

IFSCA (AML, CTF, & KYC) Compliance Handbook



Copyright:**NIYEAHMA Consultants LLP**www.niyeahma.com

All rights reserved; no part of this publication may be reproduced or transmitted by any means, electronic, mechanical, photocopying or otherwise, without the prior permission of the Company.

Version: May, 2024

Designed by:**Technovisors**www.technovisors.com

Published by:**KMS Publications**

7th Floor, Devpath Complex, B/h. Lal Bungalow, Off. C.G. Road,
Ahmedabad - 380 006.

Tel: 079-2646 1526, 6631 5450 / 51 / 52 / 53

Disclaimer:

The book has been prepared for informational purposes only, and nothing contained in this book constitutes legal advice or any other form of advice from NIYEAHMA Consultants LLP. Although reasonable care has been taken to ensure that the information in this book is true and accurate, such information is provided 'as is' without any warranty, express or implied, as to the accuracy or completeness of any such information. NIYEAHMA Consultants LLP shall not be liable for any losses incurred by any person from any use of this book or its contents.

Preface:

It is with great pleasure that we present the IFSCA (AML, CTF, & KYC) Compliance Handbook. This handbook has been developed with many hours of research, relying on our diverse experiences and with a lot of care so that it can serve as a one-stop solution for understanding the IFSC AML compliance requirements. We are sure that this handbook will provide readers with an insight into the key aspects of IFSC AML, CTF, and KYC compliance.

The strategic location of GIFT City and its business-friendly legal and operations environment have made it a highly attractive global business hub. The IFSC authority has been instrumental in ensuring ease of doing business and providing and maintaining a robust business environment that proactively counters financial crimes and safeguards the interests of its constituents.

This handbook aims to help regulated entities fight the menace of money laundering, terrorist financing, and proliferation financing. We believe that the information and illustrations provided in the handbook will help principal officers and the compliance team comprehend the legal requirements quickly and easily.

We would like to acknowledge the team NIYEAHMA's efforts in providing valuable input, insights, and contributions to this handbook.

We hope you will find this handbook informative, insightful, and valuable.

CA Pathik Shah

CA Jyoti Maheshwari

CS Dipali Vora

Table of Content

Introduction	01
Regulatory Framework governing AML Compliance	04
At National Level	05
At IFSC Level	05
Allied Laws	06
IFSCA Compliance Roadmap: Step-by-Step Guide	08
1.0 AML Principal Officer Appointment	10
2.0 FINGate Registration	12
3.0 ML/FT Enterprise-Wide Risk Assessment	13
4.0 AML/CFT Policies and Procedures	17
5.0 Customer Due Diligence	21
5.1 Know Your Customer (KYC)	24
5.2 Customer Screening	26
5.3 Customer Risk Assessment	26
5.4 Enhanced Customer Due Diligence	28
5.5 Ongoing monitoring & Periodic CDD Review	30
5.6 Other Compliances	31
6.0 Targeted Financial Sanctions	33
7.0 Identifying and Reporting Suspicious Transactions	35

8.0 AML Governance	38
8.1 Training	38
8.2 Senior Management Involvement and Support	41
8.3 Audit	42
9.0 Record-Keeping	43
About NIYEAHMA	45
Our Services	48
ML/FT Enterprise-Wide Risk Assessment	49
AML Policy and Procedures Documentation	50
In-house AML Compliance Department Set-up	51
AML Software Selection	53
AML Health Check	54
AML Training	56
Author Profiles	58

Introduction

What is Money Laundering?

Money Laundering is a process carried out to route the illegally obtained funds through a series of transactions to disguise the source and owner of such illicit proceeds and make it appear as if generated from legitimate activities.

Money laundering is not the only financial crime hampering the global socio-economic environment. Various other crimes like terrorist financing and financing of proliferation of weapons of mass destruction are also a matter of global concern.

Criminals are inventing new techniques to launder funds, using technology to create complexities in transactions that are difficult to detect.

To curb the spread of these financial crimes, efforts are being made locally as well as internationally by various countries and inter-governmental organisations.

The **Financial Action Task Force (FATF)** is actively studying evolving financial crime trends, creating awareness about recent money laundering, terrorist financing, and proliferation financing techniques, and developing international standards to mitigate these risks.

As of May 2024, more than 200 countries, including India, have adopted the FATF's Recommendations on combating money laundering, terrorism financing and other financial crimes.

The IFSC authority has been instrumental in enhancing the ease of doing business and fostering a robust business environment that proactively combats financial crimes and safeguards the interests of its constituents.

Regulatory Framework governing AML Compliance

At National Level

To begin with, the Indian Government introduced the **Prevention of Money Laundering Act, 2002**, and corresponding regulations in a dedicated effort to prevent money laundering.

PMLA aims to prevent money laundering and provides for stringent penal consequences, including confiscation of property, when the transaction or the person is identified as associated with or involved in money laundering.

PMLA and the **Prevention of Money Laundering (Maintenance of Records) Rules, 2005**, lay down stringent regulations for the identified regulated entities, directing them to implement measures like thorough customer identification, reporting any suspicious transactions, maintaining AML records, etc.

At IFSC Level

Following the PMLA and the overall FATF Recommendations, the IFSCA issued the IFSCA (Anti Money Laundering, Counter-Terrorist Financing and Know Your Customer) Guidelines, 2022.

