مـــصـــرف الـتـنـمـيـة الـــدولـــي
International Development Bank

Anti Money Laundering / Counter Financing of Terrorism Policy

Version 1.0

IDB-Dubai, Compliance Department

December 2023

International Development Bank for Investment and Finance (Regulated by the Central Bank of the UAE as a wholesale bank)
Al Shafar Investment Building, Sheikh Zayed Road, P.O. Box: 338233 Dubai - United Arab Emirates. Tel: +971 4 3057200

Document Control

Date Of Issue	Version No.	Revision Description (reason of Change)

Document Initiated By:

Date	Created by	Position	Signature
18/12/2023	Malek Hajeer	Head of Compliance	

Document Approval:

Date	Approved by	Signature
08/01/2024	Hani Idris – CEO/Regional Manager	

Table of Contents:

1. Purpose

International Development Bank, UAE (IDB) is unwavering in its commitment to upholding the highest ethical standards and adhering to all applicable laws and regulations pertaining to anti-money laundering (AML), combating the financing of terrorism (CFT), and preventing the proliferation of weapons of mass destruction (PF). IDB recognizes the significance of safeguarding its reputation and protecting the integrity of its operations. As such, IDB's management takes full responsibility towards its shareholders to ensure that the Bank implements robust risk mitigation strategies and maintains a robust framework of policies, procedures, internal control systems, and ongoing monitoring mechanisms to effectively manage and mitigate the risks associated with ML, TF, and PF.

This policy serves as a cornerstone document that outlines IDB's comprehensive approach to addressing ML, TF, and PF risks that aligns with IDB's unwavering commitment to financial integrity and regulatory compliance.

2. Scope

The Anti-Money Laundering/Counter Financing of Terrorism Policy (AML/CFT Policy) is applicable to IDB UAE only and outlines the minimum standards for complying with relevant anti-money laundering and combating the financing of terrorism regulations. These standards are designed to prevent the bank from being used for illicit activities and to protect its reputation and financial stability.

In cases where the Group policy establishes higher standards or additional requirements than those outlined in this policy, the higher standards shall prevail, to the extent permitted by the laws and regulations of the applicable jurisdiction. If any conflict arises between the Group policy and this policy, the respective compliance officer should seek further guidance from the Compliance Head to ensure adherence to the most stringent standards.

IDB is committed to implementing effective AML/CFT controls to safeguard its integrity and contribute to the global fight against financial crime.

3. Policy Objectives

This Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy establishes the overarching principles and framework for adhering to all applicable AML/CFT laws and regulations in the United Arab Emirates (UAE). By implementing this policy, IDB aims to achieve the following key objectives:

- Establish Risk-Based Controls: Implement a comprehensive risk-based approach to AML/CFT compliance that effectively identifies, assesses, and mitigates the risks associated with money laundering, terrorist financing, and other financial crimes.
- Minimize Compliance, Regulatory, and Reputational Risks: Proactively prevent and deter the use of IDB's services for illicit activities, thereby safeguarding the bank's reputation, ensuring regulatory compliance, and minimizing the potential for legal and financial penalties.
- Serve as a Central AML/CFT and KYC Reference: Provide a comprehensive and readily accessible resource for all IDB employees in the UAE, outlining the bank's AML/CFT obligations, Know Your Customer (KYC) procedures, and expectations for reporting suspicious transactions and activities.
- Foster a Culture of AML/CFT Awareness: Cultivate a workplace culture that emphasizes AML/CFT awareness, education, and training, ensuring that all employees understand their responsibilities in preventing financial crimes and upholding IDB's commitment to ethical and compliant practices.
- Promote Continuous Risk Management: Continuously evaluate and refine AML/CFT risk assessments and controls to adapt to evolving regulatory requirements, emerging threats, and changes in the bank's business operations.

4. Non-Compliance

All bank employees must comply with this policy without exception.

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment in accordance with IDB's HR policies.

In addition to disciplinary action, bank employees who fail to comply with this policy may also be held personally liable for any losses or damages that result from their non-compliance.

5. Monitoring, Evaluation and Review and Policy Revision and Maintenance

Monitoring, Evaluation, and Review

IDB's Compliance Department is responsible for overseeing the implementation of this AML/CFT policy and will conduct periodic reviews to ensure its effectiveness. The policy will be reviewed at least annually, or more frequently as needed, to address any changes in applicable laws, regulatory requirements, or emerging risks.

Evaluation

The evaluation of the policy will involve assessing its effectiveness in preventing and detecting money laundering and terrorist financing. This will include reviewing transaction monitoring reports, suspicious activity reports, and customer due diligence records. The evaluation will also consider the results of internal and external audits, as well as any feedback received from employees or regulators.

Review

Based on the evaluation, the Compliance Department will propose any necessary revisions to the policy. These revisions will be reviewed and approved by the Bank's Board/Committee before being implemented.

Policy Revision and Maintenance

The AML/CFT policy will be subject to ongoing revision and maintenance to ensure that it remains effective in addressing the evolving risks of money laundering and terrorist financing. In addition to the periodic reviews, the policy may be updated in response to:

- Changes in applicable laws, regulatory requirements, or guidance from governmental, legal, and regulatory authorities
- Changes in IDB's business strategy or risk appetite
- The identification of new or emerging risks
- Any other changes that are deemed necessary by the Bank's Board/Committee

All changes to the policy will be approved by the Head of Compliance and the Bank's Board/Committee prior to implementation.

This approach to monitoring, evaluation, and review will ensure that IDB's AML/CFT policy remains a robust and effective tool for preventing and detecting money laundering and terrorist financing.

6. Definitions and Abbreviations

Abbreviation	Description
AML	Anti-Money Laundering
CASA	Current Account and Savings Account
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer Due Diligence
CDM	Cash Deposit Machine
CFT	Countering Financing of Terrorism
Customer	Is any person or entity who enters a business relationship or carries out an occasional

	financial transaction with the bank
Authorities	The competent government authorities in the State entrusted with the implementation of any provision of this Decree law
Confiscation	Permanent expropriation of private funds or proceeds or instrumentalities by an injunction issued by a competent court
Crowd Funding	Is a practice of funding a project or venture by raising monetary contributions from large number of people
DNFBPs	Designated Nonfinancial Businesses and Professions
DSA	Direct Sales Agent
EDD	Enhanced Due-Diligence
FATF	Financial Action Task Force
Financial Illegal Organizations	Any physical or legal action aiming at providing funding to an illegal organization, or any of its activities or its members
FIU	Financial Intelligence Unit
Freezing or Seizure	Temporary restriction over the moving, conversion, transfer, replacement, or disposition of funds in any form, by an order issued by A Competent Authority
Funds	Assets in whatever form, whether tangible or intangible, movable or immovable including national currency, foreign currencies, documents, or notes evidencing the ownership of those assets or associated rights in any form including electronic or digital forms or any interests, profits or income originating or earned from these assets
KYC	Know Your Client
LEA	Law Enforcement Authorities
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
Non-Profit Organizations	Any organized group, of a continuing nature set for a temporary or permanent time, comprising natural or legal persons or not for profit legal arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural, educational, social, communal or any other charitable activities
OFAC	Office of Foreign Assets Control - it administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign states, organizations, and individuals
PEP	Politically Exposed Person (s) – An individual who is or has been entrusted with prominent public functions, for example Heads of State Government, Senior Politicians, Senior Government, Juridical or military officials. This definition extends to family members of an identified PEP
Predicate Offence	In the context of money laundering in the United Arab Emirates (UAE), a predicate offense is any underlying criminal activity that generates illicit proceeds that are subsequently laundered. The UAE's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Law broadly defines predicate offenses as any act constituting a felony or misdemeanor under the laws of the UAE, whether committed inside or outside the country, when such act is punishable in both jurisdictions. This means that a wide range of crimes can serve as predicate offenses for money laundering, including. Predicate offences can include a wide range of criminal activities, such as fraud, corruption, drug trafficking, terrorism, organized crime, tax evasion, and other serious crimes. By identifying and prosecuting predicate offences, authorities can disrupt the financial flows associated with criminal activities and prevent individuals from profiting from their illegal actions.
RBA	Risk Based Approach – Method for allocating resources to the management and mitigation of ML/FT risk in accordance with the nature and degree of the risk
SCA	Securities and Commodities Authority
SDD	Simplified Due Diligence
SDN	Specially Designated Nationals – Individuals and organizations with whom OFAC has placed a prohibition from doing business with
Settlor	A natural or legal person who transfers the control of his funds to a Trustee under a

	document
Shell Company	A company or a bank without Physical presence
State	The UAE
STR	Suspicious Transaction Report
Supervisory Authority	Federal and local authorities which entrusted by legislation to supervise financial institutions
Suspicious Transactions	Transactions that raise concerns about the possibility of money laundering or other illicit activity. These transactions may be flagged by automated systems or identified by compliance personnel based on their understanding of the customer's business, risk profile, and transaction history. Some common red flags that may indicate a suspicious transaction include:
TF	Terrorist Financing
TFS	Targeted Financial Sanctions – it is part of international sanctions regime issued by the UN Security Council under Chapter (7) of the UN for the prohibition and suppression of the financing of terrorism and proliferation of weapons of mass destruction
Trust	Legal relationship in which settlor places funds under the control of a trustee for the interest of a beneficiary or for a specified purpose.
Trustee	Natural or legal person who has the rights and powers conferred to him by the Settlor or the Trust under which he administers, uses, and act with the funds of the settlor in context of the trust conditions
UBO	Ultimate Beneficial Owner
WMD	Weapons of Mass Destruction
FIOs	Financial of Illegal Organizations
SoF	Source of fund
SoW	Source of Wealth
CSPs	Corporate Service Providers

7. Definitions AML/CFT Strategy, Legal & Regulatory Framework of the UAE

7.1. Regulatory Environment

IDB is committed to adhering to all applicable anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations, both domestically and internationally. In order to do so, IDB has carefully reviewed and incorporated into this policy and related procedures the relevant regulations issued by the Central Bank of the UAE (CBUAE). IDB also considers global best practices and the expectations of its correspondent banks, ensuring that its AML/CFT framework is both comprehensive and effective.

By adopting a risk-based approach to AML/CFT, IDB is able to tailor its controls to the specific risks posed by its customer base and products. This approach ensures that IDB is able to allocate its resources effectively and efficiently, while still maintaining a high level of compliance.

IDB's AML/CFT framework is subject to ongoing review and update, in order to reflect changes in the regulatory landscape and emerging risks. This ensures that IDB's controls remain relevant and effective in the ever-changing financial environment.

7.2. International AML/CFT Framework

The UAE's AML/CFT legislative and regulatory framework is embedded within a broader international AML/CFT architecture, encompassing a network of intergovernmental legislative bodies and international and regional regulatory organizations. This intricate framework is underpinned by international treaties and conventions aimed at combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. These

intergovernmental legislative bodies formulate international laws, which participating member countries are tasked with incorporating into their national frameworks.

In parallel, international and regional regulatory organizations develop comprehensive policies and issue recommendations. These organizations also assess and monitor the implementation of international AML/CFT standards by participating member countries. The UAE government and competent authorities actively collaborate with several key entities within the international AML/CFT framework, including:

- The United Nations (UN): The UN plays a central role in formulating and promoting international AML/CFT standards. It has adopted various resolutions and conventions, including the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988), the United Nations Convention against Transnational Organized Crime (2000), and the International Convention for the Suppression of the Financing of Terrorism (1999). These conventions provide the foundation for global AML/CFT efforts.
- The Financial Action Task Force (FATF): The FATF is an intergovernmental body established in 1989 to develop and promote effective AML/CFT policies. It sets global standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. The UAE is a fully compliant member of the FATF and actively participates in its activities.
- The Middle East and North Africa Financial Action Task Force (MENAFATF): MENAFATF is a regional AML/CFT body established in 2004 to strengthen AML/CFT measures in the Middle East and North Africa (MENA) region. The UAE is part of Gulf Cooperation Council (GCC) which is member of MENAFATF. is an active member of MENAFATF and contributes to its initiatives aimed at enhancing AML/CFT compliance in the region.

The UAE's commitment to the international AML/CFT framework is evident in its comprehensive AML/CFT legislation, robust regulatory oversight, and active engagement with intergovernmental and regional organizations. This dedication to combating financial crimes is essential for safeguarding the UAE's financial system and protecting its economy from illicit activities.

7.3. UAE AML/CFT Regulatory Landscape

The United Arab Emirates (UAE) has adopted a robust stance against money laundering (ML), terrorism financing (TF), and the financing of illegal organizations (FIOs). The country's commitment to combating these financial crimes is evident in the comprehensive legislative, regulatory, and institutional frameworks that have been established.

Unlike other jurisdictions where criminal law may vary across regions, the UAE has enacted a unified set of criminal statutes applicable throughout the country, including the financial and commercial free zones. This ensures that the crimes of ML, TF, and FIOs are consistently defined and prosecuted across the UAE.

The UAE's primary AML/CFT legislation is Federal Decree-Law No. (20) of 2018, supplemented by Cabinet Decision No. (10) of 2019 and Cabinet Decision No. (74) of 2020. These laws outline the responsibilities and obligations of financial institutions and other relevant entities in preventing, detecting, and reporting ML, TF, and FIOs. Additionally, Cabinet Decision No. (58) of 2020 establishes requirements for identifying and verifying the ultimate beneficial owners (UBOs) of entities.

The implementation and enforcement of AML/CFT regulations fall under the purview of various regulatory authorities, including the Central Bank of the UAE (CBUAE), the Securities and Commodities Authority (SCA), and the Financial Services Regulatory Authority (FSRA). These authorities issue guidelines and notices to assist financial institutions in effectively complying with AML/CFT requirements.

IDB is fully committed to adhering to the UAE's AML/CFT framework. The bank regularly reviews and enhances its AML/CFT policies and procedures to ensure compliance with the latest regulatory requirements and international best practices. This commitment is essential in protecting the integrity of the financial system and safeguarding the interests of IDB's customers and stakeholders.

7.4. UAE National Risk Assessment (NRA)

In line with the UAE's commitment to combating money laundering and terrorist financing (ML/TF), a comprehensive National Risk Assessment (NRA) was conducted. This assessment serves to deepen the understanding of the inherent ML/TF risks faced by both the public and private sectors in the UAE, thereby facilitating the development and implementation of appropriate mitigation measures. The NRA identified the onshore banking sector as one of the highest risk sectors for ML/TF due to the diverse range of products offered, the varying nature of clients, the inherent complexity of the sector, and its extensive geographical reach.

IDB is firmly committed to incorporating the findings of the NRA, including the identified ML threats and sector-specific risks, into its ongoing AML/CFT framework enhancements. The bank is dedicated to ensuring that its financial crime systems and controls undergo continuous review and improvement to effectively address the key ML/TF threats and sector-specific risks outlined in the NRA report. This steadfast commitment to risk mitigation is fundamental to IDB's mission of upholding the integrity of the financial system and safeguarding the UAE's reputation as a global financial hub.

7.5. Predicate Offences and Penalties

The AML/CFT law defines a predicate offence as any act constituting an offence or misdemeanor 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. A predicate offence is therefore any crime, whether felony or misdemeanor, which is punishable in the UAE, regardless of whether it is committed within the state or in any other country in which it is also a criminal offence.

FATF has designated 21 predicate offences, each of these has been criminalized in the legislative framework of the UAE. According to Clause (1) of Article (2) of the Law (20) of 2018, any person having the knowledge that the funds are the proceeds of a felony or a misdemeanor, and who willfully commits any of the following acts, shall be considered a perpetrator of the crime of Money Laundering:

- Transferring or moving proceeds or conducting any transaction with the aim of concealing or disguising their illegal source.
- Concealing or disguising the true nature, source, or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.
- Acquiring, possessing, or using proceeds upon receipt.
- Assisting the perpetrator of the predicate offence to escape punishment.

The crime of ML is considered as an independent crime. The punishment of the perpetrator for the predicate offence shall not prevent his/her punishment for the crime of money laundering. A conviction with a predicate offence shall not be deemed as a condition to prove the illicit source of the proceeds.

As per Article (3) of the Law (20) of 2018 Financing of terrorism as a criminal offense, which is not subject to the statute of limitations. It defines the financing of terrorism as:

- Committing any act of money laundering, being aware that the proceeds are wholly or partly owned by a terrorist organization or terrorist person or intended to finance terrorist organization, terrorist person or a terrorism crime, even if it without the intention to conceal or disguise their illicit origin; or
- 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 offence, or committing such acts on behalf of a terrorist organization or a terrorist person while aware of their true background or purpose.

The supervisory authority (CBUAE) shall impose the following administrative penalties on the financial institutions in case they violate the present Decree Law and its Executive Regulation:

- Warning

- Administrative fines of no less than AED 50,000 and no more than AED 5,000,000 for each violation
- Banning the violator from working in the sector related to the violation for the period determined by the supervisory authority.
- Restricting the powers of the board members, supervisory of executive management members, managers or owners who are proven to be responsible for the violation including the appointment of temporary inspector.
- Suspending managers, board members and supervisory and executive management members who are proven to be responsible for the violation for a period to be determined by the supervisory authority or request their removal.
- Suspending or restricting the practice of the activity or the profession for a period to be determined by the supervisory authority.
- Cancelling the license

Further penalties applicable to natural and legal persons who commit or attempt to commit ML, TF or the FIOs or anyone who violates on purpose or by gross negligence the provision of the law is specified in multiple articles of the law (20) of 2018.

8. AML/CFT Framework

8.1. Strategy and Risk Appetite

Acknowledging the various risks of financial crime to which it is exposed, the bank shall establish a well-defined AML/CFT Risk Appetite Statement which is approved by banks' Board/Committee on annual basis. The Risk Appetite Statement ensures that customers are not onboarded without a complete understanding of the potential risks of the bank's products, services and channels being used for illegal/criminal activities. The bank's senior management will ensure that The Risk Appetite is strictly enforced and that it sets clear standards to identify, monitor, detect, report, prevent and mitigate financial crime risk.

In addition:

- IDB has established a Three lines of Defense (3LoD) model that has been embedded to identify, assess, and manage all compliance related risk across the bank.
- IDB applies a risk-based approach when conducting due diligence on its customers (new and existing). This also includes the application of Enhanced Due Diligence (EDD) for customers who are deemed to pose a higher level of risk exposure to IDB from AML/CFT perspective.
- IDB only enters relationship where:
  - The purpose and nature of the relationship is clearly identified.
  - The identity of the customer including UBO(s), connected parties (i.e., authorized signatories) is established and appropriately verified.
  - All the required KYC information is obtained.
- IDB conducts risk-based periodic reviews and event driven reviews over its customer population on an ongoing basis.
- IDB has implemented automated screening controls for all customers and connected parties. Screening is conducted during various stages of the customer relationship, as per the below:
  - Customer onboarding
  - Periodic reviews
  - Event driven reviews.
  - Transactions processing
  - Portfolio screening
- IDB has implemented automated transactions monitoring controls to detect unusual/suspicious transactions. This is supplemented by appropriate investigation, escalation, and reporting protocols for unusual and/or suspicious activities.

- IDB provides AML/CFT role-based training and awareness program to assist all employees in identifying and reporting AML/CFT related issues.

8.2. Governance

IDB has adopted the Three Lines of Defense (3LoD) model to effectively identify, assess, and manage AML/CFT risks throughout the organization. This comprehensive approach ensures robust risk management and governance by clearly defining roles and responsibilities across three distinct lines of defense. Each line plays a crucial role in safeguarding IDB's operating environment from financial crimes.

First Line of Defense (FLoD)

IDB's business and support units, including Operations units, collectively form the First Line of Defense (FLoD) against financial crime. They are responsible for identifying, managing, and mitigating risks as an integral part of their day-to-day operations.

