search for the names of beneficial owners.

e - Search for names of persons and organizations with which they have a direct or indirect relationship.

f - Continuously search their customer database before conducting any transaction, or entering into a serious business relationship with any person, to ensure that their name is not listed on the Sanctions List or Local Lists.

3- Implement freezing measures, without delay, and without prior notice to the Listed Person, immediately when a match is found through the screening process referred to in paragraph (2) of this article.

4- Implement decisions to lift freezing measures without delay, pursuant to Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists.

5- Immediately notify the Supervisory Authority in the following cases:

a - Identification of funds and actions that have been taken as per requirements of Relevant UNSCRs or decisions of the Cabinet regarding the issuance of Local Lists, including attempted transactions.

b - Detection of any match with listed persons or entities, details of the match data and actions that have been taken as per the requirements of Relevant UNSCRs and Local Lists, including attempted transactions.

c - If it was found that one of its previous customers or any occasional customer it dealt with, is listed on the Sanctions List or Local Lists.

d - If it suspects that one of its current or former customers, or a person it has a business relationship with is listed or has a direct or indirect relationship with the Listed Person. 18

e - Not to take any action because of the similarity of the names, and the inability to remove this similarity through the available or accessible information.

f - Information relating to funds that have been unfrozen, including their status, nature, value and measures

that were taken in respect thereof, and any other information relevant to such decisions.

6- *Establish and effectively implement internal controls and procedures to ensure compliance with the obligations arising from this Decision.*

7- *Establish and implement policies and procedures that prohibit staff from, directly or indirectly, informing the customer or any third party that freezing or any Other Measures shall be implemented in accordance with the provisions of this Decision.*

8- *Cooperate with the Office and the Supervisory Authority in verifying the accuracy of submitted information.*

It is recommended to review the entirety of this Cabinet Decision in order to gain a full understanding of the requirements detailed within it. You can view it by selecting this link.

Sanctions implementation

Targeted financial sanctions must be implemented in accordance with the relevant UNSC Resolutions, including the UN Consolidated List, and the Local Terrorist List.

There are four main obligations on all persons, natural or legal in the UAE to implement targeted financial sanctions:

1. *Subscribe*
2. *Screen*
3. *Apply targeted financial sanctions*
4. *Report*

All natural and legal persons in the UAE must comply with the following general obligations:

Step-1 Subscribe: Subscribe to the Executive Office Notification System to receive automated email notifications on any updates to the Sanctions Lists (Local Terrorist List or UN Consolidated List)

Step-2 Screen: Undertake regular and ongoing screening on the latest Local Terrorist List and UN Consolidated list. Screening must be undertaken in the following circumstances:

1. *Upon any updates to the Local Terrorist List or UN Consolidated List. In such cases, screening must be conducted immediately and without delay to ensure*

compliance with implementing freezing measures without delay (within 24 hours).

2. *Prior to onboarding new customers.*
3. *Upon KYC reviews or changes to a customer's information.*
4. *Before processing any transaction.*

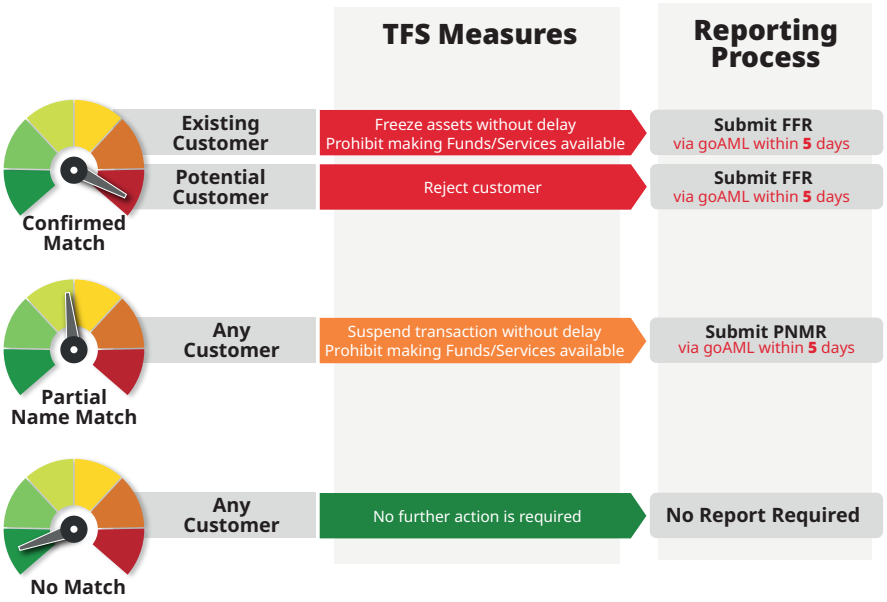
Step-3 Apply Targeted Financial Sanctions:

1. *Freezing of all funds: Freeze, without delay (within 24 hours) and without prior notice, all the funds:*
   - *Owned or controlled, wholly or jointly, directly, or indirectly, by an individual or legal entity designated by the UAE Cabinet or pursuant to a relevant UNSC Resolution.*
   - *Derived or generated from funds under item (a); or*
   - *Individuals or legal entities acting on behalf of or at the direction of an individual or legal entity designated by an individual or legal entity designated by the Local Terrorist or pursuant or the United Nations consolidated list.*
2. *Prohibition of making funds available: No individual or legal person in the UAE is permitted to provide funds to or render financial services or other services related to, whether in whole or in part, directly or indirectly, or for the benefit of any individual or legal entity listed in the Local Terrorist List or the UN Consolidated List pursuant to a relevant UNSC Resolution.*

Certain exceptions may apply, upon submitted request and written authorisation from the Executive Office for Control & Non-Proliferation, applicable authority, or in accordance with Cabinet decisions.

- Interest, profits, or other earnings due on the account; and
- Payments due under contracts, agreements or obligations agreed upon prior to the date on which the individual or legal entity was designated, **provided such additions are immediately frozen**, and the respected Supervisory Authority is informed immediately.

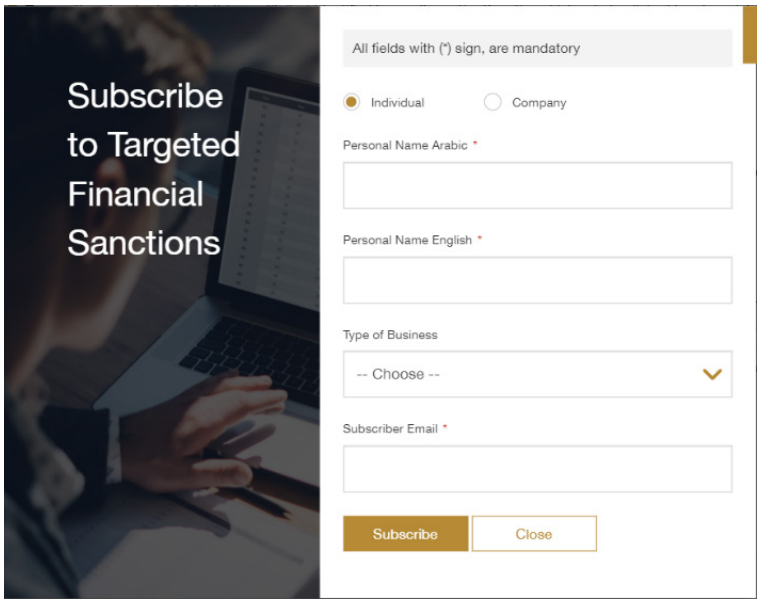
Step-4 Report: FIs, DNFBPs, and VASPs should report any freezing or suspension measures taken upon identifying confirmed or partial name matches through the goAML platform within five (5) days from taking such measures.



For non goAML users (persons that do not fall under the definition of financial institutions, DNFBPs or VASPs and are therefore not under an obligation to register on goAML), reporting should be made by sending an email to the Executive Office through iec@uaeiec.gov.ae

How to keep your list updated?

DNFBPs in the UAE are required to subscribe to the EOCN Notification System on the EOCN's website (www.uaeiec.gov.ae/en-us/un-page) to receive automated email notifications on any updates to the Sanctions List.



Which sanctions lists should you use?

As a member of the UN, the UAE is required to comply with all sanctions issued and passed by the UNSC including targeted financial sanctions requirements (terrorist financing and proliferation financing) and the UAE Sanctions List:

1- United Nations (UN) sanctions

UN sanctions are imposed by a process known as a UN Security Council Resolution (UNSCR).