These IFSCA (AML, CTF, & KYC) Guidelines elaborate on the methods the IFSCA-regulated entities must adopt to identify the risk associated with money laundering and terrorism financing and deploy adequate risk mitigation measures, such as Customer Due Diligence and training the team.

Allied Laws

The following are the 2 critical enactments that complement the PMLA and IFSCA (AML, CTF, & KYC) Guidelines in combating overall financial crime:

A. The Unlawful Activities (Prevention) Act, 1967

This act spells out the requirements related to Targeted Financial Sanctions compliance, focusing on combating terrorism and terrorist financing activities.

B. Weapons of Mass Destruction and Their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

This law lays down the directives to fight the financing of the proliferation of weapons of mass destruction.

The IFSCA (AML, CTF, & KYC) Guidelines along with the provisions of the PMLA and the allied laws, apply to all companies licensed to operate in or from IFSC and are subject to supervision by the IFSCA. Thus, every IFSC entity has to comply with the AML regulations, irrespective of the nature and size of the business activities—whether a financial institution or a non-financial business or profession.

Non-compliance with IFSCA (AML, CTF, & KYC) Guidelines by an IFSC entity can result in adverse consequences such as heavy administrative fines, cancellation, or suspension of business license, along with reputational damages and loss of customers' trust and confidence.

IFSCA (AML, CTF, & KYC) Compliance Roadmap: Step-by-Step Guide

9-Step process to mitigate ML/FT risks

-  ▶ 1.0 AML Principal Officer Appointment
-  ▶ 2.0 FINGate Registration
-  ▶ 3.0 ML/FT Enterprise-Wide Risk Assessment
-  ▶ 4.0 AML/CFT Policies and Procedures
-  ▶ 5.0 Customer Due Diligence
 - 5.1 KYC
 - 5.2 Sanctions Screening
 - 5.3 Customer Risk Assessment
 - 5.4 Enhanced Customer Due Diligence
 - 5.5 Ongoing Monitoring
 - 5.6 Other Compliances
-  ▶ 6.0 Targeted Financial Sanctions
-  ▶ 7.0 Identifying and Reporting Suspicious Transactions
-  ▶ 8.0 AML Governance
 - 8.1 Training
 - 8.2 Senior Management Involvement & Support
 - 8.3 Audit
-  ▶ 9.0 Record-Keeping

1.0 AML Principal Officer Appointment

IFSCA (AML, CTF, & KYC) Guidelines mandate that regulated entities designate an AML Principal Officer (also known as a Compliance Officer) to handle the entity's AML measures, ensure regulatory compliance, and protect the business against financial crime risks.

The person designated as the AML Principal Officer must be a management-level employee of the entity, having adequate seniority to make AML-related decisions.

AML Principal Officer serves as a cornerstone to the regulated entity's AML functions, designing the overall compliance and risk mitigation framework and overseeing its effective implementation.

The role of an AML Principal Officer is crucial in ensuring compliance with the IFSCA (AML, CTF, & KYC) Guidelines.



Appointment of a Principal Officer

- A management-level employee
- Hold adequate seniority and authority
- Must have:
 - Suitable qualification and competence
 - Adequate resources
 - Access to relevant data, including customers and transactions
- Avoid conflict of interest
- Independent of routine business functions



Key Roles and Responsibilities

- Overseeing and promoting AML Compliance across the organization
- Ensuring performance of ongoing monitoring of business relations
- Updating the team and senior management on the AML-related regulatory amendments
- Promptly addressing the ML/FT suspicions
- Reporting the suspicious transactions to FIU-IND
- Training the employees around AML/CFT measures
- Periodically reviewing the entity's compliance with AML/CFT regulations
- Timely reporting of AML/CFT compliance issues, ML/FT risks, and remedial measures to senior management

2.0 FINGate Registration

All regulated entities licensed with IFSCA are mandatorily required to register with the Financial Intelligence Unit of India (FIU-IND) by completing the enrolment on the **FINGate 2.0 Portal**.

The registration process involves furnishing the details about the business, the Principal Officer, and the regulated entity's Designated Director, who shall take care of the AML program within the organisation.

Non-registration with FIU-IND is treated as non-compliance with the IFSCA (AML, CTF, & KYC) Guidelines.

FINGate 2.0 is the primary platform through which data associated with money laundering or other crimes is furnished to FIU-IND.

FINGate 2.0 is FINNET 2.0's front-end web portal used by regulated entities to report suspicious financial transactions.

3.0 ML/FT Enterprise-Wide Risk Assessment

The degree or the nature of the money laundering or terrorism financing exposure of each regulated entity varies. And so does the extent of risk mitigation measures.

Thus, the IFSCA (AML, CTF, & KYC) Guidelines provide for adopting a **Risk-Based Approach** to manage risk and optimise resource utilisation. Under a risk-based approach, a regulated entity's primary task is to identify and understand the source or factors emitting the risks and tailor the controls and overall AML program commensurate with the ML/FT risk assessed.

Here comes the need to conduct the **Enterprise-Wide Risk Assessment (EWRA)** to evaluate and assess the money laundering and financing of terrorism risks associated with the entity's operations, business model, etc.