The head of business units is responsible for implementing the requirements of the Banks AML/CFT framework and must:

- Owning the risk identification process: Proactively identifying and assessing AML/CFT risks associated with their respective business areas, products, services, delivery channels, and jurisdictions.
- Implementing robust controls: Designing, implementing, and maintaining effective controls to mitigate identified AML/CFT risks.
- Contributing to the Enterprise-Wide Risk Assessment (EWRA): Providing inputs to the EWRA process to ensure that evolving ML/FT and sanctions risks are adequately addressed.
- Assigning CDD responsibilities: Clearly defining and assigning responsibilities for completing customer due diligence (CDD) procedures to respective business unit staff.
- Developing and enforcing SOPs: Establishing and maintaining comprehensive Standard Operating Procedures (SOPs) that align with the Bank's AML/CFT policy, relevant appendices, and applicable laws and regulatory directives.
- Ensuring CDD compliance: Overseeing the adherence of CDD procedures to ensure that they comply with the SOPs and the AML/CFT Policy guidelines.
- Defining CDD quality metrics: Establishing clear metrics to measure the quality and effectiveness of CDD records.
- Remaining vigilant for suspicious activity: Promptly identifying and reporting potential suspicious customer activity, including transactions that deviate from expected patterns or are inconsistent with the customer's profile or stated turnover.
- Establishing Quality Assurance (QA) mechanisms: Implementing a robust QA framework to regularly review and assess the effectiveness of FLoD activities.
- Collecting and analyzing management information (MI): Gathering, reviewing, and analyzing MI to ensure compliance with the AML/CFT policy and relevant SOPs.
- Defining and implementing governance processes for FLOD: Establishing clear governance processes for FLOD activities, including turnaround times and escalation mechanisms for coordinating with the Second Line of Defense (SLoD) on query resolutions.
- Developing an RFI tracker: Implementing an RFI (Request for Information) tracker that assigns clear responsibilities to business units and defines decision-making requirements based on the nature of the RFI.
- Managing KYC/CDD data: Owning, maintaining, and ensuring the accuracy and completeness of KYC/CDD data. Defining and implementing KYC data quality assessment and remediation processes, establishing robust system validation controls, and mapping/reconciling all source systems.
- Conducting due diligence on third parties: Performing appropriate due diligence and implementing adequate measures before entering into agreements with third parties where the Bank may be relying on their services or outsourcing AML/CFT functions.
- Ensuring record-keeping compliance: Defining and implementing requirements for maintaining comprehensive records in accordance with the provisions of this policy and applicable regulations.

Second Line of Defense (SLoD)

The Second Line of Defense (SLoD) encompasses IDB's control functions, which are tasked with providing independent and objective oversight, guidance, and support to the First Line of Defense (FLoD) in managing compliance risks. This collaborative approach ensures that compliance risks are effectively identified, assessed, and mitigated across all business units.

The SLoD operates independently from the business, ensuring that its assessments and recommendations are free from conflicts of interest. It holds the authority to challenge and, where necessary, halt business activities that pose unacceptable compliance risks. The SLoD comprises the IDB Compliance function, that includes the Financial Crime compliance, Assurance and Oversight, Regulatory Compliance and Advisory and Sanctions. Key Responsibilities of the Compliance Department:

- KYC and AML/CFT Policy: Define, maintain, and regularly review the AML/CFT policy to align with evolving regulatory requirements and industry best practices.
- Customer Risk Assessment (CRA) Model: Develop and maintain a robust CRA model to assess the AML/CFT and sanctions risk posed by customers. Document and maintain the detailed methodology underpinning the CRA process.
- EWRA methodology: Define and maintain EWRA methodology and facilitate EWRA exercise.
- Advisory Services: Provide timely and insightful advisory services to the FLoD on compliance-related matters.
- AML/CFT Training Material: Develop and periodically refresh AML/CFT training material, including role-specific training modules, to enhance employee awareness and understanding of ML/FT risks relevant to their respective business units.
- Record Keeping Requirements: Define and implement clear record-keeping requirements to ensure compliance with the provisions of this policy and applicable regulatory mandates.

Third Line of Defense (3LoD)

3LoD refers to the independent assurance provided by IDB's Internal Audit (IA) function.

8.3. Roles and Responsibilities

8.3.1. Board and Senior Management

Senior Management together with the members of the board of directors are ultimately responsible for the quality, strength, and effectiveness of the bank's AML/CFT framework, as well as for the robustness of its compliance culture, and setting the tone at the top.

Their responsibilities can be grouped broadly into the following:

- Implementation of governance, control, and operating systems.
- Approval of AML/CFT related policies, procedures, and controls, including the banks overall ML/FT risk appetite.
- Oversight of AML/CFT compliance program, including approving the establishment and continuance of increased risk and PEP clients, approving the establishment and continuance of relationship with correspondent banks.
- Applying the directives of Competent Authorities for implementing UN Security Council Decisions and all other directives of the relevant Competent Authorities of the State, including Cabinet Decision (10) of 2019.

8.3.2. Compliance Officer and Money Laundering Reporting Officer (MLRO)

In accordance with UAE Cabinet Decision No. (10) of 2019 and Federal Law No. (20) of 2018, IDB is mandated to appoint a designated Compliance Officer (CO) who possesses the necessary qualifications and experience to fulfill

the statutory duties and responsibilities associated with this role. The Cabinet Decision emphasizes the independent nature of this function, requiring the CO to perform their duties with utmost autonomy. The appointment of the CO is subject to prior approval from the Central Bank of the UAE (CBUAE).

IDB's Head of Compliance serves as the designated CO and the Money Laundering Reporting Officer (MLRO). The CO/MLRO enjoys unrestricted and independent access to the CBUAE, the Financial Intelligence Unit (FIU), and other relevant authorities and Law Enforcement Agencies (LEAs).

To effectively carry out their responsibilities, the CO/MLRO must receive unwavering support from senior management and have access to adequate resources. The MLRO must promptly notify senior management of any significant deficiencies in technology or resources.

The CO/MLRO's responsibilities encompass:

- Financial Crime Compliance Advisory: Providing expert guidance on financial crime risks, regulatory compliance, and best practices.
- AML/CFT Program Management and Training: Overseeing the development, implementation, and review of IDB's AML/CFT program, ensuring it aligns with current regulations and industry standards. Additionally, conducting regular training sessions for staff to enhance their understanding of AML/CFT principles and procedures.
- Policy Management: Drafting, reviewing, and maintaining IDB's AML/CFT policies and procedures to ensure they remain consistent with applicable laws and regulations.
- Customer Acceptance Management: Implementing and overseeing customer due diligence (CDD) procedures to verify the identity and assess the risk profile of new and existing customers.
- ML/FT Reporting: Promptly and accurately reporting suspicious transactions and activities to the FIU in accordance with regulatory requirements.
- Sanctions and Fraud STR Oversight.

8.3.3. Branch Compliance Officer

The Branch Compliance Officer (BCO) plays a crucial role in ensuring that branch operations adhere to IDB's AML/CFT policies and procedures and comply with applicable laws and regulations. The BCO works closely with the Head of Compliance and the MLRO to implement and maintain effective AML/CFT controls at the branch level. BCO responsibilities encompass:

- Day-to-day AML/CFT Compliance Oversight:
  - Monitor branch transactions and activities for potential indicators of money laundering, terrorist financing, or other financial crimes.
  - Investigate suspicious transactions and report them promptly to the Head of Compliance and the MLRO.
  - Ensure the proper implementation of CDD procedures for all new and existing customers.
  - Verify customer identities and assess their risk profiles.
  - Maintain accurate and up-to-date customer records.
- Training and Awareness:
  - Conduct regular training sessions for branch staff on AML/CFT principles, procedures, and regulatory updates.
  - Raise awareness among branch employees about the importance of AML/CFT compliance and their role in preventing financial crimes.
  - Facilitate ongoing communication and collaboration between branch staff and the Compliance Department.
- Policy Implementation and Review:
  - Assist in the implementation and review of IDB's AML/CFT policies and procedures at the branch level.

- Ensure that branch operations align with the latest regulatory requirements and industry best practices.
- Provide feedback and suggestions for enhancing the effectiveness of IDB's AML/CFT program.

- Risk Assessment and Reporting:
  - Conduct regular risk assessments to identify and evaluate potential AML/CFT risks faced by the branch.
  - Develop and implement appropriate mitigation strategies to address identified risks.
  - Prepare regular compliance reports for the Head of Compliance and the MLRO.
- Sanctions and Fraud Prevention:
  - Ensure the effective implementation of sanctions screening processes at the branch level.
  - Implement and monitor fraud prevention measures to protect IDB from financial losses.
  - Investigate and report any suspected fraud incidents to the Head of Compliance and the MLRO.
- Regulatory Updates and Compliance:
  - Stay informed about the latest AML/CFT regulations and industry standards.
  - Ensure that branch operations adhere to all applicable laws and regulations.
  - Provide guidance to branch staff on regulatory compliance matters.

8.3.4. Business Line Staff

- Responsibility for Ensuring Compliance: Business units are explicitly tasked with ensuring that systems and controls are in place to comply with the AML/CFT policy and procedures, emphasizing their primary role in upholding compliance.
- Letter and Spirit of the Policy: All business line staff are reminded of their obligation to comply with both the "letter" and "spirit" of the AML/CFT policy and procedures, ensuring a comprehensive understanding and adherence to its principles.
- Effective Risk Management: Business line staff are specifically instructed to be responsible for ensuring "effective management of AML and CFT risk as applicable to their role," highlighting their duty to identify, assess, and mitigate risks within their respective areas of responsibility.

8.3.5. Independent Audit Function

The Independent Audit Function plays a crucial role in evaluating the effectiveness of the bank's AML/CFT program and identifying areas for improvement. They conduct independent audits to assess the adequacy of AML/CFT policies and procedures, review customer due diligence (CDD) processes, and validate transaction monitoring systems. The Independent Audit Function also provides recommendations to enhance the bank's overall AML/CFT risk management framework.

8.3.6. Human Resources – Staff Screening

Human Resources plays a crucial role in safeguarding the organization by conducting thorough background checks for prospective employees. These screenings, particularly those focused on criminal history, serve as a gatekeeper mechanism to prevent the infiltration of undesirable individuals. Background checks are conducted at the time of employee onboarding and continue on an ongoing basis throughout their employment. This comprehensive approach ensures that the organization maintains a trustworthy and compliant workforce. Key Responsibilities as per the following:

- Develop and implement comprehensive background screening policies and procedures in alignment with industry standards, regulatory requirements, and the organization's risk appetite.
- Engage with specialized background screening providers to conduct thorough background checks for all prospective employees, including verification of education, employment, criminal history, and creditworthiness.
- Evaluate and interpret background check results in a consistent and objective manner, ensuring that any red flags are appropriately addressed and documented.

- Maintain secure and confidential records of all background check information, adhering to data privacy regulations and organizational policies.
- Collaborate with hiring managers to make informed hiring decisions based on background check findings and overall candidate suitability.
- Provide ongoing monitoring of employees through periodic background checks or rescreenings as deemed necessary based on the organization's risk assessment.
- Conduct investigations into employee misconduct or suspected violations of company policies, including those related to criminal activity.
- Maintain clear communication channels with employees regarding the background screening process, their rights, and the organization's expectations regarding conduct and compliance.
- Stay abreast of evolving legal and regulatory requirements related to background checks and employee privacy.

9. IDB Risk Based Approach to AML/CFT

IDB is fully committed to upholding the highest standards of financial integrity and combating money laundering, terrorist financing, proliferation financing, sanctions violations, and bribery and corruption. Aligned with CBUAE guidance and global best practices, IDB has adopted a risk-based approach (RBA) to effectively monitor its business activities, customers, and transactions.

The RBA empowers IDB to proactively identify, assess, and understand the diverse risks associated with its operations. This approach enables the bank to tailor its AML/CFT measures to the specific risk profile of each customer, transaction, or product. This targeted strategy ensures that IDB allocates its resources efficiently, focusing on high-risk areas while maintaining appropriate controls for lower-risk segments.

By implementing the RBA, IDB can dynamically adapt its AML/CFT strategies to address evolving risks and emerging threats. In situations where heightened risks are identified, IDB can intensify its monitoring and control measures. Conversely, for lower-risk scenarios, IDB can streamline its procedures while maintaining a robust level of compliance.

This pragmatic and proportionate approach to risk management allows IDB to effectively mitigate ML/FT and sanctions risks while maintaining a smooth and efficient customer experience. IDB is continuously refining its RBA, incorporating new insights and best practices to ensure that its AML/CFT framework remains robust and adaptable in the face of ever-changing risk landscapes.

9.1. Enterprise-wide Risk Assessment

IDB's identification and assessment of the money laundering (ML) and terrorist financing (TF) risks it faces will be conducted in a comprehensive and granular manner, considering the bank's business nature, size, and diverse operational footprint. This assessment will be based on a thorough evaluation of various risk factors and sub-factors, taking into account the latest information provided through the National Risk Assessment (NRA). The findings of this assessment will be documented in the bank's Enterprise-Wide Risk Assessment (EWRA), serving as a critical foundation for the development and implementation of effective and proportionate ML/FT risk mitigation measures.

The EWRA will encompass a detailed examination of the bank's customer base, product offerings, geographic reach, transaction patterns, and other relevant aspects of its operations. This comprehensive assessment will enable the bank to identify and prioritize ML/FT risks, allowing it to allocate resources and implement controls in a targeted and efficient manner. The EWRA will be conducted on an annual basis, ensuring that the bank's ML/FT risk management framework remains aligned with the evolving risk landscape.

IDB's EWRA is a fundamental pillar of its risk-based approach to AML/CFT. By proactively identifying and assessing ML/FT risks, the bank can effectively mitigate these risks and protect itself from potential financial and

reputational harm. The EWRA serves as a roadmap for the bank's AML/CFT compliance efforts, ensuring that the bank's controls are tailored to the specific risks it faces.

9.2. Products and Services Risk Assessment

In accordance with the AML/CFT Decision of 2019, IDB is obligated to proactively identify and assess potential money laundering and terrorist financing risks associated with the development and implementation of new products, emerging technologies, and modifications to existing product offerings.

Prior to the launch of any new product, business proposition, or modification to existing offerings, including the introduction of new channels or technologies, a thorough review and approval process must be undertaken by the Compliance department. Business owners and product managers bear the responsibility of ensuring compliance approval is secured before product or service launch.

During the review process, the Compliance department will meticulously evaluate the potential money laundering and terrorist financing risks associated with the proposed product, service, channel, or technology. Based on this assessment, the Compliance department will provide guidance on appropriate mitigation strategies to effectively address the identified risks.

9.3. Country Risk

Country risk plays a pivotal role in shaping IDB's Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) program. The bank recognizes that certain countries and jurisdictions pose a heightened risk of financial crimes, including money laundering, terrorist financing, and proliferation financing. These jurisdictions may include:

- Countries subject to international sanctions
- Countries identified as supporting international terrorism
- Jurisdictions considered primary money laundering concerns and subject to special measures
- Offshore financial centers
- Jurisdictions or countries with deficiencies in combating ML and TF

With the adoption of a risk-based approach (RBA) as the cornerstone of financial crime prevention, country factors have emerged as critical elements in assessing the financial crime risk posed by customers and in determining the overall enterprise-wide AML/CFT risk profile of the bank.

To effectively manage country risk, IDB has implemented a comprehensive Country Risk Assessment Model (CRAM). This model is underpinned by a well-defined governance framework, a structured approach, robust methodologies, and a suite of assessment tools. The CRAM incorporates a range of financial crime-relevant risk parameters and dimensions, drawing upon reputable sources of information to generate country risk scores.

IDB's Country Risk Assessment Register serves as a centralized repository of country risk information, ensuring consistency across all departments and business units when evaluating country risk from an AML/CFT perspective. This register is seamlessly integrated with the CRAM and the Enterprise-Wide Risk Assessment (EWRA), reflecting the inherent relevance of country risk in all risk assessments conducted by the bank.

9.4. Customer Risk

Implementing a risk-based approach to Customer Due Diligence (CDD) is crucial for establishing an effective Know Your Customer (KYC) policy and mitigating money laundering and terrorist financing (ML/TF) risks. The extent of CDD measures applied to customers should be commensurate with the level of ML/TF risk they pose.

Each customer's ML/TF risk profile is dynamic and can evolve over time due to various factors, such as the emergence of new information or changes in their behavior. Consequently, the appropriate level of CDD should be tailored to the specific circumstances and risk indicators identified for each customer. Therefore, the type and intensity of CDD applied should be heightened whenever the circumstances warrant. Depending on the

evolving risk profile, a customer's risk classification may need to be reassessed and, if necessary, subjected to Enhanced Due Diligence (EDD).

Customer risk assessments should be conducted regularly to reflect changes in circumstances, behavior, or risk profiles. Ongoing monitoring of customer accounts and transactions is essential for identifying potential ML/TF risks and taking appropriate action, which may include escalating to EDD or reporting suspicious transactions.

By adopting a risk-based approach to CDD, financial institutions can effectively allocate resources, target their AML/CFT efforts, and minimize the risk of facilitating illicit activities while maintaining a customer-centric approach.

9.5. Customer Risk Reporting of Key metrics to Senior Management & Board

The Bank must report key metrics to senior management to address evolving AML/CFT and Sanction concerns in the bank, enabling the senior management to make informed decisions. The metrics reported must provide accurate and timely information on the r status of the AML/CFT program and must include all aspects or critical ML/FT, Sanctions and Proliferation Financing (PF) risks, including amongst other weaknesses in the execution of policies, procedures, and risk controls.

Reporting shall include the following at a minimum:

- Portfolio composition focusing on the Risk Classification and on-boarding of increased risk, FPEP and UAE PEP NTB customers.
- Up-to-date information on the status of customer identification documents, including identification of expired documents and actions taken to address them.
- Status of periodic and thematic reviews conducted to identify and assess AML/CFT risks and compliance adherence.
- Summary of AML monitoring activities, including:
  - Number of reviewed cases.
  - Conversion rate of reviewed cases to investigations.
  - Total number of suspicious transaction reports (STRs) filed, along with the source of each investigation.
  - Identification of recurring AML typologies.
  - Number of internal STRs generated.
  - Status of outstanding STRs and investigations.
- Status on the outsourcing observations raised by regulatory, internal, external audit.
- Reporting of any breaches related to the Anti-Bribery Policy, Insider Trading Policy, or other relevant policies.
- Comprehensive data on sanctions-related activities, including:
  - Blocked payments.
  - Trade finance.
  - Payment screening.
  - Rejections by Correspondent banks.
  - Portfolio Screening.
  - Trends and hit rate analysis.
- EWRA, prevention, detection, and remediation if any.
- Training and awareness messages

The senior management committee should receive regular reports on the Bank's key AML/CFT risks and trends, along with an overall assessment of the performance of AML/CFT controls. These reports should provide insights into the effectiveness of the AML/CFT program and enable informed decision-making to mitigate emerging risks and maintain compliance with regulatory requirements.

In addition to these regular reports, the committee should also review the Bank's financial crime risk assessment, any AML/CFT regulatory reports, and the written AML/CFT program on an ongoing basis to ensure that the Bank's AML/CFT framework remains robust and aligned with the evolving regulatory landscape.

10. Know Your Customer Policy

Effective Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) frameworks rely heavily on Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures. These processes are crucial for identifying and verifying the identity of new and existing customers, ensuring they align with IDB's risk appetite.

While both KYC and CDD contribute to AML/CFT compliance, they differ in their scope and depth:

- KYC focuses on establishing a customer's identity and corporate information. This involves collecting, verifying, and classifying relevant data, including the customer's legal name, address, financial status, and ownership structure.
- CDD delves deeper into the customer's activities and risk profile. It encompasses a broader range of procedures and information gathering, including:
    - Ongoing Monitoring: Regularly reviewing customer accounts and transactions to detect suspicious activity.
    - Enhanced Due Diligence (EDD): Intensifying scrutiny for high-risk customers, such as politically exposed persons (PEPs) or those involved in sensitive industries.