When a UNSCR is passed, it is then up to member nations to implement the sanctions in their own countries. This is done through a variety of legislative processes. DNFBPs in the UAE are required to implement UN sanctions lists.

The UN also publishes the names of individuals and organisations subject to UN financial sanctions in relation to involvement with terrorism and proliferation, specifically:

Terrorism and terrorist financing:

1.	Islamic State in Iraq and the Levant (Da'esh), Al-Qaeda, and associated individuals, groups, undertakings, and entities.	UNSCR 1267 (1999), 1989 (2011) and its successor resolutions
2.	The Taliban, and associated individuals, groups, undertakings, and entities.	UNSCR 1988 (2011) and its successor resolutions
3.	Any individual or entity designated by the United Arab Emirates (Local Terrorism List').	UNSCR 1373 (2001)

The financing of proliferation of WMDs:

1.	**Democratic People's Republic of Korea (DPRK):** nuclear-related, other weapons of mass destruction-related, and ballistic missile-related programmes.	UNSCR 1718 (2006) and its successor resolutions
2.	**Islamic Republic of Iran:** nuclear programme	UNSCR 2231 (2015)

Ref: www.uaeiec.gov.ae/en-us/un-page

Local List

Overview

All UN member states must implement freezing measures with regards to individuals or legal entities designated by the UNSC. In addition, UNSCR 1373 (2001) mandates each UN member state to develop the procedures to identify and apply freezing measures with regards to individuals or legal entities that are suspected of, attempt to, and/or commit terrorist acts.

In the UAE, the Supreme Council for National Security (Supreme Council) prepares such designations. Specifically, the Supreme Council proposes a Local List that meets the designation criteria required by UNSCR 1373 (2001). The Supreme Council can include individuals or legal entities in that list without prior notice, and irrespective of whether criminal proceedings exist. Each listing must be approved by the Cabinet of the UAE.

All freezing and prohibition obligations apply to UN lists and the local list.

UAE Local Terrorist List: www.uaeiec.gov.ae/en-us/un-page

Other sanctions' lists

There may be instances where your business might fall under the purview of other unilateral sanctions, based on specific situations. If that's the case, it's important that you conform to these regulations. Factors that could determine this include the geographical areas where your business operates, your business partners, and the currencies you use for transactions. Sanctions you might have to contemplate on their pertinence could be those imposed by entities such as the EU, the UK's HM Treasury, and the US's OFAC. In every scenario, it's anticipated that you would evaluate and adopt necessary measures to abide by the relevant sanctions regimes.

Note

A key point to note is that DNFBPs need to be aware that other sanctions can be applicable if they engaged with transactions using other currencies (e.g., USD: USA/OFAC, GBP: UK/HM Treasury, EUR: EU), dealing with entities or individuals holding there nationalities or have a branch in their countries.

Case studies

In June 2014 OFAC 'announced a $963 million agreement with BNP Paribas SA ("BNPP") to settle its potential liability for apparent violations of U.S. sanctions regulations'.[12] This was part of a combined $8.9 billion settlement with US federal and state government agencies, and followed OFAC's investigation into BNPP's systemic practice of concealing, removing, omitting or obscuring references to information about US-sanctioned parties in 3,897 financial and trade transactions routed to or through banks in the US between 2005 and 2012, in apparent violation of the Sudanese, Iranian, Cuban and Burmese Sanctions Regulations.

In April 2019, OFAC announced three separate settlements totalling $611 million with the following UniCredit Group banks: UniCredit Bank AG in Germany, UniCredit Bank Austria AG in Austria and UniCredit S.p.A in Italy.

When to conduct sanctions screening

DNFBPs are required to screen prospective and (on an ongoing basis) existing clients, beneficial owners, and transactions for potential matches with the UN Consolidated List and all sanctions issued by the UAE including the UAE Local Terrorist List. Below are examples of situations requiring targeted financial sanctions screening:

- prior to onboarding new customers
- prior to processing any transaction
- during ongoing CDD and KYC reviews
- upon modifications to a customer's information, and
- whenever the UN Consolidated List and UAE Terrorist List is updated.

To ensure compliance with freezing measures, screening must be done within 24 hours of these lists being updated.

12. US Department of the Treasury, 'Treasury Reaches Largest Ever Sanctions-Related Settlement With BNP Paribas SA for $963 Million', 30 June 2014: www.treasury.gov/press-center/press-releases/Pages/jl2447.aspx – accessed December 2021.

How to implement an effective sanction screening?

Effective sanctions screening should be achieved through data filtering and monitoring systems designed to detect designated connections for customers as well as inbound or outbound payments. These systems are required to be able to scan all relevant information (e.g., name of individual or entity, date of birth, address, etc.) relating to the business activity being carried out, to identify connections affected by sanctions.

In the case of smaller DNFBPs, firms may adopt manual screening processes due to the cost associated with more sophisticated, automated systems. DNFBPs conduct manual sanctions screening by manually checking the names of their clients or potential clients against the lists of individuals or entities that are subject to sanctions. This can be done through a simple document review or by using specialised software that can cross-reference client data with sanction lists. DNFBPs need to be thorough and accurate in this process to ensure compliance with regulations, avoid potential fines, and protect against involvement in illicit activities.

Important

It is important to have sanctions controls in place at all stages of the client lifecycle and perform due diligence on relevant parties to all transactions. A robust sanctions programme should ensure screening of employees, vendors, all third parties, all payment activity and prospective clients.

Names should be screened at the outset of a relationship, and the whole database of existing customers should be screened frequently thereafter to account for changes to sanctions lists. A customer may not be on a sanctions list when a relationship is established, but they may be added later. If an automated system is implemented, the screening system needs to account for these changes by updating the lists against which the names are screened. If screening is conducted manually, this will also need to be done manually.

In addition, every time a client undertakes an international money transfer (known as a wire transfer) the transaction

should be screened to ensure it is not being sent to a sanctioned individual or entity or otherwise relating to a sanctioned activity.

Periodic reviews of the processes and systems need to be carried out, and records retained in accordance with local laws; management information should be produced regularly to give senior management oversight of sanctions risks.

Regular calibration and fuzzy logic

Firms should carry out regular reviews of the appropriateness of the screening system to ensure that the system remains up to date and effective. This includes considering whether its screening rules are calibrated appropriately for the firm's business and client list. If they are not, there is a possibility that potential matches may not be raised as alerts.

Definition: Fuzzy logic

There is a general practice to use what is known as fuzzy logic; this refers to the ability for any screening system (automated or manual) to identify misspelling, name reversals, or minor variations, etc., against a possible match.

Example

For example, if the name 'John Smith' is on a sanctions list, an input to a payment as 'Smith John' or 'Jon Smith' should generate an alert. This is particularly important not only to account for potential errors in input but also for general reasons owing to different variations for inputting a name.

A large number of false hits may be difficult to manage on a day-to-day basis for firms with large volumes of screening. In order to narrow down false hits, firms will employ a rule matching capability within their screening systems to discount false hits where possible, leaving only potential or true matches to sanctions lists for further investigation.

Using manual/automated sanction screening system

As explained, there is no legal requirement to use automated methods – however, firms, depending on the number of transactions and staff, can decide whether they will use manual or an automated screening tool. Regardless, the ultimate goal is to effectively implement sanctions screening without delay.

How does automated screening work?

These systems will employ pre-defined algorithms, approved by the firm's senior management and the designated sanctions officer. Periodic reviews must be carried out and all changes tested and analysed, approved by the relevant escalation process and documented.

Using an electronic system does not exempt companies from their responsibilities. Companies must ensure that information systems companies use all relevant lists and update them immediately upon any update, whether by addition, modification or cancellation.

How does manual screening work?

While larger DNFBPs may use automated systems, smaller organisations may not have the resources for such solutions. However, they can manually keep their sanctions lists up to date through a diligent and systematic approach.

Firstly, they need to identify the relevant sources of information (the United Nations Consolidated List, and the Local Terrorist List). These websites regularly publish updates and amendments to their sanctions lists, alternatively firms can subscribe to the Executive Office Notification System to receive automated email notifications on any updates to the Sanctions Lists.

Once the sources are identified, the next step is to regularly check these websites for updates. The frequency of checks should be aligned with the frequency of updates by the authorities. For instance, if the UN updates its list every week.

After identifying any updates, DNFBPs should promptly incorporate these changes into their own sanctions lists. This could involve adding or removing individuals, entities, or countries from the list. It is important to note that the

sanctions lists are not static but dynamic, and they can change frequently based on the geopolitical situation.

