2026-2027

IRIS GLOBAL FZCO

DUBAI, U.A.E.

POLICY STATEMENT:

Iris Global FZCO is a licensed entity with "License Number – DMCC 258286" and supervised by Ministry of Economy as its reporting entity and is committed to prevent money laundering and countering the financing of terrorism.

Iris Global FZCO, as a business entity and trade license holder conducts following business in the UAE:

1. Non- Manufactured Precious Metal Trading

The management understands the importance of application of the standards and guidelines issued by Ministry of Economy and the supplementary guidance for industry best practices while doing the transactions and conducting businesses in the UAE. The company provides its services and products to local & International markets and implements stringent compliance regime across its operations. The company has conducted internal risk assessment based on Risk based approach including the FATF Standards by considering country risk, customer risk, products, services & transaction risk & delivery channel risk including other attributes and has adopted appropriate risk classifications, it has further considered the outcomes and guidelines of UAE's NRA (National Risk Assessment) & Typologies considering the UAE's Sectorial Risks reports. The management ensures the parties its dealing is sourcing precious metals and stones are asper the UAE laws and Regulations on AML/CFT following the federal decree law no.20 of 2018 and the cabinet decision no. (10) of 2019 on the executive regulation of federal decree-law no.20 of 2018 and its amendments. The company follows the country risk ratings provided by FATF (https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2022.html) and Know your country ratings list (https://www.knowyourcountry.com/ratings-table/) to ensure the geographical & overall risks are ascertained in appropriate manner and accordingly CDD & EDD measures are undertaken.

The company engages in following ethical practices with adherence to sourcing its raw materials from its vendors and ensures it conducts all its transactions in a manner to adhere with all applicable home regulations on AML/CFT including all applicable rules, laws & regulations. The Company deals with B2B customers and retail customers trading in precious metals.

Precious metals would mean gold, silver, palladium, or platinum whether in coins, bars, ingots, granules or in any other similar form, while precious stones mean diamonds, sapphires, emeralds, tanzanite, rubies, or alexandrite. Any object concerning which at least 50 percent of its monetary value is comprised of precious metals and stones (PMS). A variety of high-value industrial metals, including so-called conflict minerals (for example, wolframite, cassiterite, and coltan), cobalt, and other platinoid metals (e.g., rhodium, etc.). A variety of semi-precious gemstones (e.g., amethysts, opals, jade, and others);

Synthetic, treated, or artificial gemstones (Diamonds, Emeralds, Rubies, Sapphires, Pearls).

This Policy is applicable to production and/or trade of precious metals or stones, whether in raw, cut, polished, or elaborated (mounted or fashioned) form. Production and/or trade in this context includes any of the following acts involving raw/rough or processed/finished PMS:

- Extraction (whether by mining or other method), refining, cutting, polishing or fabrication.
- Import or export. Purchase, sale, re-purchase, or re-sale (whether in primary, secondary, or scrap markets);
- Barter, exchange, or other form of transfer of ownership.
- Loan or lease arrangements (e.g., sale-leaseback, consignment, or memorandum sales);

- Possession (whether permanent or temporary, for example, as part of a fiduciary, warehousing, collateral, or other safekeeping arrangement; or under contract for a specific purpose such as cutting, polishing, refining, casting, or fabrication services).

This Policy is applicable to:

- Wholesale or Retail Trade
- Whether it is direct or indirect (such as through a broker or other intermediary)
- Whether it is between natural or legal persons or legal arrangements, including any other Dealer in precious metals and stones (DPMS)
- Whether the PMS are traded physically or virtually (for example, via certificates, on electronic exchanges, or via internet), irrespective of where or by whom the physical goods are warehoused, held in safekeeping, or delivered.

The management ensures to file mandatory DPMSR (Dealers in Precious Metals and Stones Reporting) on the Goaml portal which are meant for DPMS activities. The management conducts its own due diligence on suppliers as an important measure and in line with AML/CFT regulatory requirements. The company conducts trading as per the permissible activities mentioned in its license.