No business relationship can commence until the onboarding process is complete. This multi-step process ensures thorough customer vetting:

- Customer Identification and Verification: Gathering and verifying identity documents, such as passports, utility bills, or business registration certificates.
- Screening: Scrutinizing customers against PEP lists, negative news databases, and sanctions lists to identify potential risks.
- Client Risk Assessment and Classification: Assessing the customer's risk profile based on their industry, transaction patterns, and geographic location.
- Complete CDD/EDD: Conducting comprehensive CDD/EDD procedures based on the customer's risk classification.
- Obtaining Approvals: Securing necessary approvals from management or compliance teams before establishing the business relationship.
- Obtaining the required approvals

10.1. Customer Identification and Verification (CIV) – Document Collection

IDB is committed to establishing the true and full identity of all parties involved in a single relationship. We will not enter into a relationship with any individual or entity that does not successfully complete our identification and verification process.

CIV Requirements applicable to Legal Entities (Juridical Persons)

In case of juridical (legal) persons, the minimum information / documentary requirements for opening an account	• Trade License (copy of valid trade license – upon verification of the original) and should always be held on file throughout the relationship. • Article of Association or any similar documents, attested by the competent authority within the UAE. • Full name and address of the account holder • Proof of operational/physical address; if the legal person or arrangement is a foreigner (offshore or branch of foreign company), it must mention the name and address of its legal representative in the

	UAE and submit the necessary as a proof. • Understand and document the intended purpose and nature of the business relationship. • Understand the nature of customers business as well as the customers ownership and control structure. • IDB may conduct checks if required against the National Economic Register site for publicly available information on legal persons and arrangements, i.e., entity's license number, address, business activities, and the name of the manager.
Beneficial Owners and Controllers	• Full name, nationality, residential address and copy of valid government issued photo identification documents of all partners including the ultimate beneficial owner (s) (UBO*) as follows: o For Neutral/Low Risk Customers and Medium Risk Customer- if the shareholding is 15% and above. o For Increased/High Risk Customers- if the shareholding is 10% and above • In the event of multiple legal entities or arrangements with ownership interest, even where each legal entity owns less than the set thresholds as above, the UBO identification process should consider whether there are indications that the entities may be related by common ownership, which could reach or surpass the UBO threshold level of 15% or 10% in aggregate. • Full name, nationality, date of birth and title/position in the company of the person(s) holding senior management positions (e.g., CEO, CFO, COO and/or equivalent positions) and controlling persons.
Related parties	• Verify the identity of any person legally empowered to act or transact business on behalf of the customer, including signatories**, or other persons with authorized remote access credentials to an account, such as internet or phone banking users. • Verify that a person purporting to act on behalf of a customer is so authorized, through the following types of documents: o A legally valid power of attorney o A properly executed resolution of legal persons or legal arrangements governing board or committee. o A document from an official registry or other official source, evidencing ownership or the persons status as an authorized legal representative o A court order or other official decision ** it is not allowed to add non-UAE residents as Authorized Signatory (AUS) to a legal entity.
For Listed Companies	The requirement to identify and verify every shareholder, partner or UBO is not applicable provided that: the company or its holding company is listed on a regulated stock exchange subject to disclosure requirements that require adequate transparency of beneficial owners, and that the bank is able to obtain

	such information from reliable public sources* • Evidence/proof of exchange listing is required for all clients regardless of risk classification.
Trusts	For trusts, information of a settler, trustee, and the beneficiaries or identifiable class of beneficiaries, along with any other individual exercising ultimate effective control over the legal arrangement must be captured. Additionally, as part of the CDD process, the bank must identify and capture the individual as a trustee.

Beneficial Ownership

The bank is committed to identifying and verifying the beneficial ownership of all its customers, in line with its obligations under the Central Bank of the United Arab Emirates (CBUAE) guidelines on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).

Ultimate Beneficial Ownership (UBO)

The bank shall identify the ultimate beneficial owner(s) of all legal person and legal arrangement customers. An ultimate beneficial owner is the natural person(s) who ultimately owns or controls more than 25% of the shares or voting rights in a legal person, or who exercises ultimate control over the legal person or legal arrangement.

Verification of UBO Identity

The bank shall take sufficient and appropriate measures to verify the identity of the UBO, using documents, data, or information from an authenticated and independent source. This may include, but is not limited to, reviewing the following documents:

- For individuals: passport, driver's license, utility bill, or other government-issued identification document.
- For legal persons: corporate charter, articles of association, or other relevant documentation.
- For legal arrangements: trust deed, partnership agreement, or other relevant documentation.

The bank shall also obtain and review all necessary details and information about the UBO, such as their name, date of birth, address, nationality, and occupation. The due diligence measures taken by the bank shall be consistent with the degree and level of risk.

Identification of Senior Management

If no individual holds the ultimate beneficial ownership of the entity/legal person, the bank must identify the individuals/controllers who hold the senior management position(s) within the legal person. These individuals may include, but are not limited to, the chief executive officer, chief financial officer, and board of directors.

Verification of Settlor, Trustee, and Beneficiaries

For legal arrangements, the bank must verify the identity of the settlor and the trustee (or anyone holding equivalent positions for non-trust legal arrangements), the beneficiaries or class of beneficiaries, and any other individuals in control of the legal arrangements. The bank must also obtain sufficient information on the beneficial owners of a legal arrangement to enable verification of the beneficial owner when paying trust funds to the beneficial owner, or when the beneficial owner begins to exercise his or her legally acquired rights.

Demonstrating Understanding of Ownership Structure

The bank must be able to demonstrate that it understands the ownership structure of the customer and how it obtained details of the customer ownership structure and its ultimate beneficial owners (UBO's). This is typically accomplished through relevant constitutional documentation.

Complex Ownership Structures

When dealing with complex ownership structures, it is necessary to understand the indirect beneficial ownership interests within a legal structure and subject these persons to the necessary identification and verification processes. The bank should also question whether there is a legitimate economic purpose for the ownership structure of the entity.

10.2. Screening

Screening Procedures

To safeguard the integrity of the bank's operations and comply with anti-money laundering (AML) and combating the financing of terrorism (CFT) regulations, a comprehensive screening process is implemented for all customers and related parties. This involves screening against various risk categories, including criminal activities, money laundering, terrorism financing, politically exposed persons (PEPs), and sanctions.

Pre-Relationship Screening

Before establishing a new relationship or opening an additional account for an existing customer, the names of all relevant parties, including customers, power of attorney (POA) holders, authorized signatories, ultimate beneficial owners (UBOs), and any other individuals or entities involved in the relationship, must be screened against various risk lists. This screening process helps identify potential risks associated with the customer or their related parties and ensures that the bank is not inadvertently facilitating illicit activities.

The screening process encompasses a thorough review of the customer's name against recognized sanctions lists, including those maintained by the European Union (EU), United Nations (UN), United States Office of Foreign Assets Control (OFAC), and local regulatory bodies. This screening aims to prevent the bank from onboarding or conducting business with individuals or entities subject to sanctions.

External and Internal Lists

To effectively identify potential risks, the bank utilizes two types of screening lists:

External Lists: The bank employs a reputable third-party service provider, World-Check, to access and screen against external lists. This service primarily focuses on identifying potential PEPs, sanction targets, and individuals or entities associated with criminal, terrorist, or money laundering activities.

Internal List: The bank maintains and updates an internal blacklist, which serves as a repository of individuals or entities that have been declined for onboarding, deemed unacceptable, or pose a negative risk based on the bank's compliance standards. This internal list complements the external lists and ensures that the bank does not inadvertently engage with individuals or entities that have raised concerns in the past.

Risk-Based Approach to Adverse Media Screening

In addition to screening against risk lists, the bank adopts a risk-based approach to adverse media screening. This involves monitoring news sources, media outlets, and other publicly available information to identify potential red flags or negative associations related to the customer or their related parties. This approach helps uncover potential reputational or financial risks that may not be evident through traditional screening methods.

Compliance Consultation and Notification Restrictions

In cases where doubts arise during the screening process, branches and account opening units must promptly consult with the bank's compliance team for further guidance. Under no circumstances should the bank or any of its staff notify or warn customers about positive matches resulting from the screening process. Such notifications could jeopardize the bank's ability to investigate potential illicit activities and could also expose the bank to legal and regulatory repercussions.

10.3. Client Risk Assessment and Profiling

Client Risk Assessment (CRA) is an essential component of the Know Your Customer (KYC) process and a mandatory regulatory requirement. It involves evaluating the potential money laundering and terrorism financing (ML/TF) risks associated with customers and their transactions. This assessment helps determine the appropriate level of due diligence needed when establishing a relationship, as well as for ongoing due diligence and transaction monitoring throughout the relationship.

Adopting a Risk-Based Approach (RBA) to Customer Due Diligence (CDD) enables IDB to effectively identify customers with higher ML/TF risks, allowing for a more focused allocation of resources and efforts towards monitoring such customers.

CRA must be conducted for all IDB clients. For overall risk assessment and risk classification, IDB clients are categorized into the following risk categories:

- Neutral/Low Risk
- Medium Risk
- Increased/High Risk
- Very High Risk
- UAE PEP (Domestic PEP)
- Non-UAE PEP
- Un-acceptable Risk

CRA is performed on new-to-bank relationships and for existing customers at the point of periodic reviews or trigger event reviews. IDB has established the following risk factors for CRA and risk classification:

1. Customer Risk: The risk of inherent profile such as from customer industry, source of income, PEP status, etc.
2. Geographical Risk: Based on exposure to high-risk countries from ML/TF perspective.
3. Transaction Risk: Based on expected transactions, STRs raised, etc.- dynamic behavioral risk factor.
4. Product/Channel: Based on risk related to products, services and channels/mode of the transactions and delivery channels- dynamic behavioral risk factor.
5. Reputational Risk: Potential adverse publicity associated to existing and new customers.

In addition to these identified risk factors, business units and relationship managers must also consider factors such as client integrity, litigation history, regulatory/tax violations, disputes between parties, and political risk when determining the potential risk associated with a client.

It is crucial that all staff and units involved in client relationship establishment and maintenance fully understand the customer CRA process and strictly adhere to the prescribed guidelines. Completing the KYC form is mandatory for all customers.

10.3.1. Un-Acceptable Risk Relationship

The bank shall not establish relationship, open accounts, undertake one off transactions, maintain existing relationship or accounts, or otherwise conduct business through/with:

- Hawaladars and Non-Client Hawala Business Participants: Hawaladars are individuals or entities that facilitate cross-border money transfers without going through traditional banking channels. The bank will not engage with hawaladars directly or indirectly, nor will it open accounts or conduct transactions for individuals or entities that utilize hawala services.
- Sanctioned Jurisdictions and High-Risk Countries: The bank will not establish or maintain relationships with legal entities incorporated in sanctioned jurisdictions- Syria, Iran, Cuba, Ukraine (Crimea and Sevastopol), and North Korea, as well as other jurisdictions designated as Sanctioned by the bank's compliance department from time to time.
- Shell Banks and Shell Companies: Shell banks and shell companies are entities that are established or used to conceal the true ownership or purpose of their activities. The bank will not open accounts or conduct business with shell banks or shell companies.

- Financial Institutions Associated with Shell Banks: The bank will not engage with financial institutions that knowingly deal with shell banks or shell companies.

- Entities with Sanctioned Jurisdictions Residents: The bank will not establish or maintain relationships with legal entities where one or more partners, ultimate beneficial owners (UBOs), signatories, or power of attorney (POA) holders reside in a sanctioned jurisdiction.
- North Korean Nationals: The bank will not open accounts or conduct business with legal entities where one or more partners, UBOs, signatories, or POA holders are nationals of North Korea, regardless of their residency status.
- Online Gaming, Gambling, and Casino Businesses: The bank will not establish or maintain relationships with legal entities engaged in online gaming, gambling, or casino businesses.
- Virtual Offices and Flexi Desks with Trading Businesses: The bank will not open accounts or conduct business with legal entities that operate from virtual offices or flexi desks if it is engaged in trading activities.
- Virtual Asset Entities and Service Providers: The bank will not establish or maintain relationships with entities dealing in virtual assets, such as cryptocurrencies, or virtual asset service providers.
- Entities with Nominee Shareholders: The bank will not open accounts or conduct business with legal entities where nominee shareholders obscure the identity of the actual UBOs.
- Entities with Bearer Shares Structure: The bank will not establish or maintain relationships with legal entities, including their parent companies, that have a bearer shares structure, as this can hinder the identification of beneficial ownership.
- Weapons of Mass Destruction (WMD) and Proliferation Entities: The bank will not open accounts or conduct business with entities involved in the manufacturing, trading, or dealing of weapons of mass destruction (WMDs) or goods and services used in the proliferation of WMDs.

Further, IDB prohibits the following:

- Facilitating any occasional transaction for non-account holders or customers with whom there is no ongoing Business Relationship.
- Establishing or maintaining any customer or business relationship with anyone whose identities cannot be confirmed, or who does not provide all the required information.
- Establishing or maintaining any customer or business relationship with anyone who has provided false information or has provided information with significant inconsistencies.
- Establishing or maintaining any customer or business relationship or conducting any financial or commercial transactions or keeping any account under an anonymous or fictious name or by pseudonym or number.
- Establishing or maintaining any customer or business relationship or executing any financial transaction in event they are unable to complete adequate risk-based CDD/EDD measures in respect of client for any reason.
- Dealing in any way with shell banks, whether to open bank accounts in their names, or to accept funds or deposits from them.
- Establishing or maintaining relationships with individuals or entities designated by any of the watch lists such as Central Bank of UAE, UN, EU, OFAC, etc.
- Establishing or maintaining relationships with entities or their related parties known to have been involved in, but not limited to, corruption, fraud, terrorism, money-laundering or illegal activities.
- Establishing or maintaining relationships with entities where the legal and beneficial ownership is not clear and evident.
- Customer who failed the identification and verification process.
- Establishing or maintaining relationship with clients where purpose of account opening is deemed to be for tax evasion.

Where a business relationship is rejected as a direct result of failing to meet the due diligence requirements, a business unit must not under any circumstances refer the case to another business unit for consideration. Customers who have been rejected because of due diligence considerations relating to potential sanctions target, money laundering or who have otherwise been considered as posing an unacceptable risk to the business operations of IDB, should be notified directly to Compliance.

10.3.2. Very High-Risk/ High Risk Relationships

Certain legal entities pose a significantly elevated risk of money laundering (ML) and terrorist financing (TF) to the bank. These clients exhibit heightened risk factors due to their inherent characteristics, activities, business relationships, or geographic locations. They may include:

- Clients from high-risk countries or non-residents in a country where they do not hold an ID card.
- Clients with complex structures, engaging in intricate operations, or with unclear economic objectives.
- Clients conducting cash-intensive operations, transactions with unknown third parties, or operations without directly confronting any other high-risk operations identified by the bank.

The following client considered to be part of this categories due to their inherent association with ML and TF activities:

- Free trade zone entities including offshore.
- Trusts and foundations.
- Investment companies.
- Fund/asset management companies.
- Under formation companies.
- Financial institutions (FI) – Vostro and correspondent banking relationships (including respondent banks from high-risk countries).
- Non-Banking Financial Institutions (NBFI) including finance companies, insurance companies, brokerage.
- Entities involved in crowd funding / Peer to peer lending.
- Payment service providers (PSP)/ Online Payment Services/ Payment Aggregator.
- Exchange Houses and MSB's
- General Trading Companies
- Shipping lines (entities own, manufacture, or manage ships).
- Bullion / Commodity Traders.
- Diamond, Jewellery and/or precious stones dealers.
- Real estate brokers.
- Law firm/ Notaries / Audit firms/ Custodians.
- Corporate Service Providers/Registered Agents.
- Financial advisors / Consultants/ Brokers.
- Management Consultancy.
- Oil / Gas / Petroleum Trading.
- Online Marketplace.
- Used Automobile and Spare Parts Dealers.
- Auction Houses, Art or Antique Dealer.
- Cash Intensive Businesses.
- Non-Profit Organizations / Social and Charitable Organizations.
- Legal entities having one or more owner/partner/UBO national(s) of one of the following sanctioned jurisdictions (Iran, Cuba, Ukraine (Crimea and Sevastopol-Sanctioned) and Syria).
- Legal entities having one or more owner/partner/UBO national(s) of one of high-risk jurisdictions and not-resident in UAE.
- Offshore entities/ Entities incorporated outside UAE.

In accordance with the IDB policy, the bank prohibits establishing relationships with or facilitating transactions or financing of entities involved, directly or indirectly, in the manufacturing or trading of weapons of mass destruction (WMD) and/or the proliferation of goods and services used in the manufacture of WMDs (this prohibition includes both defensive and offensive goods).

10.3.3. Medium Risk Relationships

Certain relationships represent a moderate level of risk from a money laundering (ML) and terrorist financing (TF) perspective. These customers exhibit average risk to the bank, and the degree of risk may vary depending on factors such as the customer's background, the nature and location of their activities, their country of origin, source of funds, and overall profile.

The following customer categories are considered moderate risk:

- UAE-incorporated legal entities with one or more owners, partners, or ultimate beneficial owners (UBOs) who are nationals of an increased/high-risk jurisdiction while also being UAE residents.

For medium-risk customers, customer due diligence (CDD) measures should include, at a minimum:

- Proof of operating address.
- Site visit for legal entities.

10.4. Politically Exposed Persons (PEPs)

PEPs are defined by CBUAE as Natural persons who are or have been entrusted with prominent public function in the UAE 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 or political parties, and persons who are, or have previously been, entrusted with the management of an international organization or any prominent function within such an organization.

For the purpose of this policy and risk assessment, PEPs classified as either:

- UAE PEP (Domestic PEP) - PEPs who are or have been entrusted with their prominent public position in the UAE.
- Non-UAE PEP (Foreign PEP) – PEPs who are or have been entrusted with their prominent public position in any other foreign country.
- Head of International Organizations – PEPs who are or have been entrusted with the management or any prominent function within an international organization.

The distinction between domestic PEPs and foreign PEPs lies in the country that has entrusted the individual with the prominent position. While the definition of PEPs does not consider factors such as country of domicile or nationality, foreign PEPs are inherently considered to pose a higher risk due to their increased exposure to corruption or criminal activities.

In terms of risk categorization, the bank considers UAE PEPs as high-risk customers, while Head of International Organizations and Non-UAE PEPs are classified as very high-risk customers. This differentiation reflects the heightened risk associated with individuals holding prominent positions in foreign jurisdictions.

It is crucial to note that the definition of PEPs extends to direct family members of PEPs (spouses, children, spouses of children, siblings, parents) and close associates of PEPs. Close associates include:

- Individuals having joint ownership rights in a legal person or arrangement or any other close business relationship with the PEP.
- Individuals having individual ownership rights in a legal person or arrangement established in favor of the PEP.

For legal entities, the bank considers relationships to be high-risk if a partner, beneficial owner (UBO), or authorized signatory (AUS) is a PEP. However, legal entities fully owned by the UAE Government are not classified as PEPs. In contrast, legal entities owned (fully or partially) by a non-UAE Government are considered Non-UAE PEPs (Foreign PEPs).

Bank staff must be vigilant in identifying any situations where an existing individual account or legal entity structure has developed a PEP connection, particularly after the business relationship has been established. Promptly implementing the necessary Enhanced Due Diligence (EDD) measures is crucial to address any heightened risks associated with PEPs.

Time Limits for classification of a customer as a PEP:

The definition of Politically Exposed Persons (PEPs) under applicable UAE legislation does not automatically terminate a customer's PEP status upon their departure from a prominent public function. This is because the potential for corruption may persist even after the individual leaves office, given the time lag between illicit activities and their detection.

The IDB adopts a risk-based approach to declassifying PEPs, considering the following factors:

1) Declassification for Former Presidents or Heads of State:

Former presidents or heads of state will always remain PEPs, regardless of how long they have been out of office. Their high-profile status and influence, even after leaving office, warrant continued enhanced due diligence (EDD) measures.