Finally, it is recommended to keep a record of these updates. This will help in demonstrating compliance with the regulations during audits and inspections. This record should include details like the date of the update, the source of the update, and the changes made to the list.

By following these steps, small DNFBPs can manually keep their sanctions lists up to date, thus ensuring compliance with the relevant laws and regulations, and contributing to the global efforts against financial crimes.

How can firms ensure that screening is carried out consistently?

As mentioned previously, it is important for firms to establish a sanctions screening policy, and to develop and maintain operating procedures to support a consistent approach across automated and manual solutions in all jurisdictions/regions where they are active. Records must be kept for both automated and manual processes in line with record retention policies. It is crucial that the rationale for risk-based decisions is documented.

This applies to all aspects of the client lifecycle, where annual reviews and trigger events identify connections to sanctions-related jurisdictions/regions and parties. A set of minimum standards must be documented, service level agreements put in place and adequate training for all staff (at appropriate levels) are all important for achieving consistency. Operations teams, front office staff and sanctions compliance teams may wish to add or change items on this list as they build intelligence about customers or sanctions-risk parties over time.

Real-time screening may be appropriate depending on the nature of business activity (for example, the processing of transactions for financial services firms).

Who should be screened?

Firms should institute freezing measures, including the prohibition of making funds available, when they conduct any business with:

1. any individual, group, or legal entity listed in the Local Terrorist List defined by the Federal Cabinet

or listed by the UNSC in its Consolidated Sanctions List (terrorist financing/proliferation financing).

2. any legal entity, directly or indirectly owned or controlled by an individual or legal entity listed under A, and
3. any individual or legal entity acting on behalf of or at the direction of any individual or legal entity listed under A and B.

This includes:

1. **Customers**

   Individual and legal entity customers

2. **Staff**

   All staff

3. **Third-party service providers**

   All third-party service providers, including suppliers (such as suppliers of screening solutions, or staffing), those renting properties from the firm, etc.

4. **Connected/related parties**

   Parties identified as being connected to the business relationship or target of sanctions

5. **UBOs**

   Ultimate beneficial owners (and key parties to the business relationship)

6. **Products and services**

   For example, transactions such as those described in the next topic

Let's now look at each of these categories in more detail.

Individuals

Individuals who are personal customers must be screened to ensure that they are not directly or indirectly linked to a target on a sanctions list (i.e., listed on a global/local/internal watch list as detailed later in this unit).

Firms are expected to screen all the following points, at a minimum:

- full legal and any recorded name
- nationality, and
- city and country of residential address., and
- date of birth

All staff, including permanent, temporary members and contractors, are required to be screened before they are hired, and again regularly during their term of engagement.

Service providers providing outsourcing services may also screen customers of commercial clients. This approach may vary depending on the contractual arrangements and the firm's risk appetite (e.g., nature of services, jurisdictional footprint).

Entities

For legal entities, at a minimum the firm must screen:

- full legal name
- all recorded trading names
- city and country/region of registered office address in the country/region of incorporation, and
- city and country of business address (if different from the registered office address).

UBOs

Firms are required to identify all connected and related parties (both individual and entity clients), key controllers and ultimate beneficial owners and, at a minimum, to screen:

- full legal/recorded/trading names
- city, country/region of address
- city, country/region of address, and
- date of birth.

Suppliers

All third-party service providers must be screened, at a minimum:

- before a relationship (contract/ lease) is established, and
- in the event that a contract/lease is renewed.

Screening should cover:

- all individuals/entities/connected parties to the business relationship, and
- the country or region in which they operate or are physically present.

Firms may need to consider the nature of relationships maintained with suppliers and ensure that sanctions screening is applied in all areas, e.g., landlords of property rented by the firm, business introducers, etc.

Targeting terrorism: FATF Recommendations 6/7

FATF's International Best Practices Recommendation 6 requires countries to implement targeted financial sanctions regimes to comply with relevant UNSCRs.

Firms are expected to freeze funds and assets quickly and effectively to support the efforts to combat terrorist financing by ensuring that no funds/assets are made available, directly or indirectly, to designated persons or entities.

In addition to a robust terrorist financing regime, national frameworks must comply with human rights, local rule of law and due process. FATF encourages:

- exposure of monetary trails of terrorist financing
- deterrence of designated persons/entities or those willing to support designated targets
- dismantling terrorist networks
- terminating terrorist cash flow
- fostering international cooperation
- establishing effective procedures to identify and take action where Al-Qaeda/Taliban/ISIS/proliferation financing sanctions regimes are involved
- communicating designations in a timely fashion to avoid unintentional breaches
- timely freezing, without delay
- reporting and investigation processes
- managing designated targets who are resident in the country or region, and
- issuing licences to manage frozen funds/assets.

Managing alert investigations

Alerts generated for further investigation must be subject to documented escalation processes and procedures. Timescales may differ for new clients, existing clients, vendors, employees (including contract and temporary staff) or transactions to be processed. Service-level agreements for investigating potential matches to sanctions lists must be in place for all procedures conducted by one area or function on behalf of another.

Important

Higher-risk potential matches must be prioritised for investigation. Some instances may require additional time, when, for example, communication takes longer than usual with a customer. Processes and procedures must be in place to manage this, including escalation routes and recording reasons for delay on file, etc.

If it is determined a sanctions alert does not in fact relate to the sanctioned person or entity, sufficient explanations need to be provided to substantiate how the decision was reached to 'discount' or 'close' the alert.

Example

For example the name might match exactly, but investigation might reveal the person on the sanction list and the customer have different dates of birth. This should be clearly recorded and evidenced.

True matches

True matches to a sanctions list may be identified at one of the sanctions controls stages, or may first be identified as a potential match and only confirmed as a true match following an investigation.

There are three types of true match:

i. true matches to restricted countries

ii. true matches identified with payments rejected, and

iii. other true matches,

Important

A clear process must be in place to respond to confirmed hits on sanctioned lists. This may include reporting to external authorities.

Staff members who are tasked with investigating alerts must be specially trained to understand sanctions risks in relation to the nature of the business. Regular training is crucial in the evolving international environment that drives sanctions changes.

What should the alert investigation procedures cover? **Take a moment to consider this question**, then see the following for our suggestions.

Alert investigation procedures

Documented alert investigation procedures will include at a minimum:

- clear roles and responsibilities for carrying out specific parts of the investigation by staff members with appropriate technical competency
- sufficient resource to manage alert investigations within prescribed time frames and quality
- a defined process for the management of increased volumes of alerts or 'spikes' in volumes (which may, for example, result from new names being added to the sanctions watch list for screening; if these are common names, they may raise multiple potential matches for further investigation)
- prioritisation of alerts for investigation (for example, external official lists should be checked before internal lists); this may become relevant for potential 'spike' management, when higher-risk potential matches must be prioritised for investigation
- clear escalation routes for risk-based decisions
- defined reporting procedures for both internal and external reporting
- a process to ensure that all alerts are investigated, unless a documented risk-based decision is taken to exclude certain types of sanctions alert

- a defined process for discounting (see section 3 below)
- possibly, different timescales for investigations for alerts for new customers, suppliers, employees, transactions, or existing customers
- recording of the key rationale for risk-based decisions
- the creation of established Service Level Agreements if the compliance function outsources the sanctions review process or part of it (either to a third-party provider or to another function within the firm), and
- defined processes for when true matches are identified (e.g., breach reporting, licence applications).

Some instances may require additional time, for example, when communication with a customer takes longer than usual. Processes and procedures must be in place to manage this, including escalation routes and recording reasons for delay on file.

Clear steps must be established for alerts that may be:

- processed within current sanctions policy
- processed outside the current sanctions policy, using an exception rule
- blocked/rejected/exited following investigation of the alert, and
- reported to external authorities following internal procedures.

Management reporting requirements must be distributed to all key business and compliance contacts.

Investigations must be carried out in a consistent manner. Firms may choose to build specialised sanctions investigations teams in the form of hubs to create a consistent standard across global operating locations and to accommodate international secrecy or data privacy laws.

Types of alerts may include the following.

Customer alerts

For example, if a firm holds a customer relationship with John Smith and a sanctions watch list used for screening is updated with a new sanctions target called John Smith, an alert will be generated during the screening process

to highlight a connection to a potential sanctions target. The firm will then follow alert investigation procedures to determine whether it is a true match, using middle names, variations in names, date of birth, location information, etc. (More on this later in the unit.)