The management has conducted Internal Risk Assessment based on Products, types of customers and transactions, distribution channel risk and geographical locations and the supply chain intermediaries involved and accordingly identified the inherent risk and applies appropriate controls to derive Residual risk related to ML & TF and accordingly on boards and conducts its transactions including sales and purchases.

The company mainly sells to B2B customers in the segment of retailers and wholesalers by applying EDD and suitable controls which shall be subject to senior management approvals, and especially avoid sourcing from intermediaries and zones or areas which come under the Conflict-affected and high-Risk Areas (CAHRA), the company ensures to conduct EDD and senior management approval prior to dealing with any high-risk customers or suppliers.

The management of Iris Global FZCO believes that the best way to fulfill this commitment is to establish effective internal policies and procedures that are conducive to:

- Carrying out the activities and services provided in accordance with strict ethical standards and current laws and regulations.
- The implementation of codes of conduct and monitoring and reporting systems to prevent that the company is used for money laundering and terrorism financing.
- Ensuring that all the employees of Iris Global FZCO observe this policy manual and performs action to the adherence of the processes mentioned in it.

This Policy Manual is:

Reviewed and recommended by:

Compliance Officer/ MLRO

Dated: 30/03/2026

Approved by: Mr.Pranav Jaiprakash Bajaj

Owner/Board of Directors

Document Control & Schedule - Updates & Review:

Version No.	Date	Sections Changed	Summary of Changes
AML/CFT/IGD-2023-24/V1.10 Next Review – End of 2023 or on any New-Regulatory Updates.	25th March 2023	Policy Updated	FATF Country list
AML/CFT/IGD-2024-25/V1.20	25th Feb 2024	Policy Updated	Country list and Risk Scoring
AML/CFT/IGD-2025-26/V1.30	20th Feb 2025	Policy Updated	FATF Grey List, MOE circular (CRA)- Customer Risk Assessment
AML/CFT/IGD-2026-27/V1.40	25th Feb 2026	Policy Updated	Aligned with AML Federal law No.10 of 2025 Updated FATF Grey List

Table of Contents

1. BASIS OF POLICY FORMULATION AND REFERENCES

1.1. The Ministry of Economy

The Ministry of Economy is fully committed to countering money laundering, combating, detecting, and deterring terrorist financing in accordance with legislation, as the relevant authorities in the UAE have established an institutional system of supervision, control and gathering information on all practices that may lead to and respond to financial crimes, including money laundering and terrorist financing. The authorities are aware that the national framework and coordination to address money laundering and combat terrorist financing must continue to be strengthened and developed to improve its effectiveness.

This policy document is based on the guidelines issued by the following regulatory authorities and trade bodies, the document is in adherence with all applicable UAE Laws and Regulations as mentioned herein, the activities of the company and Its activities ultimately is dependent on local Banks & Licensed Financial Institutions (LFI's) for conducting and completing its financial transactions related to the business activities conducted., it's imperative for the company to abide by all laws and regulations related to AML/CFT which directly or due to its relationships with LFI's may have an impact on its activities. The below mentioned laws and regulations have been taken into consideration to enhance the company's activities with overall enhanced AML/CFT Compliance Regime.

Comparison table: key differences between the New AML Law No.10 of 2025 and the Previous Federal AML Law

Topic	Position under the New AML Law	Position under the Previous AML Law
New offences and expanded coverage of existing offences	Proliferation financing offences have been expressly included in the New AML Law. The New AML Law also expressly addresses the use of digital systems, virtual assets and encryption technologies as methods of committing the Principal Offences.	The Previous AML Law was limited to money laundering and terrorist financing offences. It did not include proliferation financing offences. The Previous AML Law did not expressly capture the use of digital systems, virtual assets and encryption technologies as methods of committing money laundering and terrorist financing offences.
Broadened definition of the predicate offence for the offence of money laundering	The definition of a 'predicate offence' for the purpose of establishing a money laundering offence now also specifically includes the crimes of terrorist financing, arms proliferation financing and indirect and direct tax evasion.	Under the Previous AML Law, a 'predicate offence' was any act constituting a felony or misdemeanor (committed within or outside of the UAE).
Lowered legal threshold for establishing the Principal Offences	The legal threshold for establishing the Principal Offences has been lowered. Under the New AML Law, knowledge that funds were illicit can be inferred from the factual and objective circumstances (an objective test).	Under the Previous AML Law, it was necessary to prove that a person had actual knowledge that the funds were illicit, in order to establish liability for a money laundering or terrorist financing offence (a