2) Declassification for Other PEPs:

For other PEPs, the decision to declassify can be considered three years after they have left the position that rendered them a PEP. The following factors are considered when making this assessment:

- Seniority, Prominence, and Power of the Previous Role:
  The higher the level of seniority, prominence, and power held by the PEP, the greater the risk of corruption and the longer the EDD measures may be necessary.
- Corruption Potential of the Previous Role:
  Roles with greater opportunities for illicit gain are more likely to involve corrupt proceeds that may extend beyond the PEP's tenure.
- Informal Influence of the PEP:
  PEPs may continue to wield informal influence over government decision-making through their current roles (e.g., leadership in lobbying organizations) or personal connections.
- Linkage of Previous and Current Roles:
  Close connections between the PEP's previous and current roles suggest a continued risk of corruption.
- Relationships to Other PEPs:
  If the PEP has family members or close associates who are also PEPs, this may elevate the risk of corruption associated with the customer.
- Nature and Purpose of the Business Relationship:
  The type of business relationship and the products or services involved can significantly impact the overall risk profile.
- Customer's Relationship to the PEP:
  Family relationships tend to be more enduring than business connections. A customer who was formerly closely associated with a PEP, but has since severed ties may present a reduced risk.

It is crucial to note that the decision to declassify a PEP is not automatic and should be made on a case-by-case basis, considering the specific circumstances and the ongoing risk assessment.

10.5. Due Diligence

Simplified Due Diligence (SDD)

1. Applicability:

- SDD measures are appropriate for individual customers who are UAE residents and maintain only credit card relationships with IDB, without opting for liability accounts or other relationships.
- IDB currently does not apply SDD due to its wholesale banking license.
- SDD may be applied to certain treasury bookings.

2. SDD Procedures:

- Identify the customer:
  - Verify customer identity through official documents.
  - Record and document verification details.
- Screen customer and related parties:
  - Check against applicable sanctions and watchlists.
  - Document screening results.

3. Risk Assessment and Escalation:

- If during the relationship, a customer or product poses a higher risk than initially assessed, additional due diligence (CDD or EDD) must be conducted.
- SDD is not applicable if there is any suspicion of ML/TF or FIOs.

Standard Due Diligence (CDD)

1. Applicability:

- CDD measures apply to customers classified as Neutral/Low Risk and Medium Risk.
- CDD must be completed before establishing the relationship or opening the account.

2. Risk Assessment:

- Conduct a risk assessment for all parties involved in the relationship:
  - Client
  - Authorized signatories
  - Power of attorney holders
  - Partners
  - Ultimate Beneficial Owners (UBOs)

3. CDD Procedures:

- Verify customer identity:
  - Use reliable and independent sources.
  - Document verification details.
- Understand the customer's business and activities:
  - Collect information on the nature of the business, purpose of the account, and anticipated transactions.
  - Document the information obtained.
- Screen customer and related parties:
  - Check against applicable sanctions and watchlists.
  - Conduct enhanced screening for PEPs.
  - Document screening results.

Enhanced Due Diligence (CDD)

1. Applicability:

- EDD measures apply to:
  - Identified very high risk, high/increased risk, and PEP customers.
  - Situations with doubts about risk classification or red flag indicators.

2. EDD Procedures:

- In-person meeting:
  - Mandatory for all customers.
  - No onboarding using non-face-to-face platforms.
- Site visit:
  - Mandatory for all customers.
  - Document the outcome and obtain proof of operational address.
- Increased scrutiny and verification:
  - Identity of client, UBOs, and controlling persons.
  - Source of funds and income.
  - Business activities and transactions.
  - SoW and related documentation.
- Background checks:
  - Use internet searches, public databases, and subscribed databases.
  - Verify information for potential inconsistencies and suspicious circumstances.
- PEP Investigation:
  - Conduct a more in-depth investigation into the individual's professional and financial background prior to becoming a customer.
  - Analyze the PEP's exposure to corruption, bribery, and other financial crimes.
  - Implement enhanced monitoring procedures for PEP accounts.

3. Documentation:

  - Document all evaluations and assessments performed during the client profiling process.
  - Clearly record any inconsistencies or suspicious circumstances identified.
  - Maintain a comprehensive audit trail of all due diligence procedures and findings.

4. Particular attention should be given to the reasonableness of the information obtained. Client profiling staff should evaluate the information for possible inconsistencies and potentially unusual or suspicious circumstances, including but not limited to:

- Reason for foreign client or beneficial owner's presence or establishment of business in the UAE:
  - Assess the stated reason for their presence or business establishment and verify it through reliable sources, such as business licenses, commercial registries, and independent market research.
  - Investigate any significant discrepancies between the stated reason and available information.
  - Consider the economic and political climate of the client's home country and how it might influence their business activities in the UAE.
- Consistency between the nature of the client's business/transactions and the client's or beneficial owner's professional background and employment history:
  - Compare the client's business activities and transactions with their stated professional qualifications and work experience.
  - Seek independent verification of the client's professional background and employment history through reference checks, professional association memberships, and other reliable sources.
  - Analyze any inconsistencies between the client's business activities and their professional background, considering potential explanations and justifications.
- Level of complexity and transparency of the client's transactions or legal structure:
  - Evaluate the complexity of the client's transactions and legal structure, including the use of shell companies, offshore entities, and complex financial instruments.

- Assess the transparency of the client's financial activities, including the availability of documentation and the willingness to provide information.
- Investigate any unusual or unexplained complexities in the client's transactions or legal structure.
- Nature of any other business interests of the client or beneficial owner:
- Identify and verify any other business interests held by the client or beneficial owner, both within and outside the UAE.
- Assess the relationship between the client's other business interests and their primary business activities in the UAE.
- Consider whether the client's other business interests pose any potential risks for money laundering or terrorist financing.

- Consistency between the client's line of business (LOB) and that of the counterparty to the client's transactions:
  - Analyse the nature of the client's counterparties and their LOBs.
  - Compare the client's transactions with the counterparties' expected business activities.
  - Investigate any significant inconsistencies between the client's LOB and the counterparties' LOBs, considering potential explanations and justifications.

EDD will also include the following:

Risk Status Category	Requirements
Very High and High/Increased Risk (other Than PEPs)	• Completion of KYC Form including EDD section • Verification of SoF and SoW through supporting documents or independent reliable sources as applicable • Supporting documentary evidence for residential or operating address as applicable • Consideration of specific country risks, where client is resident in a jurisdiction which presents an increased risk. • Public domain search • Business Unit Head Approval • Compliance Approval
PEPs (for both UAE PEPs and Non-UAE PEPs)	• Completion of KYC Form including EDD section • Verification of SoF and SoW through supporting documents or independent reliable sources as applicable • Supporting documentary evidence for residential or operating address as applicable • Consideration of specific country risks, where client is resident in a jurisdiction which presents an increased risk. • Public domain search • Business Unit Head Approval • CEO/Regional Manager Approval • Compliance Approval

10.6. Source of Funds

Understanding SoF is crucial in safeguarding against money laundering and particularly critical when establishing relationships with high-risk and very high-risk clients, as defined by the Central Bank of the United Arab Emirates (CBUAE) regulations. All reasonable and practicable measures shall be taken to identify, verify, document, and corroborate the SoF for these relationships. This will significantly reduce the risk of inadvertently assisting a money launderer or terrorist individual in handling the proceeds of crime,

bribery, corruption, illegally diverted funds, and monies intended to support terrorism, as outlined in the UAE Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regulations.

SoF encompasses two key elements:

- The activity generating funds: This includes, but is not limited to, the client's employment, profession, business nature, and other legitimate sources of income.
- Details of the remitting account/institution: This includes, where funds originate from a third party, the name and location of the account/institution, its relationship to the client, and the nature of the transaction.

10.7. Source of Funds

Source of Wealth is distinct from SoFs and describes the activities which generated the total net worth of a person, both within and outside of an IDB relationship, i.e., the client's overall wealth. Examples of common "SoW" are listed in the table below, along with description indicating level of detail that should be obtained.

Description of source (origin) of wealth	Details Required	Documentary Evidence Required (as applicable) for corroboration purposes
Income-savings from salary (basic and/or bonus)	• Salary per annum • Employer's name and address • Nature of business • Duration of employment	• Pay slip (or bonus payment) from last 3 months or • Letter from employer confirming salary on letter headed paper or • 3 months bank statements clearly showing receipt of most recent regular salary payment from names employer
Sale of investment / liquidation of investment portfolio	• Description of shares / units / deposits. • Name of seller. • How long held. • Sale amount. • Date when the funds were received.	• Investment/savings certificates, contract notes or surrender statements or • Bank statement clearly showing receipt of funds and investment company name or signed letter detailing funds from a regulated accountant on letter headed paper
Sale of Property	• Sold property address. • Date of sale • Total sale amount	• Letter detailing the property sale signed by a licensed solicitor or regulated accountant on letter-headed paper or • Copy of contract of sale
Company Sale	• Name and nature of the company • Date of sale • Total amount of clients shares	• Letter detailing the company sale signed by a licensed solicitor or regulated accountant on letter-headed paper or • Copy of contract of sale, plus bank statement showing proceeds or • Copies of media coverage (if applicable) as supporting evidence
Inheritance/Gift	• Name of the deceased • Date deceased/relationship to client • Date received. • Total amount • Donor's source of wealth • Solicitors' details	• Grant of probate (with a copy of the will) which must include the value of the estate or signed letter from licensed solicitor or estate trustees on letter-headed paper or • Copy of the will
Accumulated company profits	• Name and address of the company • Nature of business • Amount of annual profit. Date	• Copy of latest audited company accounts or Confirmation of the nature of business activity and turnover, detailed in a letter from a regulated accountant or

	of receipt of dividend and total amount	• Bank statement clearly showing receipt of funds and name of company paying dividends

For trust (and similar legal arrangements such as foundation) accounts, SoW information should be obtained for the assets settled into trust, together with SoW of the settlor.

For other corporate clients (such as Special Purpose Vehicles (SPVs), LLCs, Holding Cos), if the entity has been created to manage wealth, SoW information should be obtained in relation to the origin of the assets transferred to the company.

10.8. Approvals/Sign Off Arrangements

Customers classified as Neutral Risk do not require Compliance approval/sign off, however, a KYC form must be filled, including a four-eye check at the business level.

Clients classified as Medium Risk do not require Head of Compliance approval, however, Compliance Branch Officer should review and approve the application. Further, the Designated Business Head (or delegates) approval without which the account opening should be declined by the processing department.

Customers classified as Very High or High / Increased Risk must have the Designated Business Head (or delegates) approval and Head of Compliance Approval, without which the account opening should be declined by the processing department.

Customers classified as PEPs must additionally have CEO/Regional Manager approval. Regarding existing PEP relationship, CEO/Regional Manager should be notified, and his approval should be obtained for retaining the relationship each time any of the following situation occur.

- An existing client (or beneficial owner, UBO, POA, Authorized Signatory) becomes, or is newly identified as PEP.
- An existing PEP relationship is reviewed as part of periodic, thematic or an event basis.
- A material transaction that appears unusual or out-of-pattern for the existing PEP client.

Prospect assessed “Unacceptable” during CDD should be rejected and reported to Compliance Department. Compliance will add those entities to the Internal Blacklist.

Once the customer risk assessment has been completed and relevant due diligence measures have been performed in line with the customer’s risk classification, required approvals must be obtained as set out in the table below:

Risk Classification	**Assessed Neutral Risk**	**Medium Risk**	**Very High/High-Increased Risk**	**UAE PEP**	**Very High Risk (Foreign PEPs/Head of International Organizations, Exchange Houses, CB, NPOs/Charities)**
Approvals	• RM (Initiator) • Line Manager (approver)	• RM (Initiator) • Business Head (approver) • Compliance Branch Officer (approver)	• RM (Initiator) • Business Head (approver) • Compliance Head (approver)	• RM (Initiator) • Business Head (approver) • CEO/Regional Manager • Compliance Head (approver)	• RM (Initiator) • Business Head (approver) • CEO/Regional Manager • Compliance Head (approver)

Delegation matrix – the FLOD delegation protocols are applicable here and will be applied in relation to the provision of the requisite sign off.

10.9. Inherently Very High Relationships – detailed requirements

The section below deals with specific types of entities / relationships that are inherently very high or high risk from a Money Laundering and Terrorist Financing perspective and stipulates EDD requirements applicable to each:

10.9.1. Non-profit/Charity Organizations

Due to their inherent susceptibility to Money Laundering (ML), Terrorist Financing (TF), and Financing of Illegal Organizations (FIOs), Non-Profit/Charity Organizations (NPOs) are classified as very high-risk entities. In line with an effective risk-based approach to AML/CFT, IDB implements Enhanced Due Diligence (EDD) for all NPO relationships.

Enhanced Due Diligence (EDD) Requirements:

The Business Unit must obtain the following information for all NPOs:

- Legal, Regulatory, and Supervisory Status: Comprehensive information regarding the NPO's legal structure, regulatory framework, and supervisory oversight mechanisms.
- Ownership and Management: Detailed information about the NPO's ownership structure, including identification of ultimate beneficial owners (UBOs) and management team, with specific attention to the possibility of Politically Exposed Persons (PEPs) being involved.
- Activities and Programs: A clear understanding of the nature and scope of the NPO's activities and programs, including their intended beneficiaries and geographical areas of operation.
- Donor Base and Beneficiaries: In-depth analysis of the NPO's donor base and the beneficiaries of its activities and programs, including their risk profiles and potential vulnerabilities.
- Background Checks: Thorough background checks on key individuals associated with the NPO, such as senior management, major donors, and major beneficiaries, to identify potential matches with targeted and other international financial sanctions lists, criminal activity, or other adverse information.
- Geographic areas in which it operates, so as to be in apposition to identify, assess, and manage or mitigate the associated ML/TF risks.

Additional Requirements for NPO Accounts:

- Ministry of Community Development Letter: An original signed letter from the Ministry of Community Development is mandatory for opening accounts and collecting donations for NPOs.
- UAE Red Crescent Authorization: Prior to allowing financial transfers out of the UAE from NPO accounts, authorization from the UAE Red Crescent is required.
- CEO/Regional Manager Approval: Establishing any relationship with an NPO requires prior approval from the CEO or the Regional Manager.

10.9.2. Trust & Foundation Relationship

1. Formation and Administration:

The bank will only establish relationships with trusts and foundations formed and administered by a regulated corporate trustee/corporate service provider licensed to provide trust/foundation services in the UAE. This includes:

- Formation/creation of the trust or foundation: The bank will require evidence of proper formation and compliance with all relevant regulations.

- Administration of the trust or foundation: The bank will require evidence of ongoing administration by the licensed trustee, including record-keeping, accounting, and compliance with the trust/foundation's governing documents.

2. Identification and Verification of Underlying Parties:

The bank will identify and verify all underlying parties to the trust/foundation, as defined by the relevant UAE regulations. This includes, but is not limited to:

- Settlor: The person who creates the trust and transfers assets to it.
- Founder: The person who establishes the foundation and contributes assets to it.
- Guardian: A person appointed to care for the interests of a minor or incapacitated beneficiary.
- Protector: A person appointed to oversee the actions of the trustee and ensure compliance with the trust/foundation's governing documents.
- Trustees: The persons responsible for managing the trust/foundation's assets and carrying out its purposes.
- Beneficiaries: The persons who are entitled to benefit from the trust/foundation's assets.
- Ultimate Effective Control (UEC): Any natural person(s) who ultimately control the trust/foundation, directly or indirectly.

The bank will use commercially reasonable methods to verify the identity and source of wealth of all underlying parties, consistent with the risk profile of the trust/foundation and applicable regulations.

3. Source of Wealth Information:

The bank will obtain information regarding the source of wealth (SoW) for all assets settled into the trust, as well as the SoW for the settlor/founder. This information will be used to assess the risk of money laundering and terrorist financing associated with the trust/foundation.

4. Refusal to Disclose Information:

Any trust or foundation that refuses to disclose details of all underlying parties, including beneficiaries, settlor, protector, etc., will be treated as Unacceptable Relationship.

10.9.3. Correspondent Banking

In accordance with the Financial Action Task Force (FATF) recommendations, IDB adheres to a stringent framework for correspondent banking relationships. We recognize the inherent ML/TF risks associated with this activity due to the limited information available regarding the underlying transactions and potential anonymity of clients.

Prohibited Activities:

- Nesting: IDB prohibits nesting, where a respondent bank establishes a correspondent relationship with another bank solely to facilitate transactions for a third bank.
- Shell Banks: IDB prohibits relationships with shell banks, defined as entities lacking physical presence or legitimate business operations. Additionally, we reject institutions allowing their accounts to be used by or providing direct access to shell banks.
- Payable Through Accounts: IDB does not engage in “Payable Through Accounts,” where clients of a respondent bank directly access and utilize the correspondent account.
- Downstream Correspondent Relationships: IDB generally avoids downstream correspondent relationships, where a respondent bank acts as a conduit for other financial institutions. Exceptions are limited to legacy relationships pre-approved by Business Head and Compliance Head. In such cases, full transparency of all parties involved and upfront disclosure to the IDB correspondent are mandatory.

To address the ML/TF risk associated with correspondent banks, such relationship and on annual basis thereafter. Following due diligence measures must be applied and documented appropriately:

- Collect sufficient information about any receiving correspondent banking institution for the purpose of identifying and achieving a full understanding of the nature of its work, and to make available, through publicly available information, its reputation and level of control including whether it has been investigated by regulatory, judiciary or law enforcement authorities.
- Evaluate the AML/CFT controls applied by the receiving institution.
- Obtain approval from senior management before establishing new correspondent banking relationship.
- Take appropriate steps to assess the nature, size, and extent of their business in the countries where they are incorporated and licensed, as well as their ownership and management structures (talking into consideration the nature and extent of any PEP involvement) in order to evaluate whether they exhibit the characteristics of shell banks, and whether they offer downstream correspondent banking services (also known as "nested accounts") to other banks.
- Consider the country risk in the respondent's country.
- Assess the ML prevention and detection policies and procedures of the respondent bank, including a description of the CDD applied by the respondent bank to its clients and how it meets internationally recognized standards and sufficiently to mitigate the risk presented based upon their products, client base and jurisdiction.
- Clear understanding of the purpose of correspondent banking service provided to the respondent bank.

For information on the AML/CFT policies and procedures, bank may rely on the correspondent banking questionnaire (Wolfsberg Questionnaire) filled by the respondent bank and/or on publicly available information provided by the respondent (such as financial information or any mandatory supervisory information).