Reporting positive/false positive matches

The Executive Office of the have developed a unified mechanism to report targeted financial sanctions obligations utilising the UAE FIU online reporting platform goAML.

It is noted that the goAML platform is to be utilised as the reporting platform for all licensed DNFBPs to submit reports in order to comply with reporting obligations. The UAE FIU has developed the goAML platform to include two targeted financial sanctions related reports:

1. Funds Freeze Report (FFR), and

2. Partial Name Match Report (PNMR)

The targeted financial sanctions-related reports submitted via the goAML platform will be received simultaneously by the Executive Office–IEC and the Ministry of Economy.

The Ministry refers to the procedures mentioned as published in the following details:

Procedures on targeted financial sanctions reporting via the goAML Platform:

When a 'confirmed match' to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, Licensed DNFBPs are required to take the following necessary actions :

1) *Implement all necessary measures without delay as outlined in the Cabinet Decision (74) of 2020, Guidance on Targeted Financial Sanctions issued by the EO-IEC.*

2) *Report any freezing measure, prohibition to provide funds or services, and any attempted transactions to the Ministry of Economy and the Executive Office – IEC via the GoAML platform within two business days by selecting the Fund Freeze Report (FFR); and*

   Ensure all the necessary information and documents regarding the 'confirmed match' is submitted along with the FFR.

3) *Uphold freezing measures related to the 'confirmed match' until further instructions are received from Executive Office – IEC; and*

4) *Notify and share a copy of the report with Ministry of Economy through this email:* sanctions@economy.ae

When a 'potential match' to a listing of names of individuals, groups, or entities to the UAE Local Terrorist List or UNSC Consolidated List is identified, Licensed DNFPBs are required to take the following necessary action:

1) *Suspend without delay any transaction and refrain from offering any funds or services, as outlined in the Guidance on Targeted Financial Sanctions, and Guidance for Licensed DNFBPs on the Implementation of Targeted Financial Sanctions;*

2) *Report the 'potential match' to the Ministry of Economy and the Executive Office – IEC via the GoAML platform by selecting the Partial Name Match Report (PNMR);*

3) *Ensure all the necessary information and documents regarding the name match is submitted; and*

4) *Uphold suspension measures related to the 'potential match' until further instructions are received from Executive Office – IEC via the GoAML platform on whether to cancel the suspension or implement freezing measures.*

5) *Notify and share a copy of the report with Ministry of Economy through this email:* sanctions@economy.ae

Ministry of Economy notes to Licensed DNFBPs that they should consult the Ministry of Economy and the Executive Office-IEC's websites and published guidelines, respectively, as updated from time to time.

16. Circular No. 2-2022 Updated TFS requirements from DNFBPs. Ar. En.pdf

What are my obligations when identifying a sanctioned customer

	Type of customer	TFS measures	Reporting process
Confirmed match	Existing customer	Freeze assets* without delay (remains in effect until de-listing)	Submit Funds Freeze Report (FFR) via goAML within 5 days
	Potential customer	Reject customer	
Partial Name match**	Any customer	Suspend all transactions without delay (remains in effect until you receive further instructions from the EOCN)	Submit Partial Name Match Report (PNMR) via goAML within 5 days
False match	Any customer	No action required	Continue screening

The cost of getting it wrong

Companies operating internationally need to be aware of sanctions regimes and how to comply with them. The consequences of breaching sanctions are serious. This applies to diverse industries, including financial institutions, DNFBPs, insurers, oil and gas service companies, infrastructure and engineering companies.

While firms may feel the pinch of lost business with potentially or confirmed sanctions targets and of the cost of managing the risk, these costs do not compare to the significant cost of getting it wrong:

- large monetary fines (see list below)
- civil and criminal penalties that may include restricting business activity and the loss of revenue that may ensue or even the closure of the firm
- reputational damage
- loss of value of shares, and

- remediation costs (which may accrue for many subsequent years, involving external resources, new systems, etc.).

Consequences for any person

For individuals in the UAE failing to comply with the targeted financial sanctions obligations, any natural or legal person will be subject to imprisonment or a fine of no less than AED50,000 (fifty thousand dirhams) and no more than AED5,000,000 (five million dirhams).

Consequences for financial institutions or DNFBPs

DNFBPs are subject to supervision, and therefore any cases of non-compliance can result in enforcement action as outlined in the Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT).

The supervisory authorities of financial institutions and DNFBPs have the legal capacity to supervise the implementation of targeted financial sanctions. The supervisory authorities may also issue the following administrative sanctions:

a. Letter of warning.

b. Administrative penalties of no less than AED 50,000 (fifty thousand dirham) and no more than AED 5,000,000 (five million dirham) for each violation.

c. Banning the violator from working in the sector related to the violation for the period determined by the supervisory authority.

d. Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.

e. Suspend Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.

f. Suspend or restrict the activity or the profession for a period to be determined by the supervisory authority.

g. Cancel the License.

Source: www.moec.gov.ae/en/federal-decree-law-no-20-of-2018-on-anti-money-laundering-and-combating-the-financing-of-terrorism-and-illegal-organisations

Sanction evasion

Sanctions evasion is a deliberate attempt to circumvent sanctions regimes. Individuals and those acting on behalf of organisations, regimes and nation states have used a range of methods to evade sanctions.

Collusion involves an individual or entity aiding those seeking to deliberately circumvent sanctions through evasion.

It is essential that staff members understand their individual responsibilities. Although the tipping-off offence does not relate to sanctions, staff must remain vigilant about the information and type of advice they provide to customers.

Financial institutions, DNFBPs and VASPs should utilise active strategies to identify transactions that evade sanctions. This can be achieved by comprehending the evolving threats and susceptibilities that could be exploited by those financing terrorism or proliferation activities, executing thorough CDD, and keeping sanctions lists current. Further steps include educating about the methods of sanction evasion and reporting any suspicious transactions related to proliferation financing or terrorism financing to the FIU through goAML.

Evasion techniques and shipping

The two boxes below show how shipping companies try to evade sanctions.

Example 1

North Korean shipping company Ocean Marine Management Company (OMM) was blacklisted by the UN for arranging an illegal shipment in defiance of UN sanctions against the country's nuclear tests and missile launches. OMM responded by setting up single-ship-owner companies and changing the names of its vessels to avoid the sanctions.

OFAC also published updated guidance for the global shipping industry on the deceptive shipping practices used by North Korea to evade US and UN sanctions. North Korea used such practices to obfuscate the identities of vessels and cargo, including origin and destination, and included:

- disabling or manipulating automatic identification systems
- physically altering vessel identification
- ship-to-ship transfers to conceal the origin or destination of transferred cargo, and
- falsifying cargo and vessel documents.

Example 2

A freighter with a Hong Kong flag stopped in the South African port of Durban. The stop was not on the ship's usual route and it stayed for only one hour. It picked up a speedboat, armed with torpedoes, that was later used as a fast-attack craft in the Persian Gulf.

When it left Durban for Bandar Abbas the ship was named 'Diplomat'. Six months earlier it had been part of a state-owned fleet of the Islamic Republic of Iran Shipping Lines, known as IRISL. It went on to be renamed 'Amplify' and was spotted in Karachi.

IRISL disguised the true ownership of vessels using Western-sounding names and shell companies to avoid sanctions and continue with prohibited activity, including obtaining weapons.

The US and EU subsequently imposed sanctions on IRISL and associated shipping connections. The sanctions were ruled invalid by the European Central Court, but in 2015 the EU took steps to re-list IRISL (as reported by Lloyd's List).

Sanctions evasion red flags and typologies

The UAE Executive Office for Control and Non-Proliferation has detailed a number of sanctions evasion red flags and typologies for terrorist and proliferation financing.

Some of these red flags mirror those that we have previously discussed, but it is important to reiterate these.

Terrorist Financing – Sanction Evasion Red flags and Typologies

- *Carrying out cash withdrawals in short succession (potentially below the daily cash reporting threshold) across various locations in territories where sanctioned people have influence or are on the border of sanctioned countries.*
- *Funds are sent or received via international transfers from or to higher-risk locations.*
- *Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.*
- *The use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and funnel funds to a small number of foreign beneficiaries.*
- *Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.*
- *Individual or entity's online presence supports violent extremism or radicalisation.*
- *Irregularities during the CDD process which could include, but is not limited to:*
  - *Inaccurate information about the source of funds and/or the relationship with the counterparty.*
  - *Refusal to honour requests to provide additional KYC documentation or to provide clarity on the final beneficiary of the funds or goods.*
  - *Suspicion of forged identity documents*
- *Transactions involve individual(s) or entity(ies) identified by media and/or Sanctions List as being linked to a terrorist organization or terrorist activities.*
- *The use of funds by a non-profit organization is not consistent with the purpose for which it was established.*
- *Client donates to a cause that is subject to derogatory information that is publicly available*

(e.g., crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).