The Risk Factors

The risk may arise from various factors contributing to the business. Thus, the regulated must assess the potential ML/FT risks posed by various risk parameters such as:

- The nature and overall profile of the **customer** the regulated entity engages with
- The **jurisdictions** of the regulated entity's customers
- The nature of the **products and services** offered by the regulated entity
- Size and the complexity of the financial **transactions**
- Delivery or the **distribution channels** deployed, etc.
- Risks posed by the development of **new product, practices, and technologies**

ML/FT Enterprise-Wide Risk Assessment



Identification of the Risk

Identify the ML/FT risk the business is exposed to considering the following risk parameters–

- Type of customer & their business activities
- Geographies of business engagement
- Products and Services offered
- Delivery channels involved
- Transactions – volume and complexity
- Development of new product, practices and technologies



Analysis of Risk

Determining the probability of occurrence of risk and its resulting impact on the business



AML/CFT Policies & Control

Adopting Risk-Based Approach, determine the controls required to manage and mitigate the identified ML/FT risks. Define and implement the policies, procedures, and systems

The Analysis and Way Forward

Once the relevant risk factors have been identified, the regulated entity must evaluate the possibility of such risk occurring and its impact on the business.

This analysis will help the regulated entity determine the level and nature of risk mitigation measures (controls and systems) required to handle these risks.

Thus, after assessing the risk and the required measures, the regulated entity must outline a larger ML/FT risk management and compliance framework.

The Enterprise-Wide Risk Assessment helps regulated entities uncover the ML/FT risks and adopt a customised risk management framework, targeting the threats with effective use of available resources.

As the entire AML program is developed on the foundation of the EWRA, it is important to ensure its relevance, accuracy, and comprehensiveness. Thus, the regulated entity must review and update the EWRA at least once every two (2) years or upon a significant change in risk parameters or business operations, whichever is earlier.

4.0 AML/CFT Policies and Procedures

IFSC-regulated entities are required to craft business-specific AML/CFT policies and procedures to mitigate financial crime risks and comply with IFSCA (AML, CTF, & KYC) Guidelines.

This AML/CFT program must be comprehensive and include the relevant policies, procedures, controls, and systems for timely detection, prevention, and reporting of money laundering or terrorism financing risks.

The AML/CFT program must be in proportion to the nature and size of the business and the applicable regulatory obligations. AML/CFT policies and procedures must be developed considering the outcome of the EWRA and the provisions of the relevant laws, specifically the updated IFSCA (AML, CTF, & KYC) Guidelines.

Elements of the AML/CFT Policies and Procedures

Commitment to a risk-based approach and risk assessment mechanism

Customer onboarding process, highlighting the Customer Due Diligence Process

Implementation of the Targeted Financial Sanctions regime and other international directives

Process on identification and reporting of the ML/FT suspicious transactions

AML compliance governance framework

AML process

Features of Effective AML Policies and Procedures



Easy to understand



Practical to implement in the course of business operations



Empower the risk management efforts



Enable AML regulatory compliance

The regulated entity's AML/CFT program must be reviewed and approved by the senior management. These internal policies must be well-communicated within the organization, encouraging employee engagement and contribution towards ML/FT combat mission.

The Principal Officer must periodically review and upgrade these defined AML/CFT policies, procedures, and controls to keep them real, relevant, valid and effective.

Top 10 Deficiencies around AML Policies and Procedures

- 01 Not covering all the Essential Elements
- 02 Unsatisfactory Documentation of a Risk-Based Approach
- 03 Inadequate EDD Procedures
- 04 Ineffective Ongoing Monitoring Procedures
- 05 Missing Authorization
- 06 Inadequate Change Management
- 07 Not Updated with the Latest Regulatory Requirements
- 08 Inadequate Communication about AML policies and procedures
- 09 Missing out on procedures on Countering the Proliferation Financing
- 10 Improper Record-Keeping Measures

5.0 Customer Due Diligence

One of the risk mitigation measures at the core of the AML/CFT program is the **Customer Due Diligence (CDD)** process.

The CDD program empowers regulated entities to restrict the entry of financial criminals into their businesses by making efforts to identify potential customers attempting to launder funds or conduct transactions that may involve illegal proceeds or purposes.

The CDD is a process involving multiple components that assist in identifying the customer, assessing the potential risk the customer may pose to the business and deploying the appropriate measures to manage this risk.

Customer Due Diligence



WHAT is Customer Due Diligence?

- Identifying the customer and the beneficial owners
- Verifying the identity using reliable sources
- Understanding the nature and purpose of the business relationship
- Ongoing monitoring of business relationships and transactions

