



**SOUTH ASIAN FEDERATION OF ACCOUNTANTS
(SAFA)**



**ANTI – MONEY
LAUNDERING BEST
PRACTICES FOR
ACCOUNTANTS**

(Version II)

MESSAGE FROM PRESIDENT

SOUTH ASIAN FEDERATION OF ACCOUNTANTS (SAFA)



It is with great pleasure that I announce the release of the second version of the "AML Best Practices Booklet for Accountants."

As a professional organization committed to promoting excellence and integrity in the accounting profession, SAFA recognizes the critical role that accountants play in combating money laundering and terrorist financing. This updated booklet serves as a comprehensive guide, equipping accountants with the necessary knowledge and tools to effectively address the challenges posed by these illicit activities.

The AML Best Practices Booklet for Accountants offers practical guidance and insights, highlighting the latest international standards and best practices in the field of anti-money laundering (AML). It covers a wide range of topics, including risk assessment, customer due diligence, suspicious transaction reporting, and internal controls. By adhering to these best practices, accountants can enhance their ability to detect and prevent financial crimes, thereby contributing to the overall integrity and stability of our financial systems.

I would like to extend my heartfelt appreciation to the SAFA AML Committee for their dedicated efforts in producing this invaluable resource. Their expertise and commitment to promoting AML awareness and compliance have been instrumental in the development of this booklet.

I extend my sincere thanks to the SAFA AML Committee and all stakeholders for their unwavering support and commitment to promoting excellence and integrity in the accounting profession. Together, we can make a significant impact in the fight against financial crimes and contribute to a more secure and transparent future.

CA. Nihar N Jambusaria

President

South Asian Federation of Accountants (SAFA)

MESSAGE FROM CHAIRMAN

SAFA COMMITTEE ON ANTI – MONEY LAUNDERING

I am pleased to share the second version of the Best Practices document on Anti – Money Laundering and Combating Financing of Terrorism (AML / CFT) for the member countries of South Asian Federation of Accountants (SAFA).

This document includes the FATF Recommendations related to Designated Non – Financial Businesses and Professions (DNFBPs). It is pertinent to highlight that the Accountants fall under the category of DNFBPs and, therefore, they are obligated to comply with the FATF Recommendations. The second version includes details of the AML / CFT Regulations applicable in the South Asian Countries. In addition to this, the significant areas covered under the relevant regulations are also highlighted in the document.



The member countries are required to effectively implement the FATF recommendations (commonly known as FATF Standards on AML / CFT). These standards set out a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction.

This comprehensive document will help the member bodies in understanding the obligations under the FATF Regime and it is hoped that the member bodies of SAFA will strive to ensure compliance of the FATF recommendations in order to fight the menace of Money Laundering and Terrorism Financing and to strengthen the compliance regime of the entire region.

I would like to acknowledge the cooperation of the Committee members in providing Rules and Regulations related to AML / CFT applicable in their respective countries.

Khalid Rahman, FCA

Chairman – SAFA Committee on AML

FINANCIAL ACTION TASK FORCE (FATF)



The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter – governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to the society.

The FATF, is an inter – governmental body whose objectives include setting standards to combat money laundering, the financing of terrorism and the financing of proliferation of weapons of mass destruction (AML / CFT), and supporting the implementation of these standards.

The core documents of the FATF (referred to as the "FATF standards") include:

- 40 recommendations, including interpretative notes, of 2012;
- Methodology for assessing compliance of 2013; and
- Various best practice guidelines.

The FATF standards require countries, territories and regions to:

- Criminalize money laundering, terrorist financing and proliferation financing in accordance with international law;
- Freeze terrorist assets and confiscate the proceeds of crime;
- Establish a financial intelligence unit to collect, analyses, evaluate and disseminate suspicious transaction reports from financial institutions and other reporting entities;
- Supervise those financial institutions and other reporting entities to ensure compliance with customer due diligence and other requirements contained in the standards; and
- Ensure that comprehensive and effective mechanisms are in place to cooperate effectively on the international level given the growing international dimension to these crimes.

These standards have been accepted internationally as the global policy benchmark for anti–money laundering, anti–terrorist financing and anti–proliferation financing measures by the United Nations, International Monetary Fund, World Bank, Asian Development Bank and many other international organizations and bodies. The key changes to the FATF standards included in the 2012 revised version are as follows:

- Requirement for countries to undertake a national risk assessment;
- Measures relating to proliferation financing;
- Addition of tax crimes as predicate offences to money laundering;
- Measures relating to domestic politically exposed persons;
- Requirement for countries to ratify the UN Convention Against Corruption.