Correspondent Banking Universe

Scope		**On-boarding / Establishing Relationship**	**Post Fact Surveillance**
VOSTROs	Other banks accounts (respondent) held by IDB (correspondent) in AED currency. These accounts can be used for a wide range of services including cash management (e.g., interest-bearing accounts in variety of currencies), international wires transfers, check clearing and foreign exchange.	• Correspondent bank sends account opening request via SWIFT • Conduct EDD • Name Screening in WorldCheck and Public Media Search • Review of Wolfsberg Questionnaires • Business Group Head sign off • Compliance sign off	• On-going portfolio screening for updates to sanctions lists • Pre-fact SWIFT filtering in FIRCOSOFT • Alerts monitoring in AML monitoring solution • Periodic Reviews
OPERATING ACCOUNT	IDB Could maintain accounts for Branches/Subsidiary of a Foreign Bank (Generally DIFC based banks). Purpose of such accounts is to manage their operating expenses / (such as employees' salaries, daily business expenses, etc.) with source of funds being credits received from parent's account	• Conduct CDD • Business Head sign off	• On-going portfolio screening for updates to sanctions lists • Pre-fact SWIFT filtering in FIRCOSOFT • Alerts monitoring in AML monitoring solution
RMA Exchange	Relationship Management Application (RMA) is a service	Name Screening in WorldCheck and Public Media Search	Pre-fact SWIFT filtering in FIRCOSOFT

	provided by SWIFT to manage the business relationships between financial institutions. These messages are generally used to engage in Treasury and Trade related business i.e., essentially advising and confirming the transactions (No discounting involved)		

Nostro Due Diligence

1. Pre-Onboarding:
   - Wolfsberg Questionnaire: The Financial Institution (FI) Team will obtain and utilize the latest version of the Wolfsberg Correspondent Bank Due Diligence Questionnaire to assess the Correspondent Bank's AML/CFT controls. Any requests for clarification identified during the assessment will be raised with the Correspondent Bank.
   - Publicly Available Information: The FI Team will rely on the Wolfsberg Questionnaire and relevant publicly available information (e.g., financial information, supervisory reports) to further assess the robustness of the Correspondent Bank's AML/CFT controls. Any concerns identified during this assessment will be promptly escalated to the Compliance Team for guidance.
   - Bank Information Gathering: The FI Team will diligently collect and analyse information about the Correspondent Bank, including:
     - Nature and scope of its business operations
     - Reputation and level of regulatory control
     - Ownership and management structure
     - Presence of investigations or regulatory actions by authorities
     - Information related to Shell Bank characteristics
2. Onboarding and Ongoing Monitoring:
   - PEP and Sanctions Screening: The Compliance Team will conduct comprehensive PEP and sanctions screening on the Correspondent Bank's beneficial ownership/controlling structure and board of directors. Any matches identified will be analysed and appropriate actions taken as per established procedures.
   - Adverse Media Search: The FI and Compliance Teams may conduct additional adverse media searches on the Correspondent Bank to identify potential reputational or financial risks.
   - Periodic Review: The FI Team will periodically review the Nostro account relationship and update its due diligence documentation based on any changes in the Correspondent Bank's circumstances or risk profile.
3. Approval Process:
   - Senior Management Approval: Prior to establishing a new Nostro account, the FI Team must obtain approval from senior management. This decision will be informed by the Wolfsberg Questionnaire assessment, screening results, adverse media search findings, and any other relevant due diligence information.
   - Compliance Confirmation: The Compliance Team will provide confirmation on the Wolfsberg Questionnaire assessment, screening outcomes, and adverse media search findings (if conducted) before the Nostro account can be opened or maintained.
4. Escalation and Reporting:
   - Any concerns or potential ML/TF risks identified during the due diligence process must be promptly escalated to the Compliance Team for investigation and guidance.
   - The FI Team will regularly report on its Nostro due diligence activities to the Compliance Team and senior management.

10.9.4. Treasury Due Diligence Matrix

Treasury Due Diligence Matrix		
Transaction Type	**Counterparty Type**	**Due Diligence Type**
Money Market Deposits	Banks	1. Obtain signed Wolfsberg questionnaire from the counterparty. 2. Obtain list of directors and authorised signatories. 3. Screen names of directors, authorized signatories, and counterparties against worldcheck. 4. Perform internet research on the counterparties. 5. Obtain Compliance clearance.
	• Non-Banking Financial Institutions • Financial Brokers • Government and Semi Government Co • Other Corporate entities	Client Due Diligence
Name Screening in WorldCheck and Public Media Search	Pre-fact SWIFT filtering in FIRCOSOFT	
Derivative, Equities, Fixed Income, Foreign Exchange (for trading transactions without creation of CASA account)	• Banks • Central Banks • Non-Banking Financial Institutions • Financial Brokers • Government and Semi Government Co • Other Corporate entities	Simplified Due-Diligence
Derivative, Equities, Fixed Income, Foreign Exchange (for trading transactions with creation of CASA account)		Client Due Diligence

10.10. Money or Value Transfer Services

To mitigate the inherent money laundering and terrorist financing (ML/TF) risks associated with business relationships with money or value transfer services (MVTSs), such relationships shall be subject to Enhanced Due Diligence (EDD) prior to establishing a relationship and on an annual basis thereafter. The following due diligence measures must be implemented:

1. Verification of Licensing or Registration:

- Ensure the MVTS is duly licensed or registered with the relevant regulatory authority, specifically the Central Bank of the United Arab Emirates (CBUAE).
- Physically verify the original registration certificate issued by the CBUAE and maintain a certified copy for recordkeeping purposes.

2. Assessment of AML/CFT Policies and Procedures:

- Obtain detailed information about the MVTS's AML/CFT policies, procedures, and controls to assess their adequacy and effectiveness.
- Ensure compliance with all relevant provisions of the AML-CFT Decision, particularly those related to wire transfers. This includes, but is not limited to, customer identification and verification, transaction monitoring, and suspicious activity reporting.

3. Identification and Assessment of Agent-Related ML/TF Risks:

- Obtain a complete list of the MVTS's agents and identify any associated ML/TF risks, particularly in relation to:
  - High-risk countries: As designated by the Financial Action Task Force (FATF) or the CBUAE.
  - Other identified high-risk factors: Such as suspicious transactions, unusual customer profiles, or involvement in sanctioned jurisdictions or activities.

4. Comprehensive Customer Due Diligence (CDD) for MVTSs:

- Obtain sufficient information about the MVTS itself, including:
  - Ownership and management structure: Identify any Politically Exposed Persons (PEPs) involved or potential PEP involvement.
  - Nature and scope of business: Understand the types of services offered, target customer base, and geographic reach.
  - Customer base profile: Identify potential high-risk customers and assess associated ML/TF risks.
- Utilizing this information, identify, assess, and manage or mitigate all associated ML/TF risks effectively.

10.11. Money Dealers in Precious Metals and Stones (DPMS)

In addition to the standard CC procedures, the Bank shall implement a risk-based approach and conduct enhanced Due Diligence for customers identified as DPMS. This heightened scrutiny reflects the inherent risks associated with this sector, where the nature of business activities significantly influences the associated risk profile.

Specific Considerations for DPMS CDD:

1. Designated Non-Financial Business Profession (DNFBP) Status:

- Determine if the DPMS qualifies as a DNFBP: The Bank shall assess whether the customer falls under the definition of a DNFBP as per UAE regulations. This assessment should involve analyzing the customer's business activities and identifying any services that correspond to DNFBP activities.
- Registration with Ministry of Economy: If the customer qualifies as a DNFBP, the Bank must verify their registration with the UAE Ministry of Economy. This verification can be achieved through official documentation or confirmation from the relevant authorities.

2. DPMS-Specific Country Risk:

- Evaluate risk profile of countries where the DPMS operates: The Bank shall analyze the DPMS-specific risks associated with each country where the customer conducts business. This includes assessing the prevalence of illegal mining, smuggling of precious metals and stones, and other relevant risk factors specific to the DPMS sector in those countries.
- Utilize reliable sources: The Bank should rely on credible sources, such as international and national reports, financial intelligence analyses, and industry publications, to assess DPMS-specific country risks.

3. Products and Services Offered:

- Identify products and services attractive to illicit actors: The Bank shall identify the specific products and services offered by the DPMS that may be particularly attractive to individuals or organizations engaged in money laundering or other illicit activities.
- Enhanced scrutiny for high-risk products and services: For DPMS offering high-risk products and services, the Bank shall implement additional CDD measures, such as increased transaction monitoring, source of funds verification, and enhanced due diligence on counterparties involved in transactions.

By implementing these enhanced CDD procedures for DPMS, the Bank can effectively mitigate the risks associated with this sector and contribute to the UAE's efforts in combating money laundering and other financial crimes.

10.12. Cash Intensive Business (CIBs)

CIBs are businesses that generate a large volume of cash revenue and are inherently vulnerable to money laundering (ML), financing of terrorism (FT), and financing of illegal organizations (FIOs) due to the difficulty in tracing cash transactions. Illicit actors can exploit CIBs for ML and FT/FIOs by:

- Providing a front to launder large amounts of cash and reinvest proceeds of crime: CIBs can be used to disguise the origin and ownership of illicit funds by mixing them with legitimate business income.
- Co-mingling illicit and legitimate income: Illicit funds can be combined with legitimate business income, making it difficult to identify and track the source of funds.
- Financing terrorist activities: CIBs can be used to finance terrorist activities through small cash transactions, making them difficult to detect and trace.

CIBs operate across various industries, and while most are legitimate businesses, certain aspects of their operations can be vulnerable to ML, FT, and FIOs. To mitigate these risks, CIBs must undergo enhanced due diligence (EDD) before establishing a relationship and during periodic reviews.

Due Diligence Measures for CIBs:

- Risk-based identification: Banks must identify CIBs using a risk-based approach, considering factors like industry, cash-to-non-cash ratio, transaction patterns, and geographic location.
- Full EDD: Comprehensive EDD must be conducted on CIBs, including verification of beneficial ownership (UBO) for individuals holding 10% or more ownership.
- Understanding the business: Banks must thoroughly understand the nature of the CIB's business, including its purpose, products/services offered, primary business activity, and financial statements (audited if available). This may involve interviewing management, reviewing business licenses, and conducting online research.
- Misrepresentation: Banks should not onboard or terminate relationships with CIBs found to have misrepresented themselves or their business activities.
- High-risk classification: CIBs identified as such will be classified as high/increased risk and subjected to appropriate controls, including annual periodic reviews and ongoing transaction monitoring.

10.13. Virtual Asset Service Providers (VASP)

A Virtual Asset Service Provider (VASP) is any person, whether natural or legal, who conducts any or a combination of the following five activities as a business or on behalf of other individuals or companies, as defined by Cabinet Resolution No. (111) of 2022 Concerning the Regulation of Virtual Assets and their Service Providers:

- Exchange between virtual assets and fiat currencies: This includes buying and selling virtual assets for fiat currency, such as USD, EUR, or AED.
- Exchange between one or more forms of virtual assets: This includes converting one type of virtual asset to another, such as Bitcoin to Ethereum.
- Transfer of virtual assets: This includes transferring ownership or control of virtual assets to another user or transferring virtual assets between VA addresses or accounts held by the same user.
- Safekeeping or administration of virtual assets or instruments enabling control of virtual assets: This includes services such as custody of virtual assets, providing wallets or other tools to manage virtual assets, and issuing or managing virtual asset derivatives.
- Participation in and provision of financial services to insurers offer or sale of a virtual asset: This includes activities such as providing investment services, insurance, or lending services related to virtual assets.

For the purpose of this policy, virtual assets include cryptocurrencies, cryptocoins, payment tokens, exchange tokens, exchange tokens, convertible virtual currencies.

Virtual assets, in general, are considered a high-risk medium of exchange due to the following factors:

- Decentralization: Virtual assets are not controlled by any central authority, which can make it difficult to track and monitor transactions.
- Anonymity/pseudo-anonymity: While not completely anonymous, virtual asset transactions can be difficult to trace to the individuals/entities involved.
- Limited regulatory framework: There is currently no comprehensive global regulatory framework for virtual assets, which can create opportunities for illicit actors.
- Limited due diligence: Due to the anonymity and pseudonymous nature of virtual asset transactions, it can be difficult for VASPs to perform adequate customer due diligence (CDD) and know your customer (KYC) checks.

Given the heightened inherent money laundering (ML) and terrorist financing (TF) risks and vulnerabilities associated with VASPs, IDB will take the following steps to mitigate these risks:

- Prohibition on business relationships with VASPs: Establishing a business relationship or continuing a business relationship with VASPs is an "Unacceptable Risk" to IDB.
- Enhanced due diligence for customers with VASP activity: IDB will perform enhanced due diligence (EDD) on existing customers who engage in VASP activity, such as buying, selling, or investing in virtual assets. This may include requesting additional information from the customer, such as the source of funds used to purchase virtual assets, and the intended purpose of the virtual assets.
    - Existing non-VASP customers (natural persons or legal persons) who utilize their accounts for buying, selling, or investing in virtual assets that falls outside of their customer profile/business activity will be considered an "Unacceptable Risk" to the bank. IDB may take action to terminate the business relationship with such customers, including freezing or closing their accounts.
- Regular review of VASP risks: IDB will regularly review and update its risk assessment of VASPs and the virtual asset sector to ensure that its policies and procedures remain effective.

11. Ongoing Due Diligence

Continuous customer monitoring is a critical element of the Bank's financial crime framework. The Bank shall conduct ongoing due diligence throughout the life cycle of the customer relationship to ensure that customer KYC information, transactions, and accounts align with the Bank's understanding of the customer's business, risk profile, purpose of the relationship, and expected activity level.

Ongoing monitoring of customers comprises of the below key elements:

- CDD reviews: the bank shall ensure that the information and documentation concerning a customer's identity remains accurate and up-to-date and shall provide reasonable assurance that the bank is not being used for the furtherance of illegal activities. The bank shall ensure that the customers risk rating reflects the actual situation and that appropriate controls are applied by setting out requirements for CDD reviews on a periodic basis (periodic review), and where triggered by an event (trigger review).
- AML transaction monitoring, transaction screening and name screening: these are the controls in place detailed in Section 11 of the Policy to ensure the effective detections of transactions that are not in line with customer's profiles, which may potentially be suspicious.

The bank must perform two types of CDD reviews on a customer:

- Periodic reviews of the customer CDD; and
- Trigger reviews following the rise of specific events are defined in the section below.

11.1. Periodic Reviews

Periodic reviews should be carried out for all customers based on their risk rating, from the date of last reviews per the table below:

Periodic Review – Frequency and approval requirements					
Risk Classification	**Low/Neutral**	**Medium**	**Increased/High**	**UAE PEP**	**Very High Risk (FPEP, Exchange Houses, Correspondent Banks, NPO's/Charities)**
Frequency	Every 5 years	Every 4 years	Every 3 years	Every 2 years	Every year
Approval Requirements	RM's to complete the review	• RM (initiator) • Business Head (approver)	• RM (initiator) • Business Head (approver) • Compliance Approval	• RM (initiator) • Business Head (approver) • CEO/Regional Manager Approval • Compliance Approval	• RM (initiator) • Business Head (approver) • CEO/Regional Manager Approval • Compliance Approval

Additionally, Compliance will periodically conduct thematic reviews on selected categories based on evolving risks as noted.

From a broader risk management perspective, relevant business units are required to have appropriate review and tracking mechanisms to ensure that client information is updated and documented.

The steps required to be undertaken at such periodic CDD reviews are outlined below:

#	Review Requirements
1	Review CDD information and ensure it remains valid and accurate. Confirm any changes through independent and reliable sources or by contacting the customer.
2	If deficiencies are identified in the KYC information, obtain, and verify the valid documentation in line with the policy: • Identification and verification of the customer • Purpose of the business relationship • Ownership structure • Identification and verification of directors, signatories and UBO's • Business activity • SoF and/or SoW • PEP status • Sanctions status
3	Following a CDD information change, screening of any additional names of individuals or entities must be carried out.
4	Update expected account activity if required and request information where not consistent or where suspicious activity has been found.
5	Review adverse information findings if applicable.
6	Assess the appropriateness of the customer's current risk rating. In the event of a change in risk rating, additional requirements in terms of this Policy have to be met (e.g., obtain relevant approvals for increased risk rating).
7	For high and very high risk and PEP customers, business is required to review customer account activity during the periodic review process. Where deviation in customer transactional activity are identified, these cases should be referred to Compliance for review and advise.
8	Ensure that applicable systems contain up to date CDD information and supporting documentation has been stored appropriately including last KYC Review Date in Core System and documents uploaded in Archive System where applicable.

11.2. Trigger or event driven reviews

The Bank has implemented clear criteria to identify circumstances requiring an interim or event-driven review of customer due diligence (CDD) information, potentially accelerating the regular review cycle. These trigger events necessitate a reassessment of the customer's risk profile and CDD data before the next scheduled review.

Trigger Events:

- Changes in CDD information: This includes updates to identification documents, registration details, business activities, ownership structure, or Power of Attorney (POA) holders.
- Material CDD deficiencies identified: Inconsistencies or inaccuracies in previously gathered information.
- Discovery of contradictory information: Raising concerns about the customer's profile, risk classification, or CDD accuracy.
- Introduction of new products or services: Assessing compatibility with existing risk profile and CDD data.
- Reactivation of dormant or exit-listed relationships: Re-evaluating risk posture and CDD information.
- Potential Politically Exposed Person (PEP) links: Identifying potential risks associated with PEP relationships.
- Potential sanctions nexus: Assessing potential violation of sanctions regulations.
- Customer risk events: Any incident raising financial crime concerns, including:
    - Transaction monitoring alerts: High-risk transactions, significant cash deposits, payments to/from high-risk countries, or sanctions-related blocks.
    - Suspicious activity: Indications of potential money laundering or other suspicious behavior.
    - Potential circumvention attempts: Efforts to evade compliance controls or sanctions regulations.
    - Adverse media reports: Allegations or investigations of fraud, corruption, or other crimes involving the customer or related parties.
    - Authorities' information requests: Inquiries about the customer.
- Trigger review requests: Justified requests by any team member for reassessment of the customer.
- Qualified auditor opinion: Concerns raised by an independent auditor on the customer's financial statements.

Review Types:

- Full CDD Review: Conducted when the trigger event increases the customer's risk rating. This involves a complete re-evaluation of all CDD elements, adhering to the standards of the revised risk rating.
- Targeted Trigger Review: Conducted when the trigger event requires updating specific information related to the event, without impacting the overall risk rating. This focuses on addressing the identified issue while maintaining the existing risk classification.

Post-review Actions:

- Full CDD Trigger Review:
    - The customer's next review date is adjusted to reflect the revised risk rating and periodic review cycle.
    - Enhanced monitoring may be implemented based on the increased risk profile.
- Targeted Trigger Review:
    - The customer's next review date remains unchanged unless further risk concerns emerge.
    - The updated information is incorporated into the existing CDD file.

11.3. Termination of a client relationship – De-risking

Authority to Terminate:

IDB Compliance, in accordance with its risk-based approach, may initiate the termination of an existing client relationship due to:

- Unacceptable Risk Factors: Identified through ongoing monitoring of client profiles and transactions, in compliance with existing IDB policies and UAE regulations.
- De-risking Measures: Implemented to address broader risks identified within the financial system or specific industry sectors.

Communication and Transparency:

- Internal Communication: Instructions for termination will be provided internally through secure channels, outlining specific steps to follow. These communications are confidential and not to be shared with clients.
- Client Communication: IDB will not disclose the specific reasons behind a relationship termination to the client, whether voluntarily or otherwise.

Grounds for Termination or Non-Establishment of Relationships:

IDB reserves the right to terminate an existing relationship or decline to establish a new one based on the following:

- Confirmed Sanctions Nexus: Any indication of the client or their associates being listed on international or domestic sanctions lists.
- Material Adverse News: Significant negative information about the client that raises concerns about their integrity, financial stability, or compliance with regulations.
- Risk Misalignment: When a client's risk profile exceeds IDB's established risk appetite or poses an unacceptable risk despite mitigation measures.
- Documentation Discrepancies: Incomplete or inaccurate information provided by the client during onboarding or KYC/AML procedures.
- Veracity Concerns: Doubts regarding the authenticity or completeness of information provided by the client.

11.4. Internal Watch List Management

- Periodic Review and Update: The Compliance Department shall regularly update the internal watch list by incorporating names identified as suspicious or unacceptable during various reviews conducted by the bank. This includes, but is not limited to, customer due diligence (CDD), transaction monitoring, and sanctions screening.
- Scope of Inclusion: The internal watch list shall primarily serve two purposes:
  - Restricting Relationship Establishment/Deepening: Individuals or entities on the list may be subject to limitations on establishing new relationships with the bank or deepening existing ones. This may involve additional CDD requirements, enhanced transaction monitoring, or outright refusal to establish or deepen the relationship.
  - Transaction Handling Restrictions: Transactions involving individuals or entities on the list may be subject to restrictions or require specific approval from the Compliance Department before being processed. This ensures heightened scrutiny and potential mitigation of risks associated with these individuals or entities.
- Match Reporting and Clearance:
  - The Business and Operations Teams are responsible for promptly notifying the Compliance Department of any transaction matches identified against names on the internal watch list.
  - No transactions involving individuals or entities on the internal watch list shall be processed without prior written clearance from the Compliance Department.
  - The Compliance Department will assess the reported matches and determine the appropriate course of action, which may include additional investigation, seeking clarification from the customer, or blocking the transaction.