Proliferation Financing - Sanction Evasion Red Flags and Typologies

- Dealings, directly or through a client of your client, with sanctioned countries or territories where sanctioned persons are known to operate.
- The use of shell companies through which funds can be moved locally and internationally by misappropriating the commercial sector in the UAE.
- Dealings with sanctioned goods or under embargo. For example:
  - Oil or other commodities
  - Dual-Use items (wire nickel, inverters, etc.)
- Identifying documents that seemed to be forged or counterfeited.
- Identifying tampered or modified documents with no apparent explanation, especially those related to international trade.
- The activity developed or financed does not relate to the original or intended purpose of the company or entity. For example:
  - For companies, they are importing high-end technology devices, but they are registered as a company that commercializes nuts.
  - For a non-profit organization, they are exporting communication devices, but they are an entity aimed to provide health services.
- Very complex commercial or business deals that seem to be aiming to hide the final destiny of the transaction or the good.
- Complex legal entities or arrangements that seem to be aiming to hide the beneficial owner.

Source: www.uaeiec.gov.ae/en-us/un-page?p=3

Self-assessment questions

Congratulations, you have reached the end of Unit 5. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, continue or alternatively, you can work through the section again if you wish.

1. As per the requirements for Designated Non-Financial Businesses and Professions in the UAE, what action is required if a transaction is linked to a confirmed match to persons or entities designated under UNSCR 1718 (2006) and 2231 (2015)?
    a) The transaction should be processed as usual, then raise a Funds Freeze report via GoAML within 5 business days
    b) The account should be closed immediately and a Funds Freeze Report submitted within 30 days
    c) Raise a Funds Freeze Report via GoAML within 5 business days from implementing any freeze measures. (correct answer)
    d) Raise a Funds Freeze Report via GoAML within 30 days from implementing any freeze measures
2. Which of the following is a potential red flag indicating possible sanctions evasion?
    a) Regular and consistent business transactions
    b) Rapid movement of funds
    c) Transactions involving low-risk jurisdictions
    d) Use of traditional payment methods
3. Which of the following are consequences of breaching sanctions?
    a) Monetary fines and potential imprisonment (correct)
    b) Loss of business licenses (correct)
    c) Reputational damage (correct)
    d) Increased scrutiny from regulatory bodies (correct)

Correct answers 1??, 2b, 3a,b,c,d

Unit 6: Governance Framework/ Internal Controls

Learning Objectives

The purpose of this learning material is to:

- detail the responsibility of senior management/staff
- describe the role of the compliance officer
- explain how to implement an effective AML/CFT programme, and
- discuss the importance of ongoing employee training and a culture of compliance.

In order for the AML/CFT framework of any organisation to be effective, it must be based on the foundation of a sound governance structure and held together by a strong compliance culture. DNFBPs should make sure they possess management structures which are accountable for clear money laundering/terrorist financing risk management and mitigation measures, as well as appropriate independent control functions. Let's look at the different functions that help to establish a sound governance framework.

The responsibilities of the senior management/staff

Before we look at the role of the compliance function, we need to consider who is ultimately responsible – or accountable – for compliance in any organisation. This falls to the board of directors of the firm or organisation.

The role of the board

Let's start by looking at the role of the board. It is worth noting that for many DNFBPs in the UAE, the owner of the company acts as the MLRO or the compliance officer, and therefore should take into consideration the following points.

Accountability for compliance

Neither the head of compliance (or the compliance officer) or members of the compliance function are

accountable for a firm's compliance with the regulations. Compliance with the regulations in almost all jurisdictions is the accountability of the governing body of the firm, which typically is the board of directors. While ongoing activities and tasks to achieve regulatory compliance, and responsibility for establishing compliance policy and procedures, may be delegated to the compliance officer/head of compliance and their team, the ultimate accountability for being compliant remains with the board, and it is the board that a regulator will hold accountable should a firm be found to have breached the regulations.

Therefore, the board is accountable for compliance within the firm.

Setting the tone – corporate governance and compliance

You may have heard of the expression 'the tone from the top.' This relates to the culture or standards set by the board. For financial services firms and DNFBPs, the board is accountable for leading by example and setting a culture of compliance with the regulations. This involves a number of important aspects:

- making decisions and acting in line with regulations, and being seen to do so
- having reward structures that focus on positive, ethical, and compliant behaviours
- taking compliance accountabilities seriously by receiving and reviewing regular reports from the compliance officer/head of compliance on the levels of compliance within the organisation, and
- taking action where non-compliance is found, whether this be by ratifying a change in protocol, standard or approach so that it meets with the regulations, agreeing to compensation if customers have been affected, or by taking direct action against an individual responsible for breaching company policy. By showing that non-compliance will not be tolerated, the board sends a powerful message to its employees.

All these aspects link back to the way the firm is managed and governed. This is known as corporate governance. Corporate governance within a firm is vital to its success. It can be defined as the system of processes, policies,

principles, and general mechanisms that direct and control the way in which a firm is managed and run. Both direction and control are important because it refers to the ongoing management of the business as well as achieving strategic objectives. It also includes the relationships among the many different stakeholders of a firm (for example the board, employees, shareholders, customers, etc.).

Good corporate governance will enable a firm to achieve its long-term objectives and be successful in its business, while being in control of its ongoing activities. Compliance with regulations and discipline in following agreed internal standards and protocols, at all levels of a firm, is essential for this to happen.

Since 2001, corporate governance has had a very high profile, with failures in governance being seen as a significant contributing factor to the failure of many firms, such as Enron. In response to the failure of Enron, in 2002 the US government passed the Sarbanes–Oxley Act to restore public confidence in the way that firms are run by setting out strict requirements on the personal responsibility and accountability of senior management for compliance with regulatory requirements.

Further changes to corporate governance codes and regulations were introduced following the Credit Crisis.

Conduct considerations

In order to support good conduct within firms, strong leadership and management is needed. Boards should ensure that management levels and structures are sufficiently robust to be able to closely monitor and control conduct risks throughout the firm and should establish committees to oversee ethics, conduct and product suitability. In addition to this, some firms have created cross functional senior management committees to establish and monitor codes of conduct, policies and procedures which apply across the entire organisation.

In addition to this, value can be added through well-defined and clearly articulated risk and compliance ownership roles and responsibilities. If the roles and responsibilities satisfy these requirements of ownership and articulation, individuals in these roles are held accountable for conduct risk management. Reinforcing accountability is of considerable importance, both to firms and to regulators.

Management of conduct risk must be effective. Firms are establishing more and more initiatives which are specifically designed to strengthen conduct risk processes and controls and are treating it as one of their principal risk types. This represents a significant investment of time and resources across the industry as a whole.

The role of the compliance function

Before we progress on this topic, it is first worth understanding the differences between the roles of the compliance function and the compliance officer in the banking sector, and the similar roles within DNFBPs.

In the banking sector, compliance officers might focus on specific areas such as AML monitoring, sanctions enforcement or client onboarding. Each of these roles involves distinct tasks and responsibilities that align with the segmented operational structure typical in larger financial institutions. However, MLROs in DNFBPs often find themselves doing all of these roles. They are not only responsible for overseeing daily compliance activities but also for the development and implementation of the overall compliance strategy. This includes drafting and updating policies, conducting comprehensive risk assessments, governance practices and ensuring that the business remains compliant with UAE regulations which may change frequently and require quick adaptation.

This significant difference in roles can sometimes be overlooked by professionals moving from the banking sector to DNFBPs, leading to misunderstanding about the scope of their new responsibilities.

Overall, the role of the compliance function is to help the firm to identify, measure and manage compliance and regulatory risks effectively. It achieves this by providing a framework to the business that enables it to comply with the regulations set out by legislators and regulators in the applicable jurisdiction/s, and the voluntary codes to which the firm subscribes. The key to this is to act as an enabler: helping the business to help itself. Responsibility for managing compliance and regulatory risk rests with the first line and involves business units assessing and controlling their own risks. We must also remember that the business owns its compliance and regulatory risk, and not the compliance function.

Definition of compliance risk

In the context of financial services and DNFBPs, this risk can be defined as:

'The risk of legal or regulatory sanctions and the reputational and financial loss that may be suffered as a result of a failure to comply with laws, regulations and other standards of good practice.'