The FATF currently comprises 37 member jurisdictions, 2 regional organizations and 9 associate members (FATF Style Regional Bodies), representing most major financial centers in all parts of the globe.

The FATF–style regional bodies are:

1. Asia / Pacific Group on Money Laundering (APG) based in Sydney, Australia;
2. Caribbean Financial Action Task Force (CFATF) based in Port of Spain, Trinidad and Tobago;
3. Eurasian Group (EAG) based in Moscow, Russia;
4. Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG) based in Dar es Salaam, Tanzania;
5. Central Africa Anti-Money Laundering Group (GABAC) based in Libreville, Gabon;
6. Latin America Anti-Money Laundering Group (GAFILAT) based in Buenos Aires, Argentina;
7. West Africa Money Laundering Group (GIABA) based in Dakar, Senegal;
8. Middle East and North Africa Financial Action Task Force (MENAFATF) based in Manama, Bahrain;
9. Council of Europe Anti-Money Laundering Group (MONEYVAL) based in Strasbourg, France (Council of Europe).

All SAFA members are part of APG. The APG, in conjunction with the FATF and the other eight regional bodies, constitute a global network to combat money laundering, the financing of terrorism and the financing of proliferation of weapons of mass destruction. The FATF's 40 recommendations are the principal standards to combat these crimes.

SAFA MEMBER COUNTRIES

1. Afghanistan
2. Bangladesh
3. Bhutan
4. India
5. Maldives
6. Nepal
7. Pakistan
8. Sri Lanka



SAFA AML TASK FORCE COMMITTEE MEMBERS

Terms of Reference

1. The Committee on Anti Money Laundering shall;
2. Identify the best practices followed by SAFA member bodies to combat money laundering in their nations.
3. Identify the best practices which can be followed by all the SAFA member bodies.
4. Provide adequate awareness and training to the AML Experts (member of Accounting bodies) in South Asian Region for combating Money Laundering.

Committee Members

Sl.No.	Member Body	Member
1	CA Pakistan (Convenor)	Mr. Khalid Rahman
2	ICA Bangladesh	Mr. Md. Johirul Islam FCA
3	ICMA Bangladesh	Kazi Muhammad Ziauddin FCMA
4	ICA India	CA. Abhay Chhajed
5	ICA Nepal	CA. Chhetra Gopal
6	ICMA Pakistan	Mr. Aamir Ijaz Khan
7	CA Sri Lanka	Mr. Ashane Jayasekera
8	CMA Sri Lanka	Ms. Sureka Ketawala
9	ICA Maldives	Ms. Fathima Nasir
10	ICA India (erstwhile ICWAI)	CMA Vijender Sharma

LEGISLATIONS OF SAFA COUNTRIES ON COMBATING MONEY LAUNDERING / TERRORIST FINANCING

SRILANKA

- Prevention of Money Laundering Act, 2005
- Convention on the Suppression of Terrorist Financing (Amendment) Act, No. 41 of 2011
- Convention on the Suppression of Terrorist Financing (Amendment) Act, No. 3 of 2013
- Prevention of Money Laundering Act, No. 5 of 2006
- Prevention of Money Laundering (Amendment) Act, No. 40 of 2011
- Financial Transactions Reporting Act, No. 6 of 2006
- Prevention of Terrorism (Proscription of Extremist Organizations) Regulations
- Suspicious Transactions (Format) Regulations of 2017
- Financial Transactions Reporting Regulations 2008

MALDIVES

- Financial Intelligence Unit established under Section 27 of the Act
- Prevention of Money Laundering and Financing of Terrorism Act (2014)
- Maldives Monetary Authority” or “Authority” refers to Maldives Monetary Authority established under the Law no 6/81 (Maldives Monetary Authority Act)

INDIA

- Prevention of Money Laundering Act
- Prevention of Money Laundering Rules
- RBI (Master Directions)
- SEBI Rules
- IRDA Directions to Insurance Companies on Compliance with PMLA

BANGLADESH

- The Money laundering Prevention Act, 2012

AFGHANISTAN

- The Anti-Money laundering and proceeds of crime Law

PAKISTAN

- The Anti Money Laundering Act, 2010 Amendment act 2020
- AML / CFT Regulations by ICAP and ICMAP

OVERVIEW OF LEGISLATIONS

Appended below is the AML / CFT measures pertaining to DNFBPs defined in the member country's respective legislations.