	This means that liability can arise where a person either actually knew or it would have been reasonable for them to have known about the illicit nature of the funds in question.	subjective test). There was no objective test included in the legislation.
Increased penalties for the Principal Offences and inclusion of personal criminal liability for managers	Under the New AML Law, penalties for the Principal Offences have significantly increased, as follows: Legal entities can be subject to a fine of between AED 5 million and AED 100 million or a sum equivalent to the value of the criminal property (whichever is greater), if their representatives, managers or agents commit any of the Principal Offences on behalf of the entity or in the entity's name. Regulated entities can be subject to a fine of between AED 200,000 and AED 10 million for failure to have the requisite licensing or authorizations to conduct their operations. Courts may order the dissolution of a legal entity or the closure of its headquarters if it is convicted of a Principal Offence. Managers of legal entities can now also be subject to personal criminal liability and risk exposure to a fine or imprisonment if they have actual knowledge of a Principal Offence or if a Principal Offence occurred as a result of a breach of their employment duties.	Under the Previous AML Law, penalties for money laundering and terrorist financing offences were as follows: Legal entities could be subject to a fine of between AED 500,000 and AED 50 million, if their representatives, managers or agents committed the offences of money laundering, terrorist financing or financing of illegal organizations on behalf of the entity or in the entity's name. Regulated entities could be subject to a fine of between AED 200,000 and AED 5 million for failure to have the requisite licensing or authorizations to conduct their operations. Courts could only order the dissolution of a legal entity or the closure of its headquarters if it was convicted of an offence of terrorist financing or financing illegal organizations (but not for the offence of money laundering). There was no specific criminal liability placed upon managers of legal entities for actual knowledge of a relevant offence or if the relevant offence occurred as a result of a breach of their duties.
Introduction of a new offence targeting misuse of accounts held within financial institutions or virtual asset service providers ("**VASPs**")	Under the New AML Law, it is an offence for a person to enable a third party to benefit from use of an account within financial institutions or VASPs if that person has actual knowledge or there is sufficient evidence to suggest that the third party intends to misuse the account. A person that commits such an offence can be subject to a fine or imprisonment.	There was no similar offence under the Previous AML Law.

Expansion of the FIU's enforcement powers	The FIU has been granted the power to issue the following orders: A **seizure order**, to suspend transactions suspected to be linked to financial crime for up to 10 working days, without providing prior notice. A **freezing order**, to freeze funds suspected to be linked to financial crime, held by financial institutions, designated non-financial businesses and professions ("DNFBPs") or VASPs, for a period of 30 days (such period is extendable). Under a freezing order, the assets remain under the control of the entity that is subject of the order, for the duration of the order.	Under the Previous AML Law, only: the Governor of the UAE Central Bank and the Public Prosecutor could exercise the power to seize funds, suspected to be linked to financial crime. the Governor of the UAE Central Bank could exercise the power to freeze funds suspected to be linked to a financial crime, held by financial institutions up to a period of seven days.
Introduction of enforcement powers to foster inter-agency cooperation within the UAE	The following changes have been introduced to encourage further cooperation between UAE law enforcement authorities: The Public Prosecution has the ability to consider the FIU's input, including its financial analysis on applicable data. Other law enforcement agencies may access and share information to identify and track criminal property. The applicable law enforcement agencies also have the right to receive and follow-up on the FIU's reports.	Cooperation between law enforcement bodies under the Previous AML Law was focused on the FIU cooperating with its international counterpart agencies.
Introduction of the UAE courts' powers to implement foreign orders	The New AML Law broadens the UAE courts' powers, permitting them to implement foreign orders for 'provisional measures' or confiscate criminal property (or sums of an equivalent value) without the need to carry out a local, UAE-based money laundering investigation.	There was no similar power conferred on the UAE courts under the Previous AML Law.