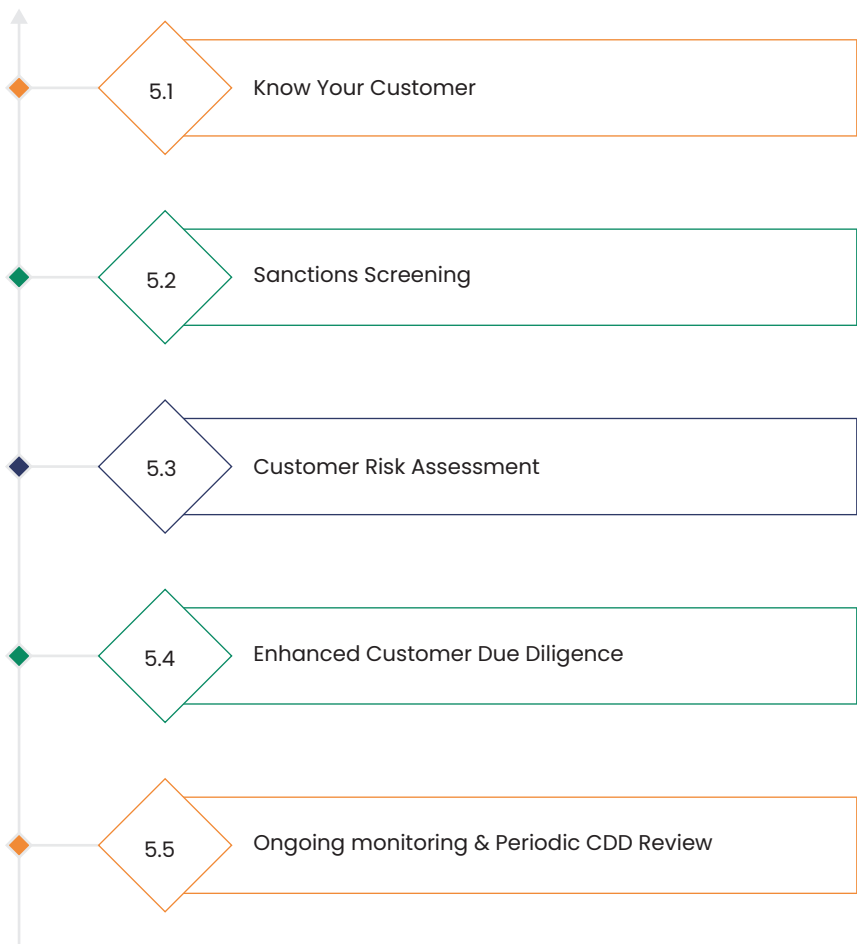


WHEN is Customer Due Diligence required?

- At the time of establishing a business relationship
- Doubt about the accuracy or adequacy of the details/ documents of existing customer
- When ML/FT suspicion is observed in a business relationship
- Change in customer's risk profile

The CDD process must be carried out before establishing the business relationship to determine the identity of the prospective customer. However, in certain exceptional circumstances, regulated entities are permitted to delay the identity verification process.

The Key Elements of an Effective CDD Process



5.1 Know Your Customer (KYC)

Know Your Customer, or KYC, is a process aimed at identifying the customer with whom the regulated entity is already engaged or proposes to engage.

The KYC process primarily revolves around seeking the identification details of natural and legal customers. Once the customer details are collated, the regulated entity must verify the authenticity of all such customer information using reliance and independent sources.

5.1.1 Natural Person

KYC details for an individual customer would include full name, unique identification number, date of birth, nationality, address, and contact details.

To verify the customer's identity and address, the regulated entity must obtain an identity document that contains a photograph of the customer, name, unique identification number, date of birth, and nationality.

For residential address verification, the regulated entity can refer to the "Officially Valid Documents" obtained for identity verifications or other documents like recent utility bills, bank statements, etc.

5.1.2 Legal Person

KYC information for a legal person would cover full legal name, trading name, unique identification number, registered or business address, principal place of business, date and place of incorporation.

Additionally, it is important to understand the customer's legal form, constitution, ownership, and controlling structure.

A regulated entity must obtain a certificate of incorporation, partnership deed/agreement, trust deed, constitutional document, certificate of registration, or any other document to verify its legal form and structure.

5.1.3 Representative and Beneficial Owners

A regulated entity must take the necessary steps to identify and verify the natural person appointed by the customer to act on their behalf.

In case when the customer is a legal person or a legal arrangement, the regulated entities are also required to understand the customer's control or ownership structure and identify the beneficial owner of the customer.

5.2 Customer Screening

Customer screening is a critical aspect of the CDD program (along with being crucial to the implementation of the Targeted Financial Sanctions program) that assists the regulated entities in identifying whether any customers are sanctioned or designated under the UNSC Lists or the local list of banned persons.

Along with **sanctions checks**, the screening process will also help uncover if the customer has some connection with criminal activities, including financial crime, or is a **Politically Exposed Person**, where the potential vulnerabilities increase.

This screening strengthens the regulated entity's efforts to identify the customer and determine the degree of exposure that such a customer may emit to the business.

5.3 Customer Risk Assessment

As part of the CDD process, the regulated entities must assess the level of money laundering and terrorist financing risk the customer poses to the business and develop the **customer risk profile**.

This risk assessment would assist the regulated entity in classifying the customer as high, medium or low, taking into account various risk parameters.