BANGLADESH

- To maintain complete and correct information with regard to identity of is customers
- Retaining of record for five years
- Report STR

SRILANKA

- Responsibilities of Financial Institutions and DNFBPs
- Responsibilities of a Compliance Officer
- ML/TF Risk Assessment
- Enhanced Customer Due Diligence
- High Risk Countries
- Reliance on Third Parties
- Customer Identification, Verification, Risk Profiling
- Compliance with UNSCR
- CTR/EFT Reporting
- Reporting Suspicious Transactions
- Record Keeping
- Sanction screenings and strategic trade controls related issues
- Training, Independent Audit on AML/CFT)
- Powers and Functions of the FIU to enforce compliance
- Offences and the Penalties involved

AFGHANISTAN

- Risk Assessment
- Identification of customers and verification
- Consequences of failure to identify customers or beneficial owners
- Special monitoring of transactions and measures for high-risk countries
- Due diligence measures for politically exposed persons
- Record-keeping
- Reporting of suspicious transactions
- Internal anti-money laundering programs at reporting entities and foreign branches and subsidiaries

INDIA

- Client Due Diligence (CDD)
- Policy for acceptance of clients
- Risk-based Approach
- Record Keeping
- Monitoring of Suspicious Transaction and Reporting
- Procedure for freezing of funds, financial assets or economic resources or related services
- Reporting to Financial Intelligent Unit
- Hiring/Employee's Training
 - Verification of identity
 - Record retention
 - Access to information
 - Enhanced due diligence
 - Powers to impose fine

PAKISTAN

- Risk Based Approach to AML/ CFT
- Customer Due Diligence (CDD) and beneficial ownership
- Reliance on Third Party Financial Institutions for CDD Measures
- TFS under UNSC Act, 1948 and ATA, 1997
- Politically Exposed Persons (PEPs)
- NGO/ NPO/ Charity/ Trust Accounts
- Reporting of Transactions (STRs/ CTRs)
- Record Keeping
- New Technologies, Internal control
- Counter Measures for High Risk Jurisdictions
- Regulation and Supervision
- Sanctions

MALDIVES

- Preventive Measures
- Customer Due Diligence (CDD)
- Record Keeping
- Reporting and Monitoring
- Exemption from Liability for Licensees
- Transitional Provisions and Definitions
- Programs to Combat Money Laundering and Financing of Terrorism
- Management of confiscated funds and properties
- Third party rights
- Disclosure of Information of Financial Transactions
- Responsibilities of Supervisory Authorities
- Offences and Penalties

FATF RECOMMENDATIONS

FATF Recommendations applicable to DNFBPs sector are:

RECOMMENDATION 22 (DNFBPs: CUSTOMER DUE DILIGENCE)

The customer due diligence and record keeping requirements set out in Recommendations 10, 11, 12, 15, and 17, also apply to designated non – financial businesses and professions (DNFBPs).

- Recommendations 10 – Customer due diligence
- Recommendations 11 – Record keeping
- Recommendations 12 – Politically exposed person
- Recommendations 15 – New technologies
- Recommendations 17 – Reliance on third parties

RECOMMENDATION 23 (DNFBPs: OTHER MEASURES)

The requirements set out in Recommendations 18 to 21 apply to all designated non-financial businesses and professions.

- Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries
- Recommendation 19 – Higher Risk Countries
- Recommendation 20 – Reporting of Suspicious Transactions
- Recommendation 21 – Tipping-Off and Confidentiality

RECOMMENDATION 28 (REGULATION AND SUPERVISION OF DNFBPs)

DESIGNATED NON – FINANCIAL BUSINESSES AND PROFESSIONS (DNFBPs)

Following are the groups that fall under DNFBPs;

- Casinos
- Real estate agents – when they are involved in transactions for a client concerning the buying and selling of real estate
- Dealers in precious metals and dealers in precious stones
- 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; v managing of client money, securities or other assets;
 - management of bank, savings or securities accounts;
 - organization 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.
- 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