Source: www.bis.org/publ/bcbs142.pdf

Helping a firm to manage compliance risk can, of course, mean recommending against a preferred course of action, or highlighting a rule that would prevent a certain activity from taking place or a new idea being pursued. This makes the role of the compliance function a challenging one; team members must be prepared to be unpopular from time to time in order to protect the interests of the firm as a whole.

Compliance management arrangements and the role of the compliance officer

In performing its role to mitigate compliance risk, the compliance function will carry out many activities. In this section, we will explore the key services and activities it carries out and the main processes and procedures requiring compliance oversight. An effective way of looking at this is that all compliance professionals must fulfil the role of being a **risk steward** for the business. These key compliance activities illustrate what this means in practice for compliance professionals.

Setting and communicating compliance policy and guidance

The compliance function is generally responsible for setting compliance policy and then guiding the business on the application of this policy. It is important that detailed operational procedures are owned by the part of the business that uses them, but the compliance function should help when regulatory requirements must be contained within procedures. Before setting policy on matters of strategic interest, appropriate liaison should take place with senior management.

Compliance plans

The compliance function should carry out its activities according to a formal plan, which should be risk based and

subject to oversight by the board or senior management. The plan should be updated annually but should be subject to frequent review.

Compliance risk assessment

The compliance function should identify (or support the identification of), document and assess the compliance risks arising from the firm's business operations and provide (or obtain) appropriate resources to oversee these risks. This can be done in various ways, for example through attendance at appropriate committee meetings, effective monitoring activities, performing risk and control assessments and, probably most importantly of all, encouraging all staff to proactively raise potential risks with the compliance function.

The compliance function should also consider ways to measure compliance risk, such as by setting appropriate performance indicators and using technology to measure and monitor performance in the areas identified. Examples of monitoring could include looking at customer complaints, internal reporting lines, irregular trading patterns or payments activity.

In the UAE

Section 8, Article (21) of the Cabinet Decision No. (10) of 2019 Concerning the Implementing of Decree Law (20) outlines the requirements for DNFBPs in the UAE to appoint a compliance officer, as well as detailing the tasks and responsibilities of the compliance officer. The Article states the following.

Financial Institutions and DNFBPs shall appoint a compliance officer. The compliance officer shall have the appropriate competencies and experience and under his or her own responsibility, shall perform the following tasks:

1. *Detect Transactions relating to any Crime.*
2. *Review, scrutinise and study records, receive data concerning Suspicious Transactions, and take decisions to either notify the FIU or maintain the Transaction with the reasons for maintaining while maintaining complete confidentiality.*
3. *Review the internal rules and procedures relating to combating the Crime and their consistency with the Decretal-Law and the present Decision, assess the extent to which the institution is committed to the application*

of these rules and procedures, propose what is needed to update and develop these rules and procedures, prepare and submit semi-annual reports on these points to senior management, and send a copy of that report to the relevant Supervisory Authority enclosed with senior management remarks and decisions.

4. *Prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organisations, and the means to combat them.*
5. *Collaborate with the Supervisory Authority and FIU, provide them with all requested data, and allow their authorised employees to view the necessary records and documents that will allow them to perform their duties.*

DNFBPs must take all appropriate steps to identify and to prevent or manage conflicts of interests between:

- *The DNFBP, its personnel including its compliance officer, or any other representatives, including any person who is directly or indirectly associated with the organisation and who has control to make decisions, and the DNFBP's customer.*
- *The compliance officer and senior management of the organization including the Board of Directors. The compliance officer must be independent and must hold a position of sufficient seniority within the organisation, to ensure informed decisions are made without undue pressure to challenge decisions that are considered ill-suited, to protect the organisation from possible ML/TF abuse. The MLRO's independence of judgement is required to be free from conflicts of interest, whether it is pecuniary or otherwise.*

The AML-CFT Decision also details that the appointment of a person to the position of compliance officer requires the prior consent of the relevant Supervisory Authority. Some DNFBPs might also appoint a Money Laundering Reporting Officer (MLRO).

When determining the competencies, level of experience, and reporting structures of a firm that are appropriate for their compliance officers, DNFBPs should take several factors into consideration, these include but not limited to:

- *the results of the National Risk Assessment and other topical risk assessments*

- *the nature, size, complexity, and risk profile of their industries and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve*
- *the organisation's governance framework and management structure, with particular consideration given to the independent nature of compliance as a control function*
- *The specific duties and responsibilities of the compliance officer's role.*

(Source: www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf/0557c726-d8a7-ea63-594b-10110e300dc8?t=1633853458984)

Implementing an effective AML programme

Any strategy to protect a business against exposure to money laundering must begin with the formulation and adoption of an AML policy that is approved at the most senior level within an organisation.

This policy serves as a clear statement of corporate intent that can be communicated to:

- employees
- clients
- regulatory authorities, and
- law enforcement bodies.

Such policies serve as a valuable indicator of effective corporate governance.

Key learning point

An organisation's attitude towards combating money laundering is increasingly viewed as indicative of the ethics with which it conducts its business.

Pressure for the financial and DNFBPs sectors to avoid money derived from or destined to fund crime was given enormous impetus by the tragic events of 11 September 2001 and subsequent allegations that firms had facilitated the attacks by providing services to the terrorists.

An appropriate statement of corporate intent in the form of an AML policy, supplemented with meaningful and effective procedures, allows an organisation to communicate its attitude clearly. Never before has it been as important for DNFBPs to do so unequivocally.

The content of a policy

The content of an AML and CFT policy requires very careful consideration. Too often businesses simply pay external advisers to draft policies that are then adopted at board level without any internal consideration or discussion. Such policies do little more than 'window dress'.

In formulating a policy, management must first decide on what the organisation wishes to achieve by its adoption, and consider a variety of factors, including:

- the nature, scale and complexity of its business
- the diversity of its operations, including geographical diversity
- the volumes and sizes of its transactions, and
- the degree of risk associated with each area of its operation.

As a bare minimum, management will wish to achieve:

i. compliance with laws and regulations and best-practice guidance (including all procedural obligations)

ii. cooperation with law enforcement and investigating authorities where necessary

iii. respect for client confidentiality

iv. clearly defined responsibilities and accountabilities for money laundering prevention within the business

v. a statement of the organisation's willingness to provide sufficient resources for money laundering prevention

vi. the acceptance of new business subject to compliance with appropriate CDD and risk-assessment procedures

vii. the continuation of existing business only where such business meets appropriate CDD, risk-assessment and monitoring procedures

viii. a statement of the approach to the education, training and awareness maintenance of all staff and management

ix. a statement of the organisation's attitude towards persistent non-compliance with AML procedures, and

x. an indication of the prevailing cultural attitude that the organisation wishes to create towards money laundering prevention.

It is always open to a business to exceed these minimum compliance principles by deciding to implement procedures or customer acceptance practices that exceed the minimum requirements laid down by the laws of a particular jurisdiction.

Where an organisation has a presence in more than one jurisdiction, it is sensible for it to adopt 'Global Standards', which, as a minimum, meet the standards of the most stringent national framework with which it has to comply.

Choosing between the AML frameworks of different jurisdictions (sometimes known as 'jurisdiction shopping' or 'regulatory arbitrage') by rejecting business in one jurisdiction and accepting it in another through a company within the same group, is short-sighted.

While the laws of the various jurisdictions in which an organisation has a presence may differ slightly, the risks of being exposed to criminally derived property are the same in each. In addition, many regulatory regimes (such as the Third EU Money Laundering Directive) require firms to ensure that all their branches and subsidiaries, wherever located, operate to the standards applicable in the firm's home jurisdiction.

AML/CFT policies and procedures

An appropriate policy needs to be supplemented by specific AML procedures. Some of these procedures, as we have seen, are required in order to satisfy the requirements of legislation or guidance. Others are designed to help an organisation to take more robust action against the threat of money laundering.

In designing an effective internal AML regime, a compliance officer should consider procedures to cover the following requirements.

The establishment and satisfactory verification of the identity of all clients (natural persons or legal entities), including:

- any person with a current or contingent beneficial interest in the property handled by the organisation, or
- any person who is able to exercise control over the property, including name, date of birth, nationality, place of birth and permanent address.

Documented CDD information on all clients, including the following.