What does the introduction of the New AML Law mean for regulated businesses?

The UAE's continuing and rapid development of its AML/CTF/CPF regime reflects its ongoing commitment to demonstrating to local, regional, and global financial markets that combating financial crime remains a top priority for the country as a leading global financial and economic center and will continue to do so.

As regards enforcement risk, even before the introduction of the New AML Law, there had been a significant increase in AML/CTF enforcement activity in the UAE. The introduction of the New AML Law may signal yet even more active enforcement to come, particularly in light of the increases to penalties for existing offences, the introduction of new offences, which capture a wider range of conduct and individuals, and the additional powers conferred on the FIU and other law enforcement authorities, which are contained in the New AML Law.

In light, of such rapidly evolving regulatory environment, companies operating in the UAE are required to

- pay closer and ongoing attention to legislative and regulatory changes, and
- carefully review all compliance arrangements and allocate sufficient resources to ensure to meet all applicable legal requirements and regulatory expectations, including rolling out adequate training to senior managers, all employees and other relevant stake Sholders.

New executive regulations to accompany the New AML Law are recently published and enter into force., the pre-existing executive regulations (Cabinet Decision No.10 of 2019) being repealed and replaced by **cabinet decision number 134/2025 shall remain in force**. The new regulations strengthen compliance for FI's and DNFBP's explicitly integrates virtual asset service providers and imposes more stringent UBO and international cooperation requirements.

- Federal Law No. (10) of 2025
- Cabinet Resolution No (134) of 2025
- Circular No. (7) and (8) of 2025 from MOET & Circular from MOE/MOET/AML/6/2025

- Strict compliance with applicable Anti-Money Laundering and Terrorism Financing Laws - Decree 20 of the Federal Law 2018 on countering money laundering offences, combating terrorist financing and financing illegal organizations and
- As well as with the recommendations and circulars issued on this subject - Regulations 10 of 2019 for a decree of federal law No. 20 of 2018 on countering money laundering crimes, combating terrorist financing, and financing illegal organizations
- Cabinet Decision No. (20) of 2019 Terrorism List Regulation and Implementation of UN Security Council Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing and proliferation of Weapons of Mass Destruction, and Related Resolutions.
- Cabinet Resolution No. (16) of 2021 on the Consolidated List of Offences and Administrative Fines
- Cabinet Resolution No. (53) for 2021 on administrative sanctions resulting from violators of the provisions of The Council of Ministers Resolution No. (58) for 2020