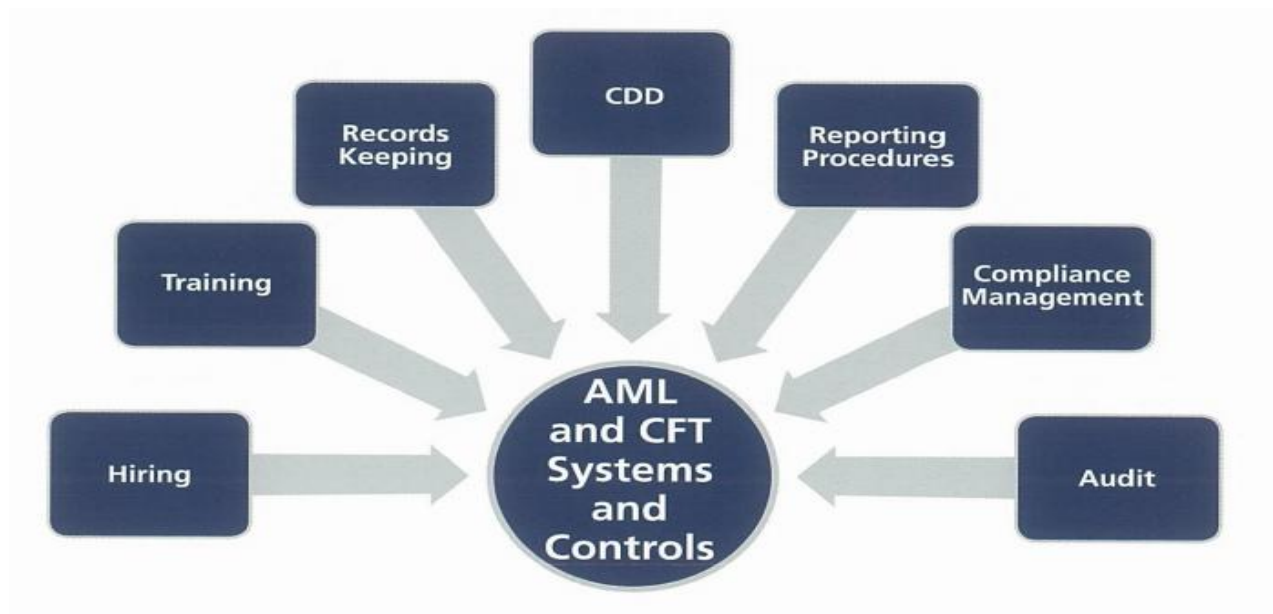
The Accountants generally carry out Trust and Company Service Providers services in many jurisdictions across the globe. Therefore, in addition to the services falls under “Accountant” services, the Accounting Profession will also be subject to compliance with FATF Recommendations if they carry out “Trust and Company Service Provider” services.

ANTI MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM

Every year, criminals launder anywhere between US \$ 800 billion and US \$ 2 trillion worldwide. The global impact is staggering. Internationally, there are increasing calls for professional accountants to adopt measures that are at least up to the international standards recommended by the Financial Action Task Force (FATF).

SUMMARY OF BEST PRACTICES FOR PROFESSIONAL ACCOUNTANTS (DNFBPs)

AT A GLANCE



A risk-based approach towards establishing AML and CFT systems and controls shall be adopted. The type and extent of the measures taken in each of the areas (see diagram above) shall be appropriate having regard to the risk of money laundering and terrorist financing and the size and nature of the business.

Customer Due Diligence (CDD)

The primary objective of CDD is to enable effective identification and reporting of suspicious activities. Unless one truly knows his clients, and well enough to understand and anticipate their behavior, one can neither reasonably nor effectively distinguish unusual suspicious activity from usual behavior.

- **Legislations with respect to CDD should at minimum cover the following aspects:**
 - When should Reporting entities conduct CDD
 - What are Required CDD measures for all customers
 - Identification and verification of Beneficial owners
 - Specific CDD measures for legal persons and legal arrangements
 - Application and Timing of CDD
 - Risk based Approach to CDD and risk profiling of customers
 - Non-compliance with CDD Requirements
 - Reliance on third parties
 - Prohibitions to provide services to designated persons and entities or their associates

- **Who to conduct CDD on:**
 - Your customer
 - Any beneficial owner of a customer
 - Any person acting on behalf of a customer

You must also complete CDD on:	Details
Your customer	<p>New Customer – Means any person engaging a reporting entity for the purposes of requesting, acquiring, or using accountant or any services or carrying out any transaction or business with the reporting entity but only for specified</p> <p>Existing customer – You must conduct CDD on existing customers if there has been a material change in the nature or purpose of the business relationship with that customer, and you have insufficient information about that customer.</p>
Any beneficial owner of a customer	<p>a) natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted; or</p> <p>(b) natural person who exercises ultimate effective control over a legal person or legal arrangement;</p>
Any person acting on behalf of a customer	<p>A person exercising a power of attorney for your customer</p> <p>A legal guardian acting on behalf of a minor who is your customer</p> <p>An employee who has the authority to act on behalf of a company that is your customer</p>