- Source of funds
- Source of wealth
- Commercial rationale for the relationship
- Occupation
- Nature of business interests, etc.
- Identity of any beneficial owner(s)

Risk assessments of prospective clients with reference to a range of factors, including:

i. geography (residence, location of business interests, location of assets), e.g. whether a country which has been known to fund or support terrorism or produce or transit drugs, features

ii. nature of business interests

iii. any sensitive activities as defined by regulatory authorities

iv. value of assets or property to be handled by the business

v. type of client, e.g., a PLC or a high-net-worth individual

vi. the nature of the client, e.g. if a high-net-worth individual, is the client a PEP?

vii. type of property or nature of assets that the business is being asked to handle

viii. if the client has been introduced, the source of the introduction

ix. if an intermediary or introducer is to be involved in the relationship, whether they are regulated, are based in an equivalent jurisdiction and can be trusted to

act as a gatekeeper to your organisation and if so, the reasons for this

x. the nature of the service that the business is being asked to provide, and

xi. the complexity of the proposed arrangement.

The requirement for independent authorisation to be granted prior to the acceptance of new clients.

- Documented client acceptance procedures.
- Verification of intermediaries or introducers of business.
- The creation of CDD profiles taking into account each of the factors outlined above.
- 30-, 60- or 90-day client reviews to ensure consistency of activity with information contained in the CDD profile.
- Risk-based monitoring of relationship activity.
- Enhanced due diligence procedures for clients deemed to pose increased risk.
- Automatic transaction-based reporting for unusual transactions.
- Annual client reviews, preferably conducted other than by the person responsible for the relationship.
- A meet-the-client policy.
- A written internal reporting system for suspicious transactions or relationships.
- Dual authorisations policy.
- Requirement for full supporting documentation on all payment requests.
- Checklists for receipts and payments of funds triggering close analysis of any exceptional fund movements or movements of funds from or to financial institutions in former or non-equivalent jurisdictions: those listed as non-cooperative countries or territories (NCCTs) by FATF, for example.
- Annual MLRO reports to the board providing an update on the status of risks and controls.

- Maintenance of a register of Powers of Attorney or any other form of delegated authority (e.g., third-party signatories on accounts).
- Procedures for the management and security of files relating to suspect client relationships.
- Procedures for the management of communications between suspect clients and their advisers.
- A PEP policy including, for example, requirement of board approval for acceptance of any PEPs.
- A procedure for exceptions and deviations from AML procedures that requires independent internal risk assessment and approval.
- A comprehensive education strategy for all new and existing employees supplemented by an awareness-maintenance programme.
- Procedures for the verification of the level of staff awareness and competence.
- Staff minimum annual leave requirement.
- AML audits.
- Regular cross-checking of names of clients and assets (where the assets are legal entities such as companies or foundations) to lists of named suspects or embargoed jurisdictions or those subject to sanctions.
- Monitoring of all fund transfers from or to accounts in jurisdictions not compliant with FATF Recommendations or other high-risk jurisdictions and from or to shell banks.
- Verification of signatures procedure.
- Recordkeeping procedures.

Important

Once an AML framework is in place it needs to be continually monitored, tested, reported upon and adjusted. An effective internal system of control is not fixed or a one-off event; instead it is dynamic and constantly evolving to take account of changing threats and emerging weaknesses.

Screening procedures to ensure high standards when hiring employees

One of the easiest ways to establish an effective compliance culture in a firm is to ensure that employees and job applicants are screened appropriately so as to recruit those who are likely to demonstrate the behaviours desired by the firm. Managers and those in high-risk positions should be subject to appropriate 'fit and proper' tests.

Many regulators set their own fit and proper standards regarding previous experience and any bankruptcy or criminal convictions, and firms are required to carry out extensive due diligence on employees going back several years to avoid 'bad actors' from repeating poor or criminal behaviours.

In addition, it is important to conduct thorough interviews with applicants to ensure that they have adequate skills to perform their duties and display the behaviours that align with the firm's compliance culture.

Ongoing employee training programme and culture of compliance

The compliance function should ensure that all employees are fully aware of their individual compliance responsibilities by:

- educating and updating all employees on compliance issues as required
- keeping employees up to date on regulatory developments
- acting as the point of contact for compliance queries, and
- establishing written guidance on the appropriate implementation of compliance requirements.

In reality, training is usually delivered by the training, or learning and development teams in firms, with the content being the responsibility of the compliance function. This means that the compliance professional will need to work with these teams to help with the design and development of compliance related training.

There are different training 'phases' such as: induction training, which is the ideal opportunity to introduce the

new starter to the firm's compliance culture and values; routine training, for employees on compliance matters; specialist training, for employees with more high-risk roles where the training has to be kept up to date; and annual or mandatory training, for all employees (covering such subjects as bribery and corruption, anti-money laundering, gifts and hospitality, health and safety, etc.).

Finally, what counts as being training and education? Is it just the formal, written or 'presented' training like intranet-based training? Or could training and education encompass anything which increases the knowledge and understanding of the recipient? Training can be face to face or online using technology such as computer-based training, the firm's intranet, Zoom or Teams. Understanding and competence should be tested at the end of the session. Encouraging feedback from both attendees and tutors can provide valuable insights into areas of success and improvement.

Alternatively, training and education can also be informal and take the form of ad-hoc advice. For example, a conversation with a business colleague during which an interpretation of regulation or some evidence to support a view on a proposed commercial development is provided, and so on, could all be classified as informal training and education.

In the UAE

In the UAE it is the responsibility of the compliance officer to:

Prepare, execute and document ongoing training and development programs and plans for the institution's employees on Money Laundering and the Financing of Terrorism and Financing of Illegal Organisations, and the means to combat them.

DNFBPs should ensure that their employees are kept up to date on an ongoing basis in relation to emerging ML/FT typologies and new internal and external risks. Depending on the nature, size and level of complexity of a DNFBP, a DNFBP should also screen staff to ensure high standards when hiring employees.

To ensure a high level of competence and AML/CFT programme effectiveness, DNFBPs should formulate and implement appropriate policies, procedures and controls with regard to staff screening and training. An effective training program

should not only explain the relevant AML/CFT laws and regulations, but also cover the institutions' policies and procedures used to mitigate ML/FT risks, scope of target employees such as but not limited:

- *customer-facing staff*
- *AML/CFT compliance staff*
- *Senior management and board of directors*

These measures should be applied across organisations and financial groups, including their foreign branches and majority-owned subsidiaries. Examples of some of the factors that should be considered when determining appropriate staff screening and training measures include, but are not limited to:

- *the results of the National Risk Assessment and other topical risk assessments*
- *the nature, size, complexity, and risk profile of DNFBPs' sectors and businesses, as well as those associated with the products and services they offer and the markets and customer segments they serve*
- *effective screening and selection methods in relation the AML/CFT cultural compatibility of their employment candidates*
- *assessment of staff AML/CFT competency in relation to training and development needs*
- *the type, frequency, structure, content, and delivery channels of AML/CFT training programmes and development opportunities*
- *the effective identification, deployment and management of both internal and external training resources*
- *appropriate methods and tools for assessing the effectiveness of staff hiring, training, and development programmes, including screening procedures to ensure high standards when hiring employees.*

(Source: www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf/0557c726-d8a7-ea63-594b-10110e300dc8?t=1633853458984)

Implementing a culture of compliance

The term 'compliance culture' has been in regular use in recent years, but do we really understand what it means? If asked, could you provide a simple definition? And why should we be concerned with how compliance sits within our firm's broader culture?

How do you define, develop and advise on an effective compliance culture?

We need to define the term 'compliance culture' so that everyone agrees exactly **what** it is and **why** it is so important. Other important questions are: how do you measure it? What can you do to improve it? How do you embed it?

So, with this in mind, let's take a look at the definition of compliance culture.

There is no one definition of a 'good' compliance culture, as 'good' is a variable term dependent upon circumstances. However, a powerful definition developed by the ICA is that 'a good compliance culture is one where everyone wants to be compliant'. The key word in this definition is of course 'wants'. If you can get everyone in your organisation to want to be compliant then you are well on your way to being so. The crucial step is therefore to find ways to make all colleagues want to be compliant, and to identify ways to motivate them accordingly.

This brings us back to the term 'the benefits of compliance'. If you can show people the benefits that good compliance brings then they are far more likely to be receptive. This is particularly true if you can make these benefits personal to them, such as through reward and remuneration, remembering that reward does not have to be financial.

Links between compliance, culture and ethics

It is not enough for firms to only put in place processes that merely meet regulatory rules. Firms must also have a compliance culture that ensures that all individuals understand and embrace adherence to these processes and the spirit or principles behind the underlying rules.