- Cabinet Resolution No. (58) for 2020 on regulating the actions of the real beneficiary
- Cabinet Resolution No. (74) of 2020 on the system of lists of terrorism and the implementation of Security Council resolutions on the prevention, suppression and financing of terrorism, cessation of arms proliferation and financing and relevant resolutions
- 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 Organization's (the "AML-CFT Decision")
- Federal Law No. (7) of 2014 regarding terrorism offences.
- GoAML Notice - High Risk Country Transaction & Activity Report - 13/04/2021
- Notice No. 3090/2021 - Updated Guidelines on AML / CFT & Illegal Organizations
- Notice No. 3236/2021 - Guidance for LFI's providing services to the Real Estate and **Precious Metals & Stones Sector**
- Notice No. 3895/2021 - Implementation of UN Security Council (UNSC) and UAE Cabinet Resolutions regarding UNSC and Local Lists
- Notice No. 2893/2021 - Guidance on **TFS** & Typologies on the circumvention of **Targeted Sanctions** against Terrorism & Proliferation of Weapons of Mass Destruction
- Notice No. 3556/2021 - Guidelines on AML & Countering Terrorist Financing
- Notice No. 3551/2021 - Guidance for LFI's - Implementation of Targeted Financial Sanctions
- Notice No. 3091/2021 - Guidance for LFI's on Suspicious Transaction Reporting
- Notice No. 4593/2021 - Guidance for LFI's Providing Services to Cash-Intensive Businesses
- Notice No. 4415.2021 - Typologies on AML & CFT in the Financial Sector
- Notice No. 4368.2021 - Guidance for LFI's on Transaction Monitoring & Sanctions Screening
- Notice No. 4711/2021 - AML/CFT & Illegal Organizations Controlled & Dual use Goods for FIs
- Notice No. 5271/2021 - Guidance for Licensed Exchange Houses & Amended Chapters of the Standards for the Regulations
- Applicable Red-flags indicators for suspicious transactions as required by the Article (16) of Cabinet Resolution No (10) of 2019
- Ministry of Economy Guidelines on applying Due Diligence Regulations for Responsible Sourcing of Gold , (Precious Metals & Stones) August 2022.

- Guidance on Targeted Financial Sanction for FIs, DNFBPs and VASPs issued by the EOCN (Executive Office for Control & Non-Proliferation)
- All other relevant laws/regulations and Typology Reports issued by UAE on AML/CFT and international initiatives and best practices, including applicable (Organization for Economic Co-operation and Development) OECD Guidelines for responsible supply chains of mineral from Conflict Affected and High-Risk Areas and its supplements applying to Refiners and other stakeholders in a gold supply chain and therein

Website: www.economy.gov.ae

1.2. The Central Bank of UAE:

The Central Bank of the United Arab Emirates is the state institution responsible for managing the currency, monetary policy, and banking regulation in the United Arab Emirates (UAE).

The Central Bank of the UAE has powers to issue and manage the currency.

- to ensure the stability of the currency.
- to manage the UAE's credit policy.
- to develop and oversee the banking system in the UAE.
- to act as the Government's banker.
- to provide monetary and financial support to the Government.
- to manage the UAE's gold and currency reserves.
- to act as the lender of last resort to banks operating in the UAE; and
- to represent the UAE in international institutions such as the International Monetary Fund, the World Bank, and the Arab Monetary Fund.

The Central Bank of UAE has the following functions: -

- Branches
- Banking Supervision and Examination Department
- Banking Operations Department
- Research and Statistics Department
- Administration Affairs Department
- Financial Control Department
- Treasury Department
- Internal Audit Department

UAE laws on AML/CFT, Frauds, Anti-Bribery and Corruptions

- CBUAE regulation 24/2000 and covers the area of corruption laws.
- Federal Law 4/2002 regarding the Criminalization of Money Laundering.
- Federal Law 9/2014 amending certain provisions of Federal Law 4/2002 concerning the Combating of Money Laundering Crimes.
- Dubai Law 4/2016 on Financial Crimes.
- Cabinet Resolution 38/2014, Executive Resolution of Federal Law 4/2002.
- Federal Law 7/2014, Combating Terrorism Crimes regulations regarding declarations by travelers entering or leaving the United Arab Emirates carrying cash and monetary or financial bearer instruments (issued in 2011).
- Federal Decree Law No 20 of 2018 issued by Ministry of Finance.
- The Standards for the Regulations Regarding Licensing and Monitoring of Exchange Business ("the Standards") Version 1.10 (February 2018)
- National Risk Assessment, issued by National Committee for combating ML/TF (NAMLCFTC) (June 2019)
- Cabinet decision No (10) 2019, issued by Ministry of Finance, (June 2019)

Website: http://cbuae.gov.ae

1.3. United Nations:

United Nations is an intergovernmental organization to promote international co-operation. It was established on 24th of October 1945. At its founding, United Nations had 51 member states. Currently United Nations has 153 members. The headquarters of the United Nations is in Manhattan, New York,

USA. The organization is financed by assessed and voluntary contributions from its member states. Its objectives include maintaining international peace and security, promoting human rights, fostering social and economic development, protecting the environment, and providing humanitarian aid in cases of famine, natural disaster, and armed conflict.