Risk Assessment Parameters



Ownership & management structure



Nature & purpose of business relationship



Location of customer



Nature of customer's activities



Estimated size or value of the transaction



Timing & seasonality of transactions



Involvement of counterparties & intermediaries



Customer's financial profile

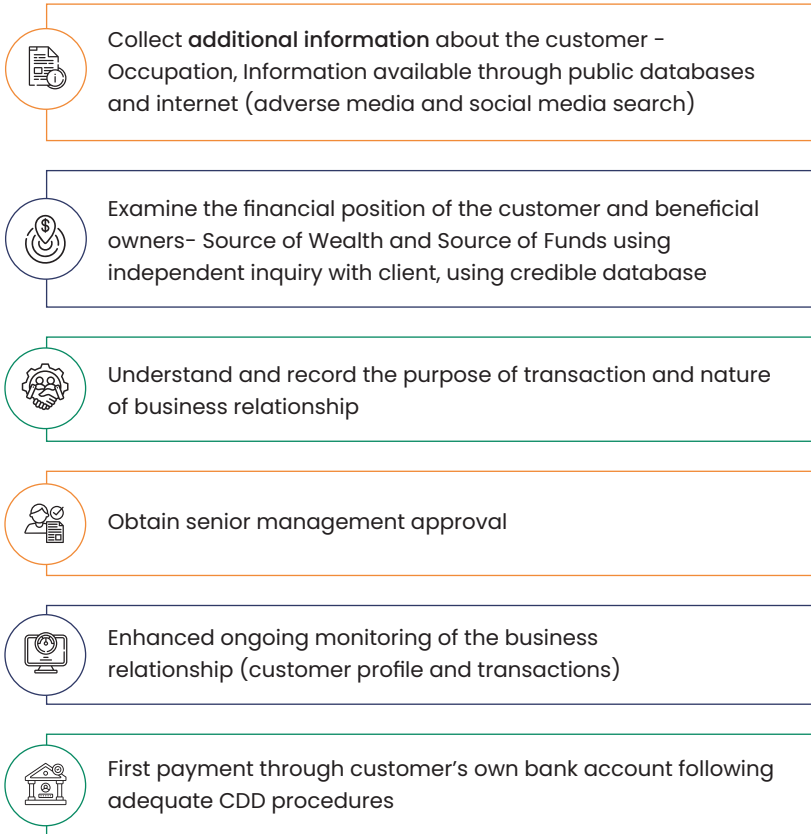
This customer risk profiling would enable the regulated entity to determine the level of due diligence measures to be applied to each customer, adopting the risk-based approach.

For example, simplified due diligence may be followed when the customer is identified as low risk or enhanced customer due diligence measures may be used to mitigate the increased ML/FT risk.

5.4 Enhanced Customer Due Diligence

The regulated entities must apply Enhanced Customer Due Diligence measures when dealing with high-risk customers.

Enhanced Customer Due Diligence Process: Additional Checks and Verification Measures



5.5 Ongoing Monitoring & Periodic CDD Review

Ongoing monitoring of business relationships is very crucial to detect unusual or suspicious activities. This includes scrutinising the transactions and maintaining the customer profile up-to-date.

An ongoing and comprehensive review of the business relationship will help the regulated entity evaluate the transaction pattern in a timely manner and determine if there are any anomalies or if such transactions align with the customer's risk profile.

Further, the IFSCA (AML, CTF, & KYC) Guidelines mandate that regulated entities review all their customers against the UNSC sanctions lists and other relevant sanctions lists, including the local list of banned individuals and organisations.

The frequency of ongoing monitoring of transactions and business relationships depends upon the customer's ML/FT risk profile, i.e., the higher the risk, the more stringent the monitoring norms.

Frequency for Periodic Review and Updating CDD Files



5.6 Other Compliances

5.6.1 Specific Due Diligence Measures

The IFSC entities are required to adopt additional risk mitigation measures to handle the increased risk involved in correspondent banking relationships and wire transfer transactions.

In the context of **correspondent banking**, the relevant regulated entities must deploy measures to adequately identify the correspondent bank, assess the risk associated with such a relationship, and evaluate the correspondent bank's AML compliance status. Further, the regulated entity must also obtain management approval prior to establishing such a relationship.

With respect to **wire transfers** handled by the regulated entities, the regulated entities must identify the transferor and the receipt involved in the wire transfer and exchange such information along with the transfer request to the intermediary or the recipient financial institution.

5.6.2 Central KYC Registry

The regulated entities are required to capture the customer's KYC records and upload the same on the Central KYC Registry (CKYCR), in case of an account-based relationship with an Indian national.

5.6.3 Reliance on Third Parties

The IFSCA permits the regulated entities to rely on third parties for Customer Due Diligence measures.

Here, the reliance on third parties for CDD suggests that a regulated entity relies upon and refers to the CDD information of a person with whom the third party already has an existing client relationship, and such third party has performed adequate CDD processes, including customer identification and identity verification.

6.0 Targeted Financial Sanctions

The IFSC entities are required to comply with the international directives from the United Nations Security Council and Section 51A of the Unlawful Activities (Prevention) Act, 1967, regarding international targeted financial sanctions.

As part of the Targeted Financial Sanctions (TFS) program, the regulated entities are required to screen each customer, beneficial owner, and other business partner to determine if any of these individuals or legal persons have been designated by the UNSC or the Ministry of Home Affairs and, if so, refrain from engaging with such designated person subject to targeted financial sanctions.

As part of TFS, the regulated entities must conduct screening against:

- ISIL (Da'esh) & Al-Qaida Sanctions List
- 1988 Sanctions List
- Local list of banned entities and individuals issued by the Ministry of Home Affairs

If any person is identified as sanctioned, the regulated entity must apply the freezing measures (freezing the assets or funds of such designated person) and immediately, not later than 24 hours, report the person to the Nodal Officer.