12. AML/CFT Transaction Monitoring

Effective AML/CFT Transaction Monitoring

To effectively combat money laundering and terrorist financing (ML/TF) risks, IDB maintains a robust Anti-Money Laundering (AML) program with a comprehensive transaction monitoring system. This system is designed to identify, review, and investigate, where necessary, transactions deemed "unusual" or potentially suspicious.

Automated Monitoring and Scenario-Based Detection:

IDB employs a sophisticated Suspicious Activity Monitoring (SAR) software solution as the core of its transaction monitoring process. This system utilizes a set of predefined detection scenarios and customizable risk factors, configured based on client portfolio segmentation and the Bank's risk appetite. Each scenario targets specific patterns of activity or risk typologies associated with ML and TF. These scenarios are reviewed and fine-tuned every 12-18 months to ensure their effectiveness and alignment with evolving risks.

Alert Review and Investigation:

The Compliance department oversees the monitoring system and is responsible for reviewing and investigating all generated alerts. A dedicated Compliance Officer assesses each alert, differentiating genuine suspicious activity from false positives. This investigation is conducted with due diligence, timeliness, and confidentiality, ultimately leading to a decision on filing Suspicious Transaction Reports (STRs) with the relevant authorities.

Beyond Automation: Additional Monitoring Sources:

Recognizing the limitations of solely automated systems, IDB utilizes a multi-layered approach to transaction monitoring. This includes:

- Employee Referrals: Customer-facing employees are encouraged to report any potential suspicious activity to the Compliance department for further investigation.
- Adverse Media Monitoring: IDB actively monitors media reports for any information regarding its clients or their activities that could raise suspicion.
- Central Bank of UAE ECDD Requests: IDB collaborates with the Central Bank of UAE by responding to Enhanced Customer Due Diligence (EDCD) requests and promptly reporting any identified suspicious activity.
- Correspondent Bank Referrals: IDB maintains open communication with its correspondent banks, proactively sharing relevant information and promptly addressing any suspicious activity referrals.
- Law Enforcement Requests: IDB cooperates fully with law enforcement authorities in their investigations of suspected financial crimes, providing necessary information and assistance.

By implementing a multi-pronged approach to transaction monitoring, IDB effectively mitigates ML/TF risks and ensures compliance with UAE regulations and international best practices.

12.1. Third Party Account Usage

Usage of IDB account by any person/entity other that the actual account holder or mandate holder/POA, and carrying transactions on behalf of another person, not identified and verified as UBO is prohibited. Any such violation may result in the termination of the relevant client relationship. Such cases should be escalated immediately to the respective branch/business manager and Compliance for taking final decision regarding the relationship.

12.1.1. Cash Dealing

A. General Cash Transactions:

- Prohibition for Non-Customers: All cash transactions, including currency exchange and traveler cheque services, are strictly prohibited for non-customers through branches, ATMs/CDMs, or any other channel.
- Customer Accounts Mandatory: Currency exchange for customers must be conducted exclusively through their designated IDB accounts.
- Source of Funds (SoF) Inquiry:
    - SoF must be consistently inquired and documented on the deposit slip for:
        - Cash deposits exceeding AED 200,000.
        - Cash deposits exceeding AED 1 million, with additional approval required from the relevant business unit or branch manager (if no assigned relationship manager).
    - SoF may be requested for any deposit amount deemed suspicious or inconsistent with customer profile or activity.
- Purpose of Withdrawal: The purpose of cash withdrawals exceeding AED 500,000 must be verified and recorded on the withdrawal slip.
- Multiple Cash Transactions:
    - Branches must monitor accounts for potential structuring activity, defined as multiple over-the-counter cash deposits or withdrawals exceeding the specified thresholds within a single day.
    - SoF or relevant documentation must be obtained for all identified instances of structuring.
- Third-Party Deposits:
    - For cash deposits made by individuals not listed on the account, their name, contact information, and a copy of their identification document must be collected and documented. Evidence of their relationship to the account holder is also required.

B. ATM/CDM Transactions:

- Thresholds and Parameters: Cash deposit and withdrawal thresholds and parameters for ATMs/CDMs must be set and approved by Compliance. Any modifications require pre-approval from Compliance.
- Non-IDB Customer Deposits: In the event of cash deposits by non-IDB customers through ATMs/CDMs, the depositor's name and Emirates ID number must be captured at a minimum.

C. Cash Pick-Up and Delivery:

- Eligibility and Due Diligence:
    - Cash pick-up services will be available only to entities deemed typically cash-intensive businesses, following satisfactory Enhanced Due Diligence (EDD) conducted by the business unit and approved by Compliance.
    - Non-cash-intensive businesses requesting cash pick-up or delivery must provide justifiable reasons, which will be validated and rationalized before approval. Such requests require approval by the respective business unit head and follow the same due diligence procedures as over-the-counter cash deposits.
- Relationship Manager Responsibility: The assigned Relationship Manager is responsible for ensuring:
    - Justification of cash pick-up/delivery transactions.

- Collection of appropriate documentary evidence from the client, as applicable.

- AML Monitoring: All cash transactions, including pick-up and delivery, are subject to ongoing AML monitoring.

12.1.2. Inward / Outward Remittance Details

In accordance with Central Bank of the UAE regulations and international compliance standards, IDB requires complete transaction details for all inward and outward remittances. This information is essential for effective Know Your Customer (KYC) and Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) due diligence.

Mandatory information:

- Ordering Client: Full name and bank details (including branch)
- Beneficiary Client: Full name and bank details (including branch)
- Client Addresses: Both ordering and beneficiary client addresses must be physical addresses (P.O. Boxes are not acceptable).
- Payment Details: If provided by the client, all relevant details must be included (amount, currency, purpose, etc.)
- Purpose of Payment: Clear and unambiguous description of the underlying transaction.

Incomplete Requests: Requests missing any of the above mandatory information will not be processed.

Customer Instructions: IDB adheres to a strict policy of processing customer instructions "as received." No amendments or alterations are permitted to the transaction details once submitted. Any changes, additions, or deletions require fresh instructions from the client.

Walk-in Clients and Occasional Transactions: As per policy, IDB does not accept inward or outward remittance instructions from walk-in clients (non-IDB account holders) or engage in occasional transactions for non-account holders.

12.1.3. Trade Finance Transactions

Trade-Based Money Laundering (TBML) Risk Management in Trade Finance

International Development Bank (IDB) recognizes the inherent risk of trade finance transactions being used by criminals to launder illicit proceeds. TBML exploits the complexity and opaqueness of international trade to disguise the origin and destination of funds. This often involves manipulating trade documentation, such as misclassification of goods, over/under-invoicing, and carousel transactions.

Red Flags Indicating Potential TBML:

- Payments by unrelated third parties: Unconventional payment structures, particularly those involving third-party intermediaries with no apparent connection to the trade transaction, warrant scrutiny.
- Misrepresentation of goods: Discrepancies between the nature of the goods traded and the client's business profile, commodity misclassification, and significant over/under-valuation of goods raise red flags.

- Unusual trade patterns: Repeated imports/exports of the same high-value goods (carousel transactions), frequent changes in shipping routes or transshipment points, and trade with jurisdictions with known ML/CFT risks require enhanced due diligence.
- Inconsistencies in documentation: Inconsistencies between trade documents and physical goods, double invoicing, and packaging incompatible with the declared commodity or shipping method should trigger suspicion.

Mitigating TBML Risk:

- Enhanced Due Diligence (EDD): IDB will conduct thorough due diligence on all trade finance clients, focusing on verifying their business profile, line of business, and the nature of goods and jurisdictions involved in the transaction. This includes verifying the legitimacy of invoices and trade documents, confirming the goods are not dual-use items, and ensuring no sanctions elements are involved.
- KYC Refreshment: Valid and updated KYC information is crucial for understanding the client's business and identifying potential anomalies. IDB will maintain a robust KYC program with regular refresh cycles, ensuring KYC information remains accurate and relevant.
- Trade Finance Operations: Trade Finance Operations personnel will receive thorough training on identifying and reporting suspicious activity. They will be responsible for scrutinizing all trade documents and raising red flags with the business and compliance teams if any discrepancies or inconsistencies are identified.

Sanctions Risk Management:

In addition to ML risks, trade finance transactions are also susceptible to sanctions risk. IDB will implement a comprehensive sanctions screening process covering individuals, entities, jurisdictions, vessels, ports, and goods involved in all trade transactions. This ensures compliance with applicable sanctions regulations and mitigates the risk of facilitating prohibited transactions.

13. Suspicious Transaction Reporting

13.1. Suspicious Activity Review, Investigation, and Reporting Timelines

This section outlines the internal timelines for reviewing, investigating, and reporting suspicious activities identified within IDB. It applies to all alerts generated through our monitoring systems or identified by staff.

Action	Maximum Timeline in Business Days
Dispositioning of alert, recommendation on whether to file an STR or SAR and decision on whether to file an STR or SAR	Within 35 days of alert generation
Filing of first STR or SAR for a complex investigation	Within 15 days of alert generation
Filing a follow up STR or SAR for a complex investigation	30 days from first STR or SAR filing (45 days from alert generation)
Filing of STR or SAR on continuing activity	Upon filing, we are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against said account holder, IDB will expedite file an STR or SAR with FIU

Circumstances Triggering Expedited Review:

- Immediate Attention Required:

- Ongoing reportable violations (e.g., money laundering scheme) as indicated by law enforcement.
- Suspected transactions related to terrorism or illegal organizations.

- Sufficient Evidence for Reporting:
  - Facts available at the alert review stage warrant immediate STR/SAR filing without further investigation.

The follow table summarizes the recommended suspicious activity review, investigation, and reporting timelines in the event of escalation for expedited review:

Action	**Maximum Timeline in Business Days**
Decision on whether to file an STR or SAR and filing of first STR or SAR	24 hours from decision to file
Filing of STR or SAR on continuing activity	Upon filing, we are expected to implement enhanced monitoring on such account holders. In the case of continued suspicious activity detected against said account holder, IDB will expedite file an STR or SAR with FIU

13.2. Internal Suspicious Transaction – Reporting Obligation

Any staff that are suspicious of a certain transaction or series of transactions is obligated to report without delay the suspicious transaction(s) to the Head of Compliance/MLRO via Compliance/AML Team email: AML@idbdubai.ae.

There is no minimum threshold or monetary value for reporting. The staff should include as much details as possible on the nature of transaction, the entities under concern and the nature of suspicion. Compliance will review ISTR and advise if any action is required by the reporting unit or Compliance will proceed with the actions as per AML SOP. The staff in all situations should ensure that the client not been informed nor made aware of the ISTR raised.

All staff members of IDB are obligated to report any suspicion of a transaction or series of transactions that may be related to money laundering or financing of terrorism (ML/FT) activities. This obligation exists regardless of the amount or value of the transaction(s) involved.

Reporting Procedure:

- Immediate Reporting: Suspicious transactions must be reported without delay to the Head of Compliance/MLRO via the dedicated Compliance/AML Team email address: AML@idbdubai.ae.
- Information Requirements: The report should include as much detail as possible, including:
  - Nature of the Transaction(s): Briefly describe the transaction(s) and any unusual features that raise suspicion.
  - Entities Involved: Identify the customers, account numbers, and any other relevant parties involved in the transaction(s).
  - Basis of Suspicion: Explain the specific reasons why you suspect the transaction(s) may be related to ML/FT activity.

Review and Action:

- The Compliance/AML Team will review the reported suspicious transaction(s) and determine the appropriate course of action. This may include:
  - Investigating the transaction further: This may involve requesting additional information.
  - Filing a Suspicious Activity/Transaction Report (SAR/STR) with the Central Bank of the UAE: This is a mandatory requirement for all financial institutions in the UAE if there is a reasonable suspicion of ML/FT activity.
  - Taking other appropriate action: This may include terminating relationships.

Confidentiality:

- Client Confidentiality: The staff member reporting the suspicious transaction must not inform the customer about the report or the suspicion of ML/FT activity. This is to preserve the integrity of any potential investigation and to avoid alerting the customer.
- Internal Confidentiality: The information reported in the suspicious transaction report should be treated with the utmost confidentiality and only shared with authorized individuals on a need-to-know basis.

13.3. External Suspicious Transaction Reporting

- Review and Decision-Making: The Head of Compliance/MLRO, regardless of the source, will review all proposed SARs/STRs. Based on the review, they will determine whether an external filing to the Financial Intelligence Unit (FIU) at the Central Bank through GoAML is warranted.
- Mandatory Reporting: If an external filing is deemed necessary, IDB shall report the case to FIU without delay.
- Client Classification and Monitoring: Clients reported to FIU will be classified as Very High Risk (unless already classified as Very High Risk) and subjected to enhanced monitoring.
- FIU Instructions and Relationship Management: IDB shall comply promptly with all instructions received from FIU in relation to the filed suspicion. In the absence of specific FIU instructions, IDB shall make an internal decision regarding the continued relationship with the client.
- Risk-Based Relationship Termination: IDB may determine, based on the suspicious activity, that the customer risk exceeds its risk appetite. In such cases, IDB may choose to exit the relationship without delay.

13.4. Protection for Reporting Persons

- **Legal Protection:**

The bank, its board members, employees, and authorized representatives are protected from any administrative, civil, or criminal liability arising from their good-faith reporting of suspicious activity to the Financial Intelligence Unit (FIU) under the relevant provisions of the UAE's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Law and Decision. This protection applies even if:

  - The precise nature of the underlying criminal activity was not known at the time of reporting.
  - Subsequent investigations fail to uncover illegal activity.

- **Scope of Protection:**

This protection extends to all legitimate reports filed in accordance with the bank's AML/CFT policies and procedures, including:

  - Suspicious Transaction Reports (STRs)
  - Suspicious Activity Reports (SARs)
  - Any other report types mandated by the FIU or relevant AML/CFT regulations.

- **Limitation of Protection:**

The protection for reporting persons does not cover:

  - Unlawful Disclosure: Disclosing, directly or indirectly, to the customer, any third party, or the public that a suspicious transaction report has been or may be filed. This includes revealing any information or data contained within the report or the existence of an ongoing investigation.
  - Malicious Intent: Reporting activities with malicious intent, personal gain, or any purpose unrelated to legitimate AML/CFT compliance.

13.5. Confidentiality and Tipping Off

IDB is committed to maintaining the strictest confidentiality regarding both the information reported in suspicious activity reports (SARs) and the act of filing these reports itself. We implement comprehensive data security measures

to safeguard the information and data reported from unauthorized access. This includes restricting access based on a "need-to-know" basis, implementing robust technical controls, and employing strict data handling protocols.

Under no circumstances shall IDB or any of its staff notify or warn a client who is the subject of an SAR or a suspicious transaction report to the relevant authorities. Disclosing such information could jeopardize ongoing investigations and hinder law enforcement efforts.

In accordance with UAE regulations, it is a federal crime for IDB, its management, employees, representatives, or any other person to directly or indirectly:

- Inform a client that a SAR has been filed or will be filed.
- Disclose any information or data contained in an SAR.
- Reveal that an investigation is underway concerning a transaction.

Client communication regarding suspicious activity is strictly limited. IDB shall not contact the customer directly or indirectly to inform them of actions taken, unless specifically authorized by the Central Bank (FIU) in writing. Clients under suspicion will be treated in the ordinary course of business unless otherwise advised by the authorities. The AML-CFT Law (20) of 2018 provides for imprisonment for no less than six months and a penalty of no less than AED 100,000 and no more AED 500,000 or any of these two sanctions shall apply to anyone who notifies or warns a person or reveals any transaction under review in relation to suspicious transactions or being investigated.

13.6. Failure to Report Suspicion

IDB is committed to upholding the highest standards of anti-money laundering (AML) and combating the financing of terrorism (CFT) compliance. This includes a mandatory obligation for all employees to report any suspicion of suspicious activity without delay.

Failure to comply with this obligation by intentionally or through gross negligence in reporting a suspicious transaction (STR, SAR, or other relevant report types) constitutes a federal crime in the United Arab Emirates (UAE) under the AML-CFT Law (20) 2018.

The AML-CFT Law (20) 2018 outlines potential sanctions for financial institutions, their managers, and employees who fail to report suspicions of money laundering (ML), terrorist financing (TF), or financing illegal organizations (FIOs):

- Imprisonment and fine of no less than AED 100,000 and no more than AED 1,000,000; or any of these two sanctions according to Article 240 of the AML-CFT Law.

IDB takes this obligation seriously and provides comprehensive training and resources to all employees to ensure they understand their reporting responsibilities. We also maintain a robust internal reporting system to facilitate the timely and accurate reporting of suspicious activity.

14. Training

Mandatory Training:

- Frequency: All staff, regardless of role or seniority, must undergo mandatory AML/CFT training at least once every 24 months.
- Content: Training covers key AML/CFT topics including:
  - AML/CFT fundamentals: definitions, risks, typologies, and red flags
  - Customer due diligence (CDD) and enhanced due diligence (EDD): procedures and best practices
  - Suspicious activity reporting (SAR): identification, reporting obligations, and escalation procedures
  - Know your customer (KYC) program: objectives, risk-based approach, and ongoing customer monitoring
  - Sanctions compliance: obligations under UAE and international sanctions regimes

Role-Specific Training:

- Tailored Training: Building upon the mandatory foundation, IDB provides role-specific training relevant to the ML/FT risks faced by different business lines and functions. This ensures staff understand the specific risks and controls applicable to their work. Examples include TBML for retail banking and correspondent banking for treasury operations and financial institution department.
- Compliance Assurance: The bank's Compliance Assurance function actively assesses training needs based on risk assessments, internal audits, and regulatory updates. This ensures ongoing training effectiveness and relevance.
- Regulatory Updates: IDB promptly delivers supplementary training to relevant staff whenever new regulations or guidance are issued by the CBUAE or other relevant authorities.

Training Delivery and Records:

- Delivery Methods: IDB utilizes a blend of classroom and online training formats to cater to diverse learning preferences and maximize accessibility.
- Resources: Training content is developed and delivered by both internal experts and external specialists, ensuring high-quality and up-to-date knowledge transfer.
- Record Keeping: Both the HR department and Compliance department maintain comprehensive training records, including staff name, ID, business unit, date, location, and content of each training session. This ensures compliance with CBUAE record-keeping requirements.

Continuous Improvement:

IDB is committed to continuous improvement in its AML/CFT training program. This includes:

- Regular evaluation of training effectiveness through feedback mechanisms and assessments
- Updating training content to reflect evolving risks and regulatory changes
- Providing ongoing opportunities for staff to deepen their AML/CFT knowledge and skills

15. Record Keeping

IDB is committed to maintaining detailed and retrievable records of all financial transactions, customer due diligence (CDD) information, and risk assessment/mitigation measures related to Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) activities. These records must be readily accessible for authorized personnel and regulatory authorities upon request.

Statutory Retention Period:

The minimum statutory retention period for all records is five (5) years, calculated from the date of:

- Account closure or termination of a business relationship.
- Completion of a casual transaction (no established business relationship).
- Conclusion of a Supervisory Authority inspection.
- Issuance of a final judicial judgment.
- Legal entity dissolution, liquidation, or termination.

Record-Keeping Policies and Procedures:

To fulfill its record-keeping obligations, IDB has implemented comprehensive policies and procedures commensurate with its size and business nature. These policies address:

- Organizational Roles and Responsibilities: Clearly defining roles and responsibilities for:
  - AML/CFT risk assessment and business continuity planning.
  - Implementation, review, and update of AML/CFT policies, procedures, and controls related to record-keeping and data protection.
  - CDD information and transaction record-keeping (logging, cataloguing, archiving, handling, transfer, and destruction).

- Physical and Cyber Security: Implementing robust security measures to protect active and archived data and records from unauthorized access, including:
  - Access control protocols.
  - Data encryption.
  - Regular security audits and penetration testing.