The UN has six principal organs:

- the General Assembly (the main deliberative assembly).
- the Security Council (for deciding certain resolutions for peace and security);
- the Economic and Social Council (ECOSOC) (for promoting international economic and social co-operation and development);
- the Secretariat (for providing studies, information, and facilities needed by the UN);
- International Court of Justice (the primary judicial organ); and
- the United Nations Trusteeship Council (inactive since 1994).

UN System agencies include the World Bank Group, the World Health Organization, the World Food Program, UNESCO, and UNICEF.

United Nations Security Council: The Security Council is charged with maintaining and security among countries. While other organs of the United Nations can only make "recommendations" to member states, the Security Council has the power to make binding decisions that member states have agreed to carry out, under the terms of Charter Article 25. The decisions of the Council are known as United Nations Security Council resolutions.

The Security Council is made up of fifteen member states, consisting of five permanent members—China, France, Russia, the United Kingdom, and the United States—and ten non- permanent members. The UN Charter is a multilateral treaty. It is the constitutional document that distributes powers and functions among the various UN organs. It authorizes the Security Council to act on behalf of the members, and to make decisions and recommendations. Resolutions by the Security Council are legally binding if they are made under Chapter VII of the Charter.

Websites:

- http://www.un.org
- http://unscr.com

1.4. Financial Action Task Force (FATF)

The Financial Action Task Force on Money Laundering (FATF) was established in 1989 at G7 Summit in Paris to combat the growing problem of money laundering. The task force was charged with studying money laundering trends, monitoring legislative, financial and law enforcement activities taken at the national and international level, reporting on compliance, and issuing recommendations and standards to combat money laundering.

At the time of its creation, the organization had 16 original members. The FATF Secretariat is housed at the headquarters of the OECD in Paris. In its first year, the FATF issued a report containing forty recommendations to fight money laundering more effectively. These standards were revised in 2003 to reflect evolving patterns and techniques in money laundering. In 2001 the purpose expanded to act on terrorism financing. In February 2012, the FATF codified its recommendations and Interpretive Notes into one document and included new rules on weapons of mass destruction, corruption and wire transfers.

FATF monitors countries' progress in implementing the FATF Recommendations by ‘peer reviews’ (‘mutual evaluations’) of member countries.

Website: http://www.fatf-gafi.org/

2. INTRODUCTION:

Iris Global FZCO, hereafter may be referred as “Iris Global FZCO, Company, Organization, Entity, We, us”,

Iris Global FZCO maintains high standards of professional, social, business ethics and relationship with regulators, customers, peers, developers, and other internal and external stakeholders.

Iris Global FZCO understands that the business activity of the company is highly Vulnerable to Money Laundering and Terrorist Financing Risks due to the fact that:

Precious Metal and Stones (PMS) represent high intrinsic value in a relatively compact form, tend to maintain (or even increase) value over time, and can be easily transported physically in many forms.

Precious Metal and Stones can be used both as means to generate criminal proceeds (i.e., through various predicate offences), as well as vehicles to launder them.

Precious Metal and Stones can be used for illicit purposes, including ML/TF, in a variety of ways, either directly (through physical exchange, as a form of currency) or indirectly (through exchange of value via various formal and informal financial systems, as well as via international trade and the financial products and services related to it)

There are large, well-established, decentralized, and often cash-based markets for certain types of precious metals and stones (particularly for gold and diamonds, but for other PMS as well), often allowing them to be traded or exchanged with relative anonymity.

In its relentless efforts to exercise caution in all its transactions, organization have planned to implement policies and procedures and provide suitable trainings to its staff for the awareness and implementation of guidelines as issued by the Ministry of Economy on AML/CFT.