The regulated entities have a similar freezing and reporting obligation under Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005.

Here, the IFSC entities are prohibited from engaging with the countries, organisations or persons sanctioned by the UNSC or the local authorities in the context of being associated with the financing of the proliferation of weapons of mass destruction.

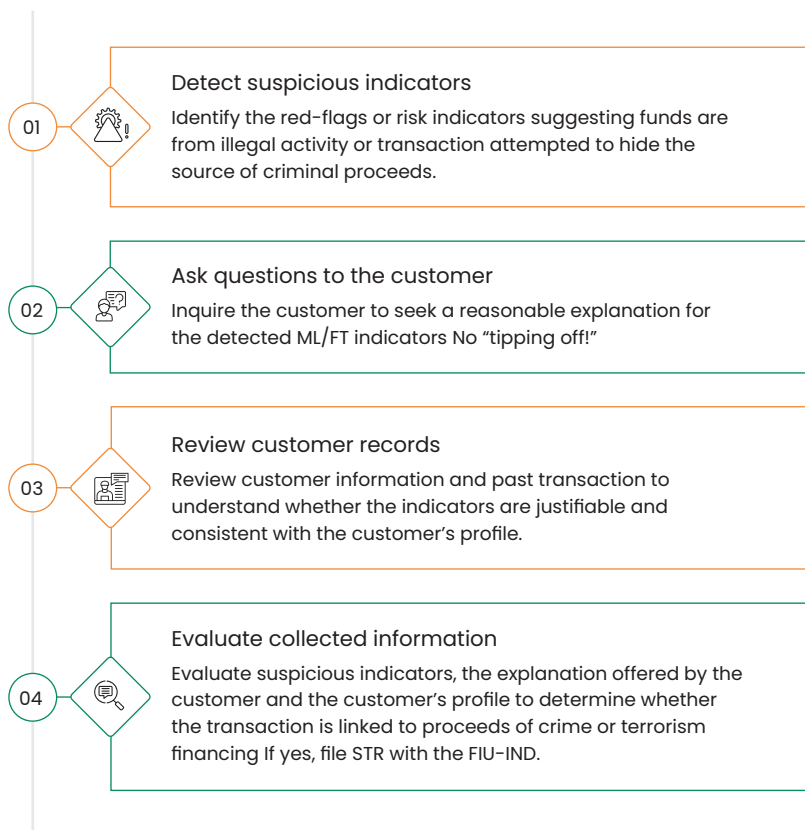
Similar to TFS, the regulated entity must freeze the resources of such a sanctioned person and intimate the relevant details to the Nodal Officer within 24 hours.

7.0 Identifying and Reporting Suspicious Transactions

The entire AML/CFT program revolves around the timely identification and reporting of transactions suspected of being associated with money laundering, terrorism financing or involving the proceeds of crime.

The regulated entities are obligated to define the necessary internal procedures and systems to foster the detection and reporting of suspicious transactions. This includes developing a sector-specific list of the risk indicators or ML/FT red flags that the team must understand and be cautious of to spot the attempted ML/FT activities in a timely manner.

4-Step Process for Identification and Reporting of Suspicious Transactions



Once the risk indicator is identified and the regulated entity has reasonable grounds to suspect the involvement of the ML/FT, the same must be reported to the FIU-IND by submitting a Suspicious Transaction Report (STR) without any delay.

During this entire process of identifying and reporting the suspicion, the regulated entity and team must ensure there is no “tipping off” to the customer or third party.

8.0 AML Governance

For effective and successful implementation of the AML program and ensuring compliance with the IFSCA (AML, CTF, & KYC) Guidelines, the regulated entities must develop a robust AML compliance governance structure.

The key components of a good AML governance framework are:

8.1 Training

To effectively implement the AML program across the organisation, the support of the entire workforce is crucial.

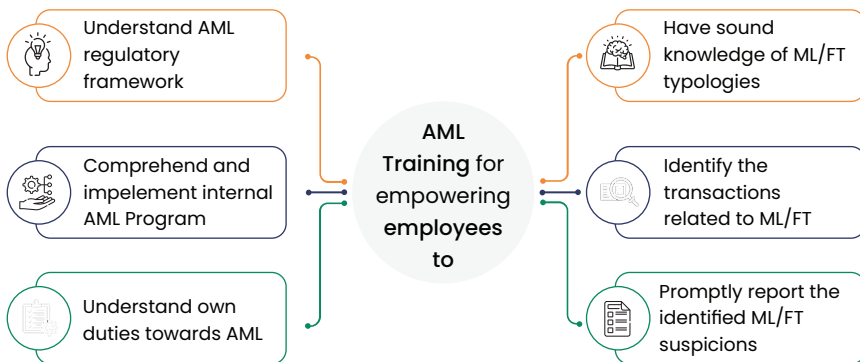
Here, a regular and well-designed AML training program will be helpful in creating awareness and equipping the team with the necessary AML knowledge and skills to identify the risk indicators and handle money laundering and terrorism financial risks.

An effective AML training program must include job-specific sessions, along with general AML conceptual discussions.