- Audit and Quality Assurance: Establishing appropriate audit and quality assurance testing policies to ensure record-keeping compliance and data integrity.

Record Categories:

IDB maintains various types of records, categorized broadly as:

- Financial Transaction Records: Operational and statistical records of all domestic and international financial transactions executed or processed by the bank.
- CDD Records: Records related to customer information, due diligence activities, and ongoing monitoring of business relationships. This category includes:
  - Customer identification and verification documents.
  - Company information and documentation.
  - Risk assessments and profiles.
  - Third-party CDD reliance documentation (if applicable).
  - Suspicious Transaction Reports (STRs).

Record Maintenance and Responsibility:

Respective business units, back office, and operations teams are responsible for maintaining all relevant financial transaction and CDD records in line with established record-keeping procedures.

Safeguarding Physical Records:

Records may be stored in physical or electronic formats. Regardless of format, the minimum five-year retention period applies. Safeguards must be implemented to ensure:

- Record integrity: Preventing tampering, alteration, or destruction of records.
- Accessibility: Maintaining easy access for authorized personnel.
- Security: Protecting records from environmental damage and unauthorized access.

16. Vendor Due Diligence

The bank must not establish a business relationship until the identity of the potential business partner has been established. As part of the procurement due diligence process and prior to on boarding a vender or supplier, appropriate due diligence and name screening must be conducted as per the requirements set out in this policy.

At a minimum, the bank must ensure that:

- The legal or natural person conducting business with the bank is identified and properly verified.
- The following are the minimum requirements prior to the on-boarding of vendors:
  - Identification and verification of the vendor and its beneficial owners / controllers.
  - Obtain the trade license/commercial registration (CR) copy (if overseas, the CR must be officially certified by the relevant embassy and ministry of foreign affairs).
  - Obtain the ID/passport copy of the authorized signatory (I.e., person signing the contract and whose name is in the CR).
  - Conduct name screening of the vendor and beneficial owner/controller as applicable.
- Records must be retained to provide an audit trail and adequate evidence to the law enforcement agencies in their investigations.
- All vendor relationships are reviews on a regular basis and are subject to ongoing name screening.

17. Exceptions

- Compliance Ownership: The Compliance department holds full ownership and accountability for this AML/KYC/CFT policy and its associated procedures.
- Exceptions: Any deviation from this policy must be documented and formally approved in writing by the Head of Compliance or their designated delegate. Such exceptions should be granted only under limited and exceptional circumstances, and only when demonstrably necessary for the bank's legitimate business interests, while maintaining compliance with relevant UAE regulations and the Financial Action Task Force (FATF) Recommendations.
- Extraordinary Circumstances: If extraordinary circumstances (e.g., lockdown, natural disaster) hinder the practical implementation of mandatory policy elements (e.g., site visits, in-person meetings), the Compliance department must promptly inform the Head of Compliance. The Head of Compliance, in consultation with relevant stakeholders, will then determine an acceptable alternative arrangement and a suitable timeframe for compliance, ensuring alignment with UAE regulations and FATF standards. This temporary arrangement must be documented and reviewed periodically until the extraordinary circumstances cease

18. Appendixes

Appendix 1- UAE Regulations and Guidelines

Regulations:

- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations.
- Federal Decree-Law No. (26) of 2021 Amending Certain Provisions of Federal Decree Law No. (20) For 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing of Illegal Organizations.
- 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 Organizations.
- Cabinet Decision No (74) of 2020 regarding Terrorism Lists Regulation and Implementation of UNSC Resolutions.
- Ministry of Finance Decision No. 228 Bank Accounts for Ministries.
- Ministry of Finance Decision No. 146 Bank Accounts for Ministries.
- Cabinet Resolution No. (58) of 2020 on the Regulation of the Procedures of the Real Beneficiary (UBO Resolution).

- Cabinet Resolution No. (24) of 2022 on Combating Money Laundering and the Financing of Terrorism and Illegal Organizations.

Guidance and Notices:

- Guidance Dates June 2021 for Licensed Financial Institutions Providing Services To The Real Estate And Precious Metals And Stones Sector.
- Guidance Dates June 2021 on Anti-Money Laundering and Combatting The Financing Of Terrorism And Illegal Organizations.
- Guidance Dated June 2021 for Licensed Financial Institutions Providing Services To Legal Persons And Arrangements.
- Guidance Dated December 2021 on Targeted Financial Sanctions and Typologies.
- Guidance Dated 2021 For Licensed Financial Institutions Providing Services to Cash Intensive Businesses.
- Interpretative Note Dated May 2022 on Assessing Jurisdictional Risk and The Consequential Application Of AML/CFT Obligations in Light of The UAE Being Among the Jurisdictions Under Increased Monitoring by the FATF.
- Guidance Dated May 2022 On AML/CFT Minimum Standards and Supervisory Expectations.
- Guidance Dated August 2022 for Licensed Financial Institutions on The Risk Relating to Payments.
- Guidance Dated August 2022 for Licensed Financial Institutions on The Risks Relating to Politically Exposed Persons.
- Guidance Dated November 2022 for LFIs On Digital Identification for Customer Due Diligence.

Appendix 2- Recordkeeping: Examples of the Types of Records to be Retained

Examples of Records (not Limited to)
Financial Transactions Records
• Customer credit or debit advice, and transaction orders or applications (including those for cash deposits or withdrawals, currency exchange transactions). • Credit-related documentation, including loan or guarantee applications, agreements, amendments and supporting documents, disbursement or repayment records, collateral pledges, letter of credit documentation, promissory notes. • Deal tickets, trade blotters and ledgers, settlements and dividend payment records related to foreign exchange, securities dealing or investing transactions. • Escrow or fiduciary account transaction records. • Insurance policy premiums, pay-outs, and related transaction records and documents. • Money transfer records, including book transfers orders, and domestic and cross-boarder wire transfer orders, and their related originator and beneficiary records. • Statistics and analytical data related to customers' financial transactions, including their monetary values, volumes, currencies, interest rates and other information.
CDD records
• Customer account information and files. • Customer correspondence. • Copies of personal identification documents, CDD forms, profiles and supporting documentation, and results of due diligence background searches, queries, and investigations. • Customer risk assessment and classification records. • Company formation, registration, deregistration, liquidation, dissolution, or expiry, including documents such as share registers, MOA, deeds of settlement and foundation charters, or similar documents, along with any amendments to them. • Change to company information such as name, registered address, legal representatives, and corporate officers or legal form. • Identification and identity verification documents related to beneficial owners, shareholders, nominee

shareholders, directors, and senior management officers and, in the case of legal arrangements, settlors or founders, protectors, beneficiaries, trustees or executers, governing council or committee members or similar controlling persons.
- Transaction review, analysis, and investigation files, with their related correspondence.
- Customer correspondence and relevant CDD records.
- Transaction handling decision, including approval or rejection records, together with analysis and correspondence.
- Suspicious transaction indicator alert records, logs, investigations, recommendations and decision records, and all related correspondence.
- Competent authority request for information, correspondent bank request for assistance, and their related investigation files and correspondence.
- CDD and business relationship monitoring records, documents and information obtained as part of analyzing and investigation of suspicious transactions and related communications and correspondence.
- STRs (internal and external), logs, and statistics, together with their related analysis, recommendations and decision records, and all related correspondence.
- Notes concerning feedback provided by the FIU with respect to reported STR's, as well as notes or records pertaining to any other actions taken by, or required by the FIU.

Appendix 3- Money Laundering and Terrorist Financing Description

What is Money Laundering:

Money laundering is the illegal process of disguising the origin of money obtained from criminal activities and making it appear legitimate. It's essentially washing "dirty" money into "clean" money. This allows criminals to use the funds without fear of detection or legal consequences.

What it involves:

- Hiding the source: Criminals try to obscure the origin of their ill-gotten gains, usually from activities like drug trafficking, corruption, tax evasion, or terrorism.
- Conversion: They then move the money through a series of financial transactions designed to make it appear legitimate. This can involve things like:
    - Smurfing: breaking down large sums into smaller amounts and depositing them in different accounts.
    - Structuring: just below the reporting threshold for banks.
    - Shell companies: using fake businesses to disguise the source of funds.
    - Layering: moving money through complex financial networks to obscure its origin.
    - Integration: finally placing the money back into the legitimate economy through investments, purchases, etc.

Why it matters:

- Undermines financial stability: Money laundering fuels criminal activities and weakens the financial system.
- Funds other crimes: The laundered money is often used to fund further criminal activity, perpetuating a cycle of crime.
- Erodes trust: It undermines trust in financial institutions and the rule of law.

Combatting money laundering:

- International cooperation: Governments around the world work together to share information and track illegal funds.
- Anti-money laundering (AML) regulations: Financial institutions have to implement certain procedures to detect and report suspicious activity.

- Public awareness: Educating the public about money laundering helps prevent people from unwittingly becoming involved.

The standard methodology employed in laundering money involves three stages:

The standard methodology employed in laundering money typically involves three stages: placement, layering, and integration. These stages work together to disguise the illicit origin of funds and make them appear legitimate.

1. Placement:

- This is the initial stage where criminals physically introduce their dirty money into the financial system. This can be done through various methods, such as:
    - Depositing cash in small amounts at multiple banks to avoid suspicion (smurfing)
    - Structuring cash transactions to stay below reporting thresholds
    - Using shell companies or fake businesses to disguise the source of funds
    - Purchasing high-value goods, such as cars or jewelry, with cash

2. Layering:

- Once the funds are in the financial system, the criminals will then layer them through a complex series of transactions to obscure their origin and make them difficult to track. This can involve:
    - Transferring money between multiple accounts, both domestic and international
    - Using wire transfers, foreign exchange transactions, and other financial instruments
    - Investing in assets, such as stocks, bonds, or real estate

3. Integration:

- Finally, the criminals will integrate the laundered funds back into the legitimate economy, making them appear as legitimate income. This can be done through:
    - Investing in businesses or real estate
    - Making large purchases with cash
    - Funding personal expenses

As per Article 2 Federal Decree-law No. (20) of 2018; Money Laundering defined as:

As per Article 2 of Federal Decree-law No. (20) of 2018 of the United Arab Emirates ("Decree-Law 20/2018"), money laundering is defined as any of the following acts:

a) Transferring or converting proceeds or conducting any transaction with the aim of concealing or disguising their illegal source: This covers a wide range of activities, including:

- Smurfing: Breaking down large sums of cash into smaller amounts and depositing them in different accounts to avoid suspicion.
- Structuring: Dividing transactions into amounts just below the reporting threshold for banks.
- Using shell companies: Creating fake businesses to disguise the ownership and source of funds.
- Layering: Moving money through a complex web of transactions to make it difficult to track its origin.

b) Concealing or disguising the true nature, source, location, ownership, or movement of proceeds of a crime: This involves taking steps to hide the fact that the money came from illegal activity. This can include:

- Falsifying documents, such as invoices or bank statements.
- Using nominees or strawmen to hold assets on behalf of the criminals.
- Transferring money through offshore accounts or other jurisdictions with weak AML laws.

c) Acquiring, possessing, using, or converting proceeds of a crime: This includes any act of benefiting from money that came from illegal activity, even if the person did not know or suspect that it was dirty money. Examples include:

- Investing laundered money in legitimate businesses.
- Using laundered money to buy luxury goods or real estate.
- Funding personal expenses with laundered money.

d) Assisting the perpetrator of the predicate offense to escape punishment: This includes any act that helps the person who committed the original crime avoid being caught or punished. This can include:

- Providing false or misleading information to law enforcement.
- Helping the criminal to flee the country.
- Hiding or destroying evidence of the crime.

What is Terrorist Financing?

Terrorist financing is the act of providing funds or financial support to individuals or groups engaged in terrorist activity, with the intention of furthering their objectives. It fuels terrorism by enabling them to:

- Acquire weapons and explosives: Funding for purchasing weapons, ammunition, and other materials used in terrorist attacks.
- Plan and carry out attacks: Resources for travel, logistics, training, and operational costs.
- Recruit and radicalize new members: Funding for propaganda, indoctrination, and recruitment activities.
- Support infrastructure and networks: Resources for maintaining communication channels, safe houses, and other operational needs.

Types of Terrorist Financing:

- Direct Funding: Providing money or resources directly to terrorists or terrorist organizations.
- Indirect Funding: Raising funds through donations, charitable organizations, or criminal activities, with the knowledge or intention that they will be used for terrorism.
- Self-financing: Generating income through legitimate or illegal businesses, extortion, or other means to support terrorist activities.

Methods of Terrorist Financing:

- Traditional Banking System: Using legitimate financial institutions to transfer funds, often disguised as donations or business transactions.
- Informal Value Transfer Systems: Utilizing hawala or hundi systems, which are informal remittance networks that operate outside of the formal banking system.
- Cash and Precious Metals: Physically transporting cash, gold, or other valuables across borders to avoid detection.
- Cybercrime: Exploiting online platforms for fundraising, fraud, or other illegal activities to generate funds.

Combating Terrorist Financing:

- International Cooperation: Global efforts by governments, financial institutions, and intelligence agencies to share information, identify suspicious activity, and disrupt terrorist funding networks.
- Anti-Money Laundering (AML) Regulations: Implementing stricter regulations for financial institutions to identify and report suspicious transactions.
- Countering the Financing of Terrorism (CFT) Legislation: Laws criminalizing terrorist financing and providing legal frameworks for investigation and prosecution.
- Public Awareness: Raising awareness about the dangers of terrorist financing and how to identify and report suspicious activity.

Money Laundering Vs. Terrorist Financing

While both money laundering and terrorist financing involve illegal financial activities, there are some key differences between them:

Source of funds:

- Money laundering: The source of funds being laundered is always illegal activity, such as drug trafficking, corruption, or tax evasion. The aim is to make these funds appear legitimate.
- Terrorist financing: The source of funds can be legal or illegal. Terrorists can raise money through legitimate businesses, donations, or even criminal activity. The purpose is to use the funds for terrorist activities.

Motivation:

- Money laundering: The primary motivation for money laundering is personal gain or avoiding prosecution for the underlying crime. Criminals want to enjoy the benefits of their illegal activities without facing legal consequences.
- Terrorist financing: The motivation for terrorist financing is ideological. Terrorists use the funds to support their cause, carry out attacks, and spread their ideology. They are not primarily concerned with personal gain.

Intention:

- Money laundering: The intention is to conceal the origin and nature of illegal funds, making them appear legitimate.
- Terrorist financing: The intention is to provide funds for terrorist activities, regardless of their source. The focus is on using the funds to advance their agenda.

Legal framework:

- Money laundering: Both international and national laws criminalize money laundering. These laws typically focus on specific predicate offenses, such as drug trafficking or corruption.
- Terrorist financing: There are also international and national laws specifically targeting terrorist financing. These laws often have broader scope than money laundering laws, as they can criminalize the financing of any terrorist activity, regardless of the underlying crime.

Feature	Money Laundering	Terrorist Financing
Motive	Personal gain	Furthering terrorist goals
Target funds	Illicit proceeds from any crime	Funds for or from terrorism
Destination	Legitimate financial system	Terrorist needs (weapons, training, etc.)
Complexity	High (layering, integration)	Variable (simple to complex)
Detection focus	Financial activity	Terrorist links and activities
Legal framework	AML laws	CFT laws
Global effort	FATF and regional initiatives	UN Security Council and FATF

Appendix 4- Red Flags – Money Laundering and Terrorism Financing

- Possible Money Laundering Via Cash Transactions

    - Customer makes large cash payments that seem suspicious given their occupation or claimed income source
    - Customer deposits cash that smells like marijuana, appears discolored, or seems otherwise unusual
    - Individual makes multiple cash deposits under $10,000 to avoid reporting requirements
    - Customer has a pattern of making cash deposits just under reporting thresholds across different branches/days
    - Individual requests cashing numerous cashier's checks, money orders, or traveler's checks
    - Customer presents cash for deposit wrapped in rubber bands or with drug residue
    - Deposits contain counterfeit bills or cannot be authenticated as legitimate currency
    - Customer exhibits unusual nervousness, agitation, defensiveness or evasiveness with cash transactions
    - Cash transactions involve recently incorporated shell companies or companies with no real business purpose
    - Frequent large cash deposits made into personal accounts inconsistent with the customer's occupation
    - Multiple individuals depositing cash into a single account without reasonable explanation
    - Customer makes cash deposits and withdrawals with rapid turnover of deposited funds
    - Individual attempts to avoid cash transaction reporting by breaking up deposits across accounts, days, bank branches, etc.
    - Customer's description of the nature/source of cash deposits doesn't make sense or changes frequently
    - Individual has no record of past or present employment that could reasonably account for large cash transactions
    - Cash deposits carry traces of chemicals, money bands, packaging materials, or other signs they could be from illegal drug sales
    - Customer exhibits lack of concern about significant bank fees, commissions, or other transaction costs

- Cash deposits reference vague or doubtful purposes (e.g. “personal expenses”, “office supplies”, etc.)
- Unusually large cash transactions relative to what would be expected for a customer’s profile and banking history
- Cash deposits from known high-risk businesses (e.g. bars, strip clubs, casinos, etc.) without logical business purpose

- Possible Money Laundering Via Clients Accounts

  - Frequent large round-dollar transactions lacking clear legitimate business purpose
  - Client exhibits sudden spike in transaction volume inconsistent with past activity
  - Multiple cash deposits from various individuals into a single corporate account
  - Transactions involve higher-risk jurisdictions known for money laundering
  - Company has complex corporate structure across international borders lacking clear business rationale
  - Frequent wire transfers from or to parties unrelated to client’s business
  - Account activity drastically increases without reasonable explanation
  - Payments reference vague descriptions failing to link to legitimate goods/services
  - Bank can’t obtain transparent ownership structure for corporate client
  - Transactions moved quickly between client’s accounts or through multiple accounts
  - Corporate account appears to act as a pass-through for other entities’ money flows
  - Company registered overseas in jurisdiction with weak AML reporting rules
  - Large transactions consistently occurring just under reporting thresholds
  - Client company’s ownership recently changed hands or shows indications it could be a shell company
  - Frequent transactions involving cash, cash equivalents, or currency exchange that lack clear business rationale
  - Payments to or from trading partners where legitimacy can’t be verified
  - Accounts show high velocity movement of funds incongruent with the nature of the business
  - Bank can't authenticate client company's physical operational activity or employees
  - Unexpected/illogical level of account activity for company of its size and industry
  - Transactions prominently include parties in industries/sectors prone to higher money laundering risk
  - Inability to confirm legitimacy of client’s suppliers, customers, or counterparties
  - Payments reference goods or services markedly inconsistent with client’s line of business
  - Beneficial owners of account change substantially before money flows take place
  - Large incoming payments from institutions having no logical connection to client
  - Company shows sudden increase in transaction activity after long period of account inactivity
  - Uncorroborated explanations given when questioned about suspicious money flows
  - Attempts to disguise identities of originators or beneficiaries per banking investigations

- Possible Money Laundering Via Investment Related Transactions

  - Customer makes large investments in cash or cash equivalents without plausible explanation of the funds’ origins
  - Client investment account shows sudden spike in Wire Transfers and Journal Transfers involving unassociated third parties
  - Transaction volumes through investment accounts vastly outweigh customer's apparent income/net worth
  - Back-to-back transactions moving funds between multiple accounts lacking economic rationale
  - Securities transactions by customer exhibit unexplained repurchasing activity or high turnover
  - Customer opens account and shortly thereafter requests liquidation with plan to direct proceeds offshore
  - Investment account owner appears to act at the direction of unknown controlling parties
  - Transactions involve bearer securities outside of a recognized market or securities firm
  - Investments reference entities in higher-risk offshore jurisdictions with ownership opacity
  - Individuals/entities transferring proceeds unexpectedly donate them to charity foundations exhibiting unusual activity

- Customer exhibits limited investment savvy/interest in performance returns on invested funds
- Explanations regarding origins of funds moved into investment account seem opaque, complex or constantly changing

- Possible Money Laundering Via International Banking and Financial Transactions

  - Payments to or from parties in higher-risk jurisdictions identified by government AML authorities
  - Client transactions involve countries identified as tax havens lacking financial transparency
  - Funds moved to personal accounts lacking business purposes offshore after clearing domestic accounts
  - Individuals make large over/under payments referencing imports/exports without logical follow-on activity
  - Attempts by parties to disguise identities, jurisdictions, companies, goods, etc related to transactions
  - Customer transactions exhibit unexplained complexity or involve more parties/accounts than typical
  - Payments reference family members or close associates not tied to underlying goods/services
  - Offshore shell or front companies receiving payments soon disburse funds to other foreign parties
  - Bank can't determine legitimacy of offshore company transaction counterparts or affiliates
  - Transactions depict goods/capital flows differing from client's line of business without explanations
  - Unexpected activity from client involves jurisdictions considered high risk for sanctions evasion

- Possible Money Laundering Via Letters of Credit and Other Methods of Trade Finance

  - Beneficiaries and applicants show affiliation despite claiming to be unrelated third parties
  - Signs terms or parties for trade transactions differ across separate documents lacking explanations
  - Invoices, packing lists and other paperwork reflect conflicting descriptions of goods and timelines
  - Letters of credit transaction values, volumes or frequencies spike for no substantiated reason
  - Trade finance transaction counterparties reluctant or unable to provide details if questioned
  - Vessel movements show import/export irregularities regarding quantities, weights, timing or locations
  - Parties involved refuse to provide supporting KYC/CDD transparency into identities, ownership, etc.
  - Beneficiary requests payouts to bank accounts unaffiliated to the party orchestrating transactions
  - Applicant exhibits unusual indifference about fees/costs for high-value letter of credit or factoring
  - Attempted capital transfers just under reporting thresholds via trade transactions
  - Finance requests reference goods markedly mismatching client's normal line of business/expertise

- Possible Money Laundering Via secured and unsecured loans

  - Borrower unable to demonstrate legitimate source of funds used to collateralize loans
  - Loan collateral unexpectedly moved offshore just prior to securing financing
  - Unusual surge in loan payoffs or repayments that can't be validated against a legitimate income source
  - Loans paid down much quicker than the formal amortization and borrower's profile would dictate
  - Borrower offers rates/fees significantly above market prices without attempts to negotiate terms
  - Loans requested by Shell companies, offshore entities, or parties unable to justify a valid business purpose
  - Loans cycled between interrelated parties exhibiting affiliation despite claiming independence
  - Frequent attemps to take out cash advances, overpayments, or access credit line funds via unusual methods
  - Sudden requests to increase loan disbursements or credit lines without reasonable business explanations
  - Attempts to obscure source of funds used as collateral through third party arrangements or opacity in documentation
  - Loan payments coming from accounts unrelated to stated income sources, employers, business affiliates etc.