The **CDD measures** to be taken are:

- (a) Identifying the client;
- (b) Identifying the beneficial owner;
- (c) Verifying the identity of the client using reliable, independent source documents, data or information;
- (d) Verifying the identity of the beneficial owners using reasonable measures;
- (e) Understanding and obtaining information on the purpose and intended nature of the business relationship; and
- (f) Conducting ongoing due diligence on any continuing business relationship and scrutiny of transactions undertaken during the course of the relationship.

Application and Timing of CDD

The CDD measures shall be undertaken when establishing business relations; carrying out occasional transactions; when there is a suspicion of money laundering or terrorist financing; or where there are doubts about the veracity or adequacy of previously obtained client identification data. Generally, the verification of the identity of the client and the beneficial owner should be performed before or during the course of establishing the business relationship.

➤ **Non-compliance with CDD Requirements**

Where the reporting entity is unable to carry out the CDD measures, for example, due to client's refusal to provide evidence of identity or other information, business relations shall not commence/shall be terminated; and consideration shall be made as to whether a suspicious transactions report is necessary.

➤ **Risk Based Approach to CDD**

The Risk-Based Approach to CDD

All the CDD measures shall be applied. However, the extent of such measures would depend on the risks of money laundering and terrorist financing.



⁷ Politically exposed person (PEP) – An individual who is or has been entrusted with prominent public functions.

➤ **Politically exposed persons (PEP)**

In summary a PEP is a person, or an immediate family member or someone who has close business ties to that person, who holds or has held a prominent public function. This may be because they are or were a head of state, senior politician, or an official with a public profile, such as a Supreme Court Judge, or a highly ranked military official.

The following categories of PEPs should be defined:

- Foreign and domestic PEP
- Close Associate of PEP
- Family Members of PEP

- risk management systems to determine whether a customer or the beneficial owner is a PEP should be in place
- obtain senior management approval before establishing (or continuing, for existing customers) such business relationships
- take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and
- conduct enhanced ongoing monitoring on that relationship

**relevant requirements should apply to family members or close associates of all types of PEP.*

➤ **Reliance on Third Parties**

Reporting entities may rely on third parties to perform the CDD measures, provided certain criteria are met i.e. ultimate responsibility for CDD measures should remain with Reporting entity and it should:

- obtain immediately the necessary information concerning elements of CDD (identification of the customer; identification of the beneficial owner; and understanding the nature of the business)
- take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
- satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with standards set by the FATF
- When determining in which countries the third party that meets the conditions can be based, reporting entities shall have regard to information available on the level of country risk.

➤ **Higher Risk Countries**

Reporting entities should be required to:

1. apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.
2. countermeasures proportionate to the risks: (a) when called upon to do so by the FATF; and (b) independently of any call by the FATF to do so.

Suspicious Transactions Report (STR) & Record Keeping

➤ **Reporting of Suspicious Transactions**

Suspicious Transaction Report (STR)

STR should be filed if Reporting entity suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

Requirement to report all suspicious transactions, including attempted transactions, regardless of the amount of the Transaction.

Currency Transaction Report

The purpose of Currency Transaction Report (CTR) is to identify cash transactions (deposits and withdrawals) with the financial system, either directly or via designated non businesses and professions (DNFBPs), including by reporting firms. Similar to STRs, the aim is to provide additional information to the FMU to develop financial intelligence for law enforcement agencies to investigate potential ML, TF or other offences.

➤ **Record Keeping**

The Reporting entity shall promptly provide any records, documents or information upon request from respective authorities

Record Type	Retention period
Transaction records sufficient to enable the transactions to be fully reconstructed at any time	5 years from the completion of the transaction
Where transactions, customers or instruments are involved in litigation or where relevant records are required by a court of law or other competent authority,	Reporting entity shall retain such records until such time as the litigation is resolved or until the court of law or competent authority indicates that the records no longer need to be retained
Identity and verification evidence (as reasonably necessary to enable the nature of the evidence to be readily identified at any time)	5 years from the end of the business relationship or the completion of the occasional transaction or activity
Risk assessments, AML/CFT programs and audits	5 years after the date on which they cease to be used on a regular basis
Information relevant to the establishment of a business relationship and any other records that explain the nature and purpose of a business relationship and the activities relating to that business relationship	5 years from the end of the business relationship