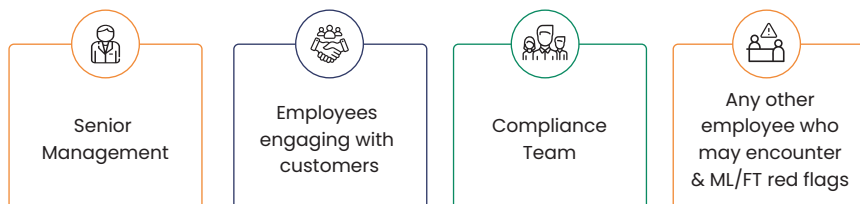
Fundamental Aspects to be included in the AML Training Agenda

- 01 ML/FT typologies and potential vulnerabilities
- 02 IFSCA (AML, CTF, & KYC) Guidelines and the compliance obligations imposed thereunder
- 03 Risk factors and methodology for conducting Enterprise-Wide Risk Assessment
- 04 Customer Due Diligence (including KYC, customer risk assessment, Enhanced Customer Due Diligence)
- 05 Understanding the red flags
- 06 Recognizing and reporting the Suspicious Transactions
- 07 AML documentation requirements
- 08 Implementation of the sanctions program and the screening systems
- 09 Roles and responsibilities of employees and the consequences of non-compliance

Significance of AML Training



***Relevant Employees (including new joiners):**








8.2 Senior Management Involvement and Support

Senior management is responsible for setting the right tone at the top for effective AML/CFT compliance and governance culture.

Further, the senior management of the regulated entities plays a vital role in reviewing and approving the AML/CFT program, ensuring that the necessary controls are in place to mitigate the risks.

Additional AML Functions entrusted upon the Senior Management

-  Ensuring compliance and efficacy of AML/CFT Policy
-  Appointment of AML Principal Officer
-  Approval to onboard high-risk customer
-  Ensuring compliance with the IFSCA (AML, CTF, & KYC) Guidelines
-  Timely & effective action against non-compliance

8.3 Audit

The IFSC entities must have an AML audit function to periodically test the effectiveness and quality of the AML/CFT program and identify the gaps that need improvement.

The AML audit function must be independent and be adequately staffed to carry out the audit diligently.

Activities to perform during AML Audit



Check adequacy of Internal AML/CFT Framework



Evaluate quality and timeliness of reporting (internal and external)



Check compliance with internal AML Program



Evaluate the application of the Risk-Based Approach



EWRA: Adequacy of risk assessed & methodology adopted



Evaluate adequacy of the AML Training

With this regular review, the entities can ensure that their AML efforts stay relevant and efficient in managing the ML/FT risk.

9.0 Record-Keeping

The essentials of Record-Keeping

Time Period

For a minimum period of six (6) years from:

- End of the business relationship, or
- Completion of the transaction

Records To Be Maintained

- Documents and information on Customer Due Diligence, including Customer Risk Assessment and ongoing monitoring
- Records pertaining to ML/FT Business Risk Assessment
- Records about transactions
- Observations related to unusual or suspicious activities and internal intimations filed with the Principal Officer
- STRs filed with FIU-IND
- AML training logs

Proper Maintenance Of Adequate AML Records

The AML records maintained by the regulated entity must allow the following:

- Easy retrieval of the records when requested by the authorities
- Assessment of the level of the entity's regulatory compliance by IFSCA
- Reconstruction of the already executed transaction
- Identification of a customer

The regulated entities are permitted to retain the AML records in an electronic form or can even be kept outside IFSC. Here, the only condition is that such records must be easily accessible and maintained in a manner that adheres to the IFSCA (AML, CTF, & KYC) Guidelines.

About NIYEAHMA

Inspired by the Sanskrit term

“ नियमा ”

**which means rules, laws, and order,
we call our professional organisation – NIYEAHMA
as we say “yeah”/YES to these rules and regulations and help
you comply with them.**

NIYEAHMA is a global AML consulting firm in India assisting reporting entities to comply with the requirements of the Prevention of Money Laundering Act, 2002 and the International Financial Service Centre Authority (AML, CTF, and KYC) Guidelines, 2022.

We are continuously striving to improve businesses' compliance in India, helping them implement relevant controls, improve KYC and customer onboarding processes, and assist in setting up a solid in-house AML compliance department to reduce money laundering risks.

With our years of global experience in AML/CFT compliance and understanding of regulated businesses, we offer tailored consultancy services.

We conduct Enterprise-Wide Risk Assessments to identify the entity's exposure to financial crime risk and determine the necessary controls and systems to mitigate these risks. Based on this assessment, we design a comprehensive, tailor-made AML compliance program where business safety against vulnerabilities seamlessly meets AML compliance.

We understand your AML compliance requirements and design a business-specific AML training program.

With our end-to-end AML support, master your AML compliance and timely manage the money laundering risks.

Our Services

ML/FT Enterprise-Wide Risk Assessment

NIYEAHMA helps companies carry out their business risk assessment and control AML risks. It helps organisations identify inherent and residual risks related to products, services, customers, delivery channels, and geographies.

Businesses can assess their ML/FT risk exposure and apply suitable policies and controls to mitigate such risks and keep them within the limits of their risk appetite.

Our Approach to Business Risk Assessment

01 Understanding the Business

02 Identifying the Risk Scenarios

03 Risk Classification and Impact Analysis

04 Defining Controls and Monitoring

An Enterprise-Wide Risk Assessment performed on the basis of reliable qualitative and quantitative data ensures that the regulated entities' ML/FT risks are within their risk appetite.