- Possible Money Laundering Via Electronic Banking Services

  - Sudden unexplained electronic funds transfers, especially involving higher-risk jurisdictions

- Customer exhibits unfamiliarity with details of electronic payments they supposedly initiated or authorized
- Attempts to disguise recipient details for electronic funds transfers
- Payments or transfers involve parties unrelated to customer without logical business explanations
- Electronic banking channels used to pay invoices differing materially from client's line of business
- Unexplained wire transfers quickly followed by requests to withdraw funds with little time lag
- Electronic payments reference generic goods/services descriptions masking true underlying purposes
- Individuals withdraw cash soon after receiving electronic deposits from unknown third parties
- Dramatic increases in e-banking transaction volumes fail to correlate to customer profile or historical norms
- Third party payments into accounts followed by immediate international transfers via e-banking
- Sudden activity from previously dormant internet or mobile banking channels without cause

- Red Flags for Terrorist Financing:

  - Transactions involving high-risk geographies of known terrorist activity without reasonable explanation
  - Client demonstrates little to no concern or knowledge regarding account finances or transactions
  - Charitable donations made to foundations later found to have affiliations with known terrorist groups or activities
  - Payments from or to parties sanctioned as Specially Designated Nationals by regulatory authorities
  - Individuals associated with non-profit organizations exhibit unusual aversion to transparency over donation sources/uses
  - Multiple cash deposits/withdrawals with signs structuring to avoid reporting thresholds
  - Funds transferred bear hallmarks of comingled legitimate financing and value from criminal/terrorist sources
  - Inability to reasonably justify sources related to wires, money orders, traveler's checks over certain thresholds
  - Account dealings portray latest known terrorist financing typologies and methodologies
  - Ill-defined series of international transactions adding intermediaries subtly shifting funds to high risk locales
  - Individuals or non-profits supporting good causes abroad unwilling to reveal full details on specific aid/grantee parties
  - Transactions involve front companies operating in high-risk jurisdictions identified for terrorism financing vulnerability
  - Accounts of non-profit organizations, charities, or foundations show unusual cash or credit activity
  - Client donations reference receiving parties resembling aliases of known terrorists on restricted lists
  - Bank can't obtain definitive information validating listed purpose, beneficiaries for wire transfers
  - Inflated transaction fees relative to typical ranges without reasonable explanation
  - Inability to reasonably explain extensive use of small money transmitter services for flows to high-risk regions
  - Intelligence suggests certain conduits like import/export firms or smugglers connected to terrorist plots
  - Employing other money laundering typologies like trade-based techniques seen to fund terrorism
  - Expressed statements showing extremist, intolerant views regarding certain races, religions or nationalities

<u>Some of Financial Crime Red Flags as per UAE Central Bank:</u>

The FIU published the following typologies and indicators in their Biannual Financial Crime Trends and Typologies Report (January - June 2020). These typologies and indicators, as well as any future ones the FIU may determine, should be incorporated into an LFI's AML/CFT program with a view to update policies, procedures, detection scenarios, and red flag indicators for identifying potentially suspicious activity.

1. According to the FIU, the following indicators are present in many of the typologies used in money laundering and the financing of terrorism and illegal organisations.
   - Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.

- Significant and/or frequent transactions in contrast to known or expected business activity.
- Significant and/or frequent transactions in contrast to known employment status.
- Ambiguous or inconsistent explanations as to the source and/or purpose of funds.
- Where relevant, nervous or uncooperative behavior exhibited by the LFI's employees and/or customers.

2. Wire transfers to and from bank accounts

- How it works: Transferring proceeds of crime from one person to another via money remittance services.
- Possible indicators
  - Significant and/or frequent cash payments for transfers.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers to high-risk countries or known tax havens.
  - Transfers to numerous offshore jurisdictions with no business rationale.
  - Same home address provided by multiple remitters.
  - Reluctant to provide the LFI with identification details.

3. Purchase of valuable commodities

- How it works: Laundering proceeds of crime by purchasing valuable commodities, for example, precious metals or gems.
- Possible indicators
  - Significant and/or frequent cash purchases of valuable commodities.
  - Regularly buying and selling of valuable commodities that is not supported with a business purpose and/or does not make economic sense.

4. Purchase of valuable assets

- How it works: Laundering proceeds of crime by purchasing valuable assets, for example, property or vehicles.
- Possible indicators
  - Purchase/sale of real estate above/below market value irrespective of economic disadvantage.
  - Cash purchases of valuable assets with cash and/or cash deposits for valuable assets.
  - Low value property purchased with improvements paid for in cash before reselling.
  - Rapid repayment of loans/mortgages with cash or funds from an unlikely source.

5. Offshore companies

- How it works: The process of registering companies in the UAE, especially in the free zones, with foreign directors and/or shareholders in order to open bank accounts to facilitate money laundering and/or the financing of terrorism and illegal organisations by unverified beneficiaries.
- Possible indicators
  - Large numbers of companies registered with the same office address.
  - Address on file is for a 'Virtual office'.
  - Accounts/facilities are opened/operated by company formation agents.
  - Lack of information regarding overseas directors/beneficiaries.
  - Complex ownership structures.
  - Companies where there is no apparent business purpose.
- Additional indicators:
  - same natural person is the director for a large number of single director companies.
  - The same person (natural or corporate) is the shareholder of a large number of single-shareholder companies.
  - Use of a small number of local 'agents' who undertake transactions with the companies' register.

6. Nominees, trustees, family members or third parties

- How it works: Utilizing other people to carry out transactions in order to conceal the true identity of the individual ultimately controlling the proceeds of crime.
- Possible indicators
  - Transactions where third parties seem to be retaining a portion of funds, which would indicate the use of mules.
  - Accounts operated by someone other than the account holder.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Significant and/or frequent transactions made over a short period of time.

7. Trade-based money laundering

- How it works: Manipulating invoices, often in connection with international trade, by overstating the value of a shipment providing criminal entities with a paper justification to either launder proceeds of crime and/or send funds overseas to finance terrorism.
- Possible indicators
  - Invoice value greater than value of goods.
  - Discrepancies in domestic and foreign import/export data.
  - Suspicious cargo movements.
  - Suspicious domestic import data.
  - Discrepancies in information regarding the origin, description, and value of the goods.
  - Discrepancies with tax declarations on export declarations.
  - Sudden increase in online auction sales by particular vendors (online auction sites).
  - Frequent purchases between same buyers and vendors (online auction sites).

8. Cancellation of credits or overpayments

- How it works: Laundering proceeds of crime by overpaying then requesting refund cheques for the balance.
- Possible indicators
  - Frequent cheque deposits issued by car dealers, dealers in jewelry, etc.
  - Significant and/or frequent payments to utility companies, for example, prepaid cards for fuel, telecom e-wallets etc.
  - Frequent cheque deposits issued by utility companies (i.e., electricity providers).
  - Significant and/or frequent payments for purchases from online auction sites.
  - Frequent personal cheque deposits issued by third parties.

9. Electronic transfers to and from bank accounts

- How it works: Transferring proceeds of crime from one bank account to another via LFIs.
- Possible indicators
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Transfers involving accounts located in high-risk countries or known tax havens.
  - Transfers to offshore jurisdictions with no business rationale.
  - Multiple transfers sent to the same person overseas by different people.
  - Departure from the UAE shortly after transferring funds.
  - Transfers of funds between various accounts that show no economic purpose (i.e., multiple transfers incurring bank fees where one single transfer would have been sufficient).

10. Co-Mingling

- How it works: Combining proceeds of crime with legitimate business takings.
- Possible indicators
  - Significant and/or frequent cash deposits when business has electronic funds transfer at point-of-sale facilities.
  - Large number of accounts held by a customer with the same LFI.
  - Accounts operated by someone other than the account holder.

- Merging businesses to create layers.
- Complex ownership structures.
- Regular use of third-party accounts.

11. Gatekeepers/professional services

- How it works: Utilizing 'Professionals' to establish seemingly legitimate business activities, for example, Lawyers, Accountants, Brokers, Company Formation Agents.
- Possible indicators
  - Accounts and/or facilities opened and/or operated by company formation agents.
  - Gatekeepers that appear to have full control.
  - Known or suspected corrupt professionals offering services to criminal entities.
  - Accounts operated by someone other than the account holder.

12. Cash deposits

- How it works: Placement of cash into the financial system.
- Possible indicators
  - Large cash deposits followed immediately by withdrawals or electronic transfers.

13. Structuring

- How it works: Separating large transactions into small transactions to avoid scrutiny and detection from LFIs.
- Possible indicators
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Small/frequent cash deposits, withdrawals, electronic transfers made over a short time period.
  - Multiple low value domestic or international transfer.

14. Smurfing

- How it works: Utilizing third parties or groups of people to carry out structuring.
- Possible indicators
  - Third parties conducting numerous transactions on behalf of other individuals.
  - Many transactions conducted at various LFIs and/or branches, in one day.
  - Accounts operated by someone other than the account holder.

15. Credit Cards/Cheques/Promissory Notes

- How it works: Instruments used to access funds held in an LFI, often in another jurisdiction.
- Possible indicators
  - Frequent cheque deposits in contrast to known or expected business activity.
  - Multiple cash advances on credit card facilities.
  - Credit cards with large credit balances.

16. Transactions inconsistent with intended purpose of the account

- How it works: Transactions that are out of the ordinary for the individual or conducted without a clear rationale.
- Possible indicators
  - Transactions to or from unrelated parties.
  - Transaction amounts that are inconsistent with the account's expected volumes or frequencies.
  - Transactions that are out of the ordinary for the customer's profession or business activity.

17. Cash couriers

- How it works: Concealing the movement of currency from one jurisdiction to another using people, luggage, mail, or any other mode of shipment, without declaration.
- Possible indicators
  - Transactions involving locations with poor AML/CFT regimes or high exposure to corruption.
  - Customers originating from locations with poor AML/CFT regimes/high exposure to corruption.
  - Significant and/or frequent cash deposits made over a short period of time.
  - Significant and/or frequent currency exchanges made over a short period of time.

18. Other payment technologies

- How it works: Utilizing emerging or new payment technologies such as virtual currencies/crypto- currencies, peer-to-peer (P2P) lending etc. to facilitate money laundering and/or the financing of terrorism and illegal organisations.
- Possible indicators
  - Excessive use of stored value cards.
  - Significant and/or frequent transactions using mobile telephone services.
  - Unjustified transactions to and from Cryptocurrency platforms and digital assets exchanges.

19. Underground banking/alternative remittance services

- How it works: Transferring proceeds of crime from one person to another via informal banking mechanisms such as unregistered Hawaladars.
- Possible indicators
  - Mostly prevalent under the auspices of a general trading company license.
  - Significant and/or frequent cash payments for transfers in which the cash deposits could be from many different individuals using the cash deposit machines.
  - Cash volumes and transfers in excess of average income of migrant account holders.
  - Transfers to or from locations that have poor AML/CFT regimes or high exposure to corruption.
  - Large transfers from accounts to potential cash pooling accounts.
  - Significant and/or frequent transfers recorded informally using unconventional bookkeeping.
  - Significant and/or frequent transfers requested by unknown or intermittent customers.
  - Numerous deposits to one account followed by numerous payments made to various people.
  - Vague invoices and documentation which may deliberately be made to appear complex.

20. Cash exchanges

- How it works: Exchanging low denomination notes for high denomination notes (also known as refining) as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- Possible indicators
  - Significant and/or frequent cash exchanges from small to large denominations.

21. Currency conversion

- How it works: Converting one currency into another as a means to launder proceeds of crime, as well as reduce large volumes of cash obtained from serious crime.
- Possible indicators
  - Significant and/or frequent local or foreign currency exchanges.
  - Opening of foreign currency accounts with no apparent business or economic purpose.

Appendix 5- Emerging Trends in Money Laundering/Terrorism Financing

Here are some key emerging trends in money laundering and terrorism financing, with a focus on virtual currencies, prepaid cards, mobile/online payments, and social media fundraising:

1. Virtual Currencies

The rise of cryptocurrencies like Bitcoin and Ethereum have introduced new channels for money launderers and terrorist financiers to exploit. The pseudo-anonymous qualities of most cryptocurrency transactions, along with exchanges operating in countries with weak anti-money laundering regulations, enables the transfer and laundering of illicit funds at higher volumes. Services like cryptocurrency tumblers or mixers add additional layers of obscurity by blending multiple transaction streams. New regulations and enhanced analytics techniques are needed to curb the use of cryptocurrencies for illicit financing.

- Increased use of cryptocurrencies like Bitcoin that allow pseudo-anonymous transactions
- Crypto exchanges in jurisdictions with weak AML regulations being exploited
- Anonymizing services and mixers used to obscure crypto transaction histories and wallets

2. Prepaid Cards

Prepaid debit and gift cards have also grown as a mechanism for money laundering. Cards can be loaded with funds from criminal activities and used to make normal purchases without raising the same suspicions as large cash transactions. They can also be used internationally by withdrawing cash from ATMs in different countries, moving money across borders much more easily. Many prepaid card programs still feature less stringent customer due diligence requirements compared to traditional bank accounts. Regulators have grown concerned about unlinked cards loaded with substantial amounts.

- Loading with funds from illicit sources and using cards to make purchases or withdrawals
- Abilities to quickly move funds across borders through ATM cash withdrawals
- Limited customer due diligence on many prepaid card programs

3. Mobile Payments & Online Services

There is rising regulatory concern around the use of mobile payments apps, online accounts, and fintech services for illicit fund transfers and laundering. These technology platforms allow cheap, rapid global transactions with minimal oversight into source of funds in many cases. Launderers exploit these systems by creating funnel accounts, including multiple e-wallets through app-based services, to shift money between accounts across borders. The scale and complexity across an interconnected network of accounts makes tracking the ultimate origins or destinations of funds a major challenge.

- Mobile payment apps and fintech payment platforms enabling fast, global transfers
- Creating funnel accounts and moving funds between multiple e-wallets across borders
- Limited oversight of source of funds with accounts linked to payment apps/services

4. Social Media Fundraising

Finally, social media has been exploited by terrorist sympathizers and groups to openly solicit donations and financing, often linking to prepaid cards or cryptocurrency wallet details to receive funds. The relative anonymity around personal profiles on platforms like Facebook and the ability to instantly communicate with global users makes preventing terrorist financing highly complex. Additionally, humanitarian causes and charities often use the same platforms, providing covers that malign actors exploit to conceal funding for illegal activities. Advanced analytics around connections, profiles, and transfers represents one emerging approach.

- Terrorist sympathizers exploiting social media for soliciting financial support

- Crypto wallets and prepaid cards used in conjunction with social media fundraising outreach
- Difficulty tracking and validating where funds ultimately end up
- Exploiting charities and non-profits also active on platforms like Facebook to disguise flows

The following are a few methods and trends identified by FATF

1. Concealment of Beneficial Ownership

Perpetrators have increasingly used legal entities and complex corporate structures across various international jurisdictions to conceal the true beneficial ownership and disguising the origins of illicit funds. This involves long chains of shell companies, formal nominees, informal nominees and external shareholders, especially via tax haven jurisdictions. Red flags include inability for banks to determine ownership, newly created offshore companies, multiple payments between related shell entities, unnecessary complexity in corporate structures, nomination shareholders inconsistent with size of holdings, and more. Regulators are now focusing on ownership verification.

2. Professional Money Laundering

The scale and complexity of modern money laundering often requires expertise, with third party specialists like lawyers, accountants and investment advisors complicit in laundering proceeds for criminal networks and rogue entities. Recognizing these professionals require advanced training and typologies. Red flags include affiliation with known crime groups, lavish lifestyles inconsistent with services, unusual or deception client relationships, mixtures of personal with business accounts or source of funds, and reluctance to provide details. Targeted surveillance and reporting rules are being implemented.

3. Covid-19- related Money Laundering and Terrorist Financing Risks

New COVID-19-related threats around misappropriated, stolen or diverted funds as well as exploitative cybercrime and fraud taking advantage of the global crisis were brought into focus during 2020. Tracking and preventing laundering of these criminal profits presents regulatory obstacles. Recent red flags include suspicious transactions against government funds, loans or grants related to pandemic funds and spikes in cybercrime, extortion campaigns exploiting public fears over COVID-19 vaccines, health data privacy, e-commerce skimming, and other citizen fears.

4. Money Laundering and the Illegal Wildlife Trade

The illegal trafficking of animals or wildlife and related products is a key global challenge. Financial flows related to poaching and illegal trade in wildlife frequently involve money laundering via transnational networks and criminal syndicates. Regulators are now being asked to monitor financial transactions for reference to endangered animals or animal products. Commercial poaching and animal trafficking violates national and international laws.

5. Money Laundering and Human Trafficking

There is also rising priority by regulators to detect potential red flags involving human trafficking through payments, electronic transfers and loans. Human trafficking involves forcefully exploiting vulnerable individuals against their will and benefiting from commercial sex trade or forced labor/slavery among victims including migrant workers. Tactics include frequent travel payments with same senders/beneficiaries, seemingly unrelated or offshore parties transacting around an individuals' travel, payments by third parties linked to illegal transportation schemes, sparse payments histories, and indicators of physical or psychological control over individuals consistent with traffickers.