The culture must be one that ensures that the values at the heart of internal processes and practices are based on the best interests of customers and other stakeholders.

It is worth reiterating that such a culture should be in place not only to facilitate the achievement of compliance and the maintenance of regulatory relationships, but also to enhance commercial ones. Where a firm is associated with poor compliance or unethical behaviour, this will have a knock-on effect on its reputation and could influence consumers' buying decisions.

Increasingly, customers vote with their feet and choose to engage with businesses that they believe have higher moral standards or cultural values. Some organisations when conducting due diligence exercises, before entering into contracts with other firms, will ask questions about their attitudes towards compliance with regulations, and will request details of actions taken to meet specific regulatory requirements. The response to such questions will have an influence on any decision to do business or be associated with that firm.

One of the key enforcement mechanisms that regulators use for non-compliant behaviour is the issue of public censures – or 'naming and shaming'. Due to the reputational damage inflicted, public censures are potentially more damaging to a firm than any size of fine that could be imposed. Certainly, with the extent of the financial services market today – and indeed any other sector's market – the choices available to customers are wide ranging. As a result, ethical practices and a culture of compliance can be a significant competitive advantage for a firm.

The question of how to develop the culture and ethics (and consequently the behaviours) that senior management want all their employees to demonstrate is a difficult one to answer. The 'tone from the top' – or the standards that the board wants to exemplify – needs to be seen, understood and the benefits demonstrable to all employees so the buy-in can be generated. The board and senior managers need to 'walk the walk' as well as 'talk the talk' to set examples to all employees.

However, commercial pressures can mean that the messages could be in direct conflict with the responsibility to deliver business results that is held by middle managers. This layer of middle management can be very influential

because their task is to manage the front-line employees that quite often are the main points of contact with consumers. So, it is important to gauge the success of the cascading of cultural and ethical standards at this middle level, for example by assessing the question of what is the 'mood in the middle'?

Practical steps

The firm's control environment sets its moral tone and compliance culture. A key element of a firm's compliance culture is whether managers and employees within the firm exhibit integrity in their day-to-day activities. There are several actions that management can take to establish the proper control environment for a business, including the steps outlined below.

Establishing of a code of ethics/conduct for the firm

The code should be explained to all employees, and every new employee should be required to read and sign it. The code should also be followed by contractors who do work on behalf of the firm. Under certain circumstances, firms may face liability for the actions of independent contractors. It is therefore particularly important to explain the firm's standards to any outside party with whom it conducts business.

Careful screening of job applicants

As we have previously discussed, one of the easiest ways to establish an effective compliance culture in a firm is to ensure that employees and job applicants are screened appropriately so as to recruit those who are likely to demonstrate the behaviours desired by the firm.

Proper assignment of authority and responsibility

In addition to hiring qualified, ethical employees, it is important to enable employees to succeed without behaving unethically. Firms should provide employees with well-defined job descriptions and performance goals that are not overly reliant on achieving financial targets at the expense of good compliance. Performance goals should be routinely reviewed to ensure that they do not encourage poor practices.

Effective disciplinary measures

No control environment is effective unless there is a consistent disciplinary process to deal with non-compliant behaviour. This requires a well-defined and communicated performance management framework which strictly and consistently follows the prescribed disciplinary measures. If one employee is punished for an act and another employee is not punished for a similar act, the value of the company's ethics policy is diminished. The levels of discipline must be sufficient to deter poor behaviours. It is also advisable to reward ethical conduct, to reinforce the importance of organisational ethics in the eyes of employees and demonstrate that personal benefits are the keys to creating a compliance culture.

Independent audit function to test the system

The audit function plays a pivotal role in an effective compliance programme. This function is responsible for evaluating the efficacy of a company's internal control systems, accounting practices, and compliance with regulations. The audit function primarily aims at ensuring the accuracy and reliability of financial and non-financial information, promoting operational efficiency, and fostering adherence to managerial policies.

The audit function is essentially a watchdog mechanism that oversees corporate activities, identifies potential risks, and recommends measures to manage them effectively. It is conducted by internal or external auditors who have a deep understanding of the company's operations, the industry it operates in, and the regulatory environment.

Internal audit

The internal audit function typically has responsibility for assessing the appropriateness and effectiveness of business-wide systems and controls. While the independence of internal audit must be maintained, compliance monitoring activities can be used as triggers for internal audit review work, and vice versa.

External audit

External auditors are independent entities hired to perform audits. They provide an unbiased and objective view of the

company and its compliance with laws and regulations. They play a significant role in enhancing the credibility of the company and providing confidence to stakeholders.

The audit function forms an integral part of the compliance programme as it provides assurance that the company is operating within the boundaries of law and in accordance with established policies and procedures. Regular audits help in identifying compliance issues before they become serious problems and provide an opportunity to correct them timely.

Furthermore, the audit function plays a critical role in enhancing corporate governance by ensuring transparency, accountability, and integrity in a company's operations. It helps in building trust and confidence among stakeholders including investors, customers, and regulators.

In the UAE

DNFBPs are obliged to have in place an independent audit function to test the effectiveness and adequacy of their internal polices, controls and procedures relating to combating the crimes of money laundering and the financing of terrorism and of illegal organisations. DNFBPs therefore should ensure that their independent audit function is appropriately staffed and organised, and that it has the requisite competencies and experience to carry out its responsibilities effectively, in line with the ML/FT risks to which the DNFBPs are exposed, and with the nature and size of their businesses.

Depending on the nature and size of the business, some DNFBPs, in particular smaller ones, may not necessarily have the resources to maintain a fully functioning and effective internal audit unit. In these instances, those DNFBPs should ensure that they take adequate measures to obtain the necessary capabilities from qualified external sources. It is also important to also ensure that they have adequate internal capabilities in place to provide sufficient coordination with and oversight of any external resources they may utilise, and that such external resources are adequately regulated and supervised by relevant Competent Authorities.

The periodic review and testing of DNFBPs AML/CFT compliance programmes, including ML/FT business risk assessment and AML/CFT mitigation measures, and CDD policies, procedures and controls, should be incorporated into their regular audit plans. All branches and subsidiaries should also be included in the audit.

Some of the factors DNFBPs should consider in determining the appropriate frequency and extent of audit testing of their AML/CFT programmes by their independent audit functions include but are not limited to:

- *The results of the National Risk Assessment and other topical risk assessments*
- *The nature, size, complexity, and geographic scope of the DNFBPs' businesses, and the results of their ML/TF business risk assessments*
- The risk profile associated with the products and services they offer and the markets and customer segments they serve
- The frequency of supervision and inspection by, and the nature of the feedback (including the imposition of administrative sanctions) they receive from, Supervisory Authorities, relative to enhancing the effectiveness of their AML/CFT measures
- Internal and external developments in relation to ML/FT risks, as well as developments pertaining to the management and operations of the DNFBPs.
- The scope of such audits should include but not be limited to:
- Examine the adequacy of AML/CFT and CDD policies, procedures and processes, and whether they comply with regulatory requirements
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule, attendance tracking and escalation procedures for lack of attendance.
- Review all the aspects of any AML/CFT compliance function that have been outsourced to third parties, including the qualifications of the personnel, the contract and the performance and reputation of the company.
- Review case management and STR systems, including an evaluation of the research and referral of unusual transactions, and a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines to the personnel responsible for investigating unusual activity.

(Source: www.moec.gov.ae/documents/20121/469920/AMLCFT+Guidance+for+DNFBPs.pdf/0557c726-d8a7-ea63-594b-10110e300dc8?t=1633853458984)

Self-assessment questions

Congratulations, you have reached the end of Unit 6. Let's take a moment before we move on to do a quick knowledge check. If you are ready to do this, **continue** or alternatively, you can work through the section again if you wish.

1. Who is ultimately responsible for compliance within an organisation?
   a) The board of directors
   b) The head of compliance
   c) The compliance officer
   d) The employees
2. Which three of the following are roles of the compliance function within an organisation?
   a To identify and measure compliance and regulatory risks (correct)
   b) To set compliance policy and guide the business on its application (correct)
   c) To ensure all employees are aware of their individual compliance responsibilities (correct)
   d) To observe external auditors during compliance reviews
3. What is a key element of a firm's compliance culture?
   a) The existence of a compliance policy
   b) The use of automated screening methods
   c) The extent of the firm's business operations
   d) The demonstration of integrity in day-to-day activities by managers and employees

Correct answers 1a, 2a,b,c, 3d