Under the tipping off recommendation, reporting entity and its employees should be prohibited by law from disclosing the fact that an STR or related information is being filed with the Financial Intelligence Unit. Furthermore, reporting entity and its employees should be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU. This protection should be available even if

they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

New Technologies

Reporting entities shall take into consideration the risks of money laundering and terrorist financing that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Risk assessment shall take place prior to the launch of the new products, business practices or the use of new or developing technologies and take appropriate measures to manage and mitigate those risks



Internal Controls and Foreign Branches and Subsidiaries

Implementation of compliance programs against ML/TF risk including for targeted financial sanctions with regard to ML/TF risks and the size of the business, and which include the following internal policies, procedures and controls:

- compliance management arrangements including the appointment of a compliance officer at the management level. Compliance officer will be responsible for DNFBPs compliance with AML / CFT respective legislations, including but not limited to effectively implementing all of the elements of AML / CFT policies and procedures; CDD, record keeping, ongoing training, risk assessment and monitoring the effectiveness, reporting to senior management
- screening procedures to ensure high standards when hiring employees;
- an ongoing employee training programme; and
- an independent audit function to test the system.



Foreign Branches and Subsidiaries

The reporting entity shall ensure that its foreign branches apply AML & CFT measures consistent with home country laws where the minimum AML & CFT requirements are less strict than home country, to the extent of that host country laws. If the foreign country does not permit the proper implementation of AML/CFT measures consistent with that of the home country requirements, reporting entity should apply appropriate additional measures to manage the risks.

REGULATION AND SUPERVISION OF **DNFBPs**

Designated competent authority or Self-Regulatory Bodies responsible for monitoring and ensuring compliance of DNFBPs with AML/CFT requirements. The designated competent authority or self-regulatory body (SRB) should:

- have adequate powers to perform its functions, including powers to monitor compliance;
- take the necessary measures to prevent criminals or their associates from being professionally accredited, or holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function in a DNFBP; and
- have sanctions (proportionate and dissuasive sanctions) available to deal with failure to comply with AML / CFT requirements. The sanctions should not only apply to Reporting entity but also to directors and senior management.
- Countries should require casinos to be licensed
- Supervision of DNFBPs should be performed on a risk-sensitive basis, including:
 - (a) determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and
 - (b) taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

DISCLAIMER:

- 1) All reasonable care has been taken in the preparation of this Guideline document, but it necessarily contains information in summary form and is therefore intended for general guidance only. The publication does not amend or override, and it is not intended to be a substitute for reading the Laws, Regulations and guidance issued in SAFA Countries as well as by the United Nations.
- 2) A person should utilize his / her professional judgment and the facts and circumstances involved in each particular case. The information presented in this Guideline document should not be construed as legal, auditing, or any other professional advice or service. The preparer of this document do not accept any liability to any party for any loss, damage or costs howsoever arising, whether directly or indirectly, whether in contract, or otherwise from any action or decision taken (or not taken) as a result of any person relying on or otherwise using this document or arising from any omission from it.

SOURCES

- <https://www.fatf-gafi.org/>
- <https://www.dia.govt.nz/AML-CFT-Information-for-Accountants>
- <https://www.ccab.org.uk/anti-money-laundering-guidance-for-the-accountancy-sector/>
- <https://www.dia.govt.nz/AML-CFT-Legislation>
- <https://isca.org.sg/media/780574/ep-200-mar-2017.pdf>
- <https://www.acra.gov.sg/public-accountants/professional-resources/anti-money-laundering-and-counter-financing-of-terrorism-resources>
- <https://www.legislation.gov.uk>
- <https://www.icap.org.pk/>

GLOSSARY

TFS	Targeted Financial Sanctions
RE	Reporting Entities
FATF	Financial Action Task Force
STR / SAR	Suspicious Transactions Reports / Suspicious Activity Reports
FIU	Financial Intelligence Unit
AML	Anti – Money Laundering
CFT	Countering Financing of Terrorism
TF	Terrorist Financing
PF	Proliferation Financing
DNFBPs	Designated Non – Financial Businesses and Professions
SRB	Self – Regulatory Body
CDD	Customer Due Diligence
CTR	Currency Transaction Reports
PEP	Politically Exposed Persons
UN	United Nations