AML Policy and Procedures Documentation

We create for you the right policies, rules, and procedures revolving around the AML/CFT regulatory framework and your business exposure.

We have a deep understanding of all the laws, regulations, rules, guidelines, and notifications related to AML/CFT and understand its implications; we use this knowledge and experience to develop the apt AML/CFT policies and procedures for your business operations.

We also frame guidelines and manuals for KYC, CDD, and EDD to make your operations efficient and smooth. Our AML policy, controls, and procedures documentation service is comprehensive enough to cover each aspect of AML/CFT regulation.

We use internationally accepted best practices of AML compliance to create your AML/CFT program that can reduce your business's exposure to illicit money.

In-house AML Compliance Department Set-up

We at NIYEAHMA have the expertise to develop an AML/CFT compliance department for your organisation.

Our Process:



We can help you set up an in-house AML compliance department to handle everything related to your organisation's AML/CFT programs and policies.

With such a compliance department in place in the organisation, you will be better positioned to identify the risks to your business, develop policies to mitigate them and achieve compliance with AML/CFT requirements.

AML Software Selection

AML software enables organisations to comply with the legal requirements created to fight financial crime in the world. The adoption of the right AML software is a part of the AML strategy and AML compliance program to identify suspicious transactions, clients, and business partners.

NIYEAHMA has a good network of AML software and solution providers that excel in their offerings and provide feature-rich, scalable, and cost-effective solutions that align with the general AML/CFT and KYC compliance needs.

Our team of business analysts, technology enthusiasts, and AML experts understands the basic needs of AML software—KYC, screening, transaction monitoring, and overall compliance with AML regulations — and, therefore, suggests solutions to shift you from non-compliance to compliance .

AML Health Check

Protect your business against money laundering and terrorist financing risks with a proactive approach.

The AML/CFT Health check will help you understand where your entity stands in terms of applicable AML/CFT guidelines. This quick and easy solution will help your business determine which areas require immediate attention and improvements.

We will provide you with our AML Health check report, which includes:

01

Review of the existing AML program

02

High-level observation of the company's AML framework

03

Identifying areas for process improvements, if any

04

Recommending the remediation plan to smoothen the AML process

05

Observations on the overall AML compliance level of the company

We will provide you with our AML Health check report, which includes:

01

Review of the existing AML program

02

High-level observation of the company's AML framework

03

Identifying areas for process improvements, if any

04

Recommending the remediation plan to smoothen the AML process

05

Observations on the overall AML compliance level of the company

AML Training

NIYEAHMA is an expert provider of AML compliance consulting services, including relevant AML/CFT training for employees, including the compliance team and senior management.

We provide customised training based on the industry of your business operations. Our tailor-made AML training program for your employees makes your organisation capable enough to handle AML compliance requirements so that you become safe from any possibility of money laundering and terrorism financing activities.

Our AML Training program:

01 Understanding the concept – AML, CFT and CPF

02 FINGate Portal and registration thereon

03 Relevant regulations (IFSCA (AML, CTF, & KYC) Guidelines, including PMLA)

04 Enterprise-Wide Risk Assessment

05 AML Compliance Program (Policies and Procedures)

06 KYC & CDD/EDD, decoding beneficial ownership

07 STR and other AML Reporting Requirements

08 Sanctions compliance

09 Principal Officer Roles & Responsibilities

10 Effects of AML International Bodies – FATF

11 Record Keeping

12 Sectoral Red Flags

About Authors

Pathik is a Chartered Accountant with more than 25 years of experience in compliance management, Anti-Money Laundering, risk management, system audits, technology consulting, and digital marketing.

He has extensive knowledge of local and international AML rules and regulations. He helps companies with end-to-end AML compliance services, from understanding the AML business-specific risk to implementing the robust AML Compliance framework.

Pathik leads the firm from the front and is responsible for giving it strategic direction.



Pathik Shah

Founder

FCA, CAMS, CISA, CS,
DISA (ICAI), FAFP (ICAI)



Jyoti Maheshwari

Partner

ACA, CAMS

Jyoti is a Chartered Accountant and Certified Anti-Money Laundering Specialist (CAMS), having around 7 years of hands-on experience in regulatory compliance, legal advisory, policy-making, tax consultation, and technology project implementation.

Jyoti holds experience with AML regulations prevalent across various countries. She helps companies with risk assessment, designing and deploying adequate mitigation measures, and implementing the best international practices to combat money laundering and other financial crimes.

Dipali is an Associate member of ICSI and has a Bachelor's in Commerce and a General Law degree. She has 7 years of overall experience in the compliance domain, including Anti-Money Laundering, due diligence, secretarial audit, and managing scrutiniser functions.

She currently assists clients by advising and helping them navigate the legal and regulatory challenges of AML laws. She also helps companies develop, implement, and maintain effective AML/CFT and sanctions programs.

She specialises in Enterprise-Wide Risk Assessment, Customer Due Diligence, and Customer Risk Assessment.



Dipali Vora

Partner

ACS



aml india

 info@amlindia.in

 www.amlindia.in



N NIYEAHMA

 info@niyeahma.com

 www.niyeahma.com

Follow us on