This internal policy is based on the guidelines issued by the Ministry of Economy for DNFPBs and Supplemental Guidance for Dealers in Precious Metals and Stones in the UAE, and other international recommendations and practices by FATF.

3. GOVERNANCE FRAMEWORK:

3.1. Governance Structure for AML/CFT Compliance – Figure 1

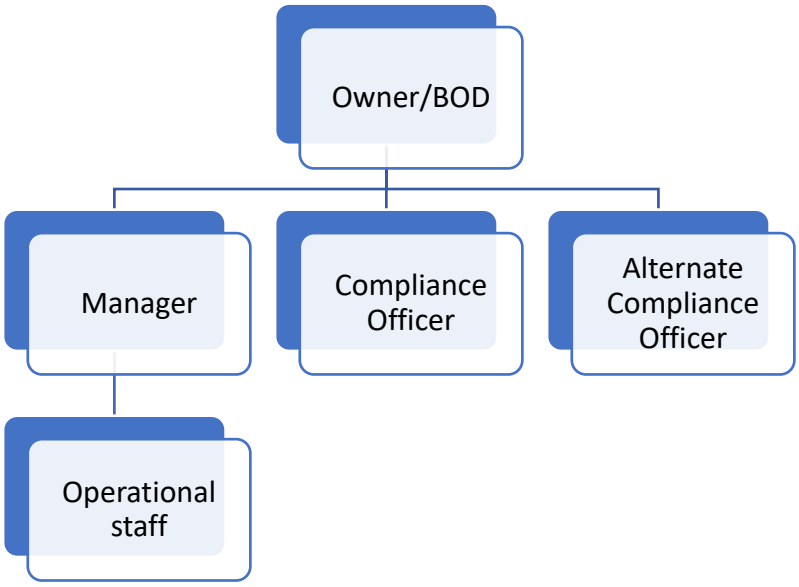


Figure 1: Governance Structure – Iris Global FZCO, as of March 2026

3.2. Roles and Responsibilities:

3.2.1. Management Roles and Responsibilities: Owner

3.2.1.1. Minimum requirements:

Owner of Iris Global FZCO must undertake and govern the compliance activities and functions in Iris Global FZCO.

Following Functions Shall be undertaken by the Owner:

- Undertake a risk assessment which identifies the vulnerability of the company to be used to launder money or finance terrorists.
- Based on the risk assessment, implement a risk management framework to ensure that the company is not used to launder money or finance terrorists.
- Ensure that the risk management framework is developed, and sufficient resources being devoted to dealing with higher-risk customers and transactions.
- Ensure that the company has appropriate compliance management arrangements, including the appointment of a compliance officer at management level; and
- Devote sufficient resources to deal with money laundering and terrorist financing, including ensuring that the compliance function is adequately resourced, and that staff receive appropriate and adequate training.

3.2.1.2. Actions required.

Owners Must:

- Carry out a risk assessment, which should be reviewed and updated on a regular basis, identifying where the business is vulnerable to money laundering and terrorist financing.
- Based on the risk assessment, develop internal policies, procedures, and controls to combat money laundering and the financing of terrorism.

- Ensure staff effectively implement the internal policies, procedures, and controls and receive appropriate training; and
- Monitor the implementation of the company policies, procedures, and controls and make improvements where required on the basis of changes to the company`s money laundering and terrorist financing risk assessment or as recommended by the regulatory authority and/or the financial intelligence unit.

3.2.1.3. Responsibilities

Owner is responsible for the effective implementation of a risk framework of money laundering and terrorist financing risk.

The management of risk needs to be reviewed and updated from time to time to reflect changes in the company`s strategy or other factors such as changes to the law.

Policies and procedures should consider risk factors relating to the customer, product and service, delivery channel, and geographic location of the customer.

Where higher risks are identified, based on the Company`s risk assessment, the staff must take extra measures and senior management should ensure that the staff fully understand and implement the requirements of the policies and procedures.

3.2.2. Management Roles and Responsibilities – Compliance Officer

The Anti Money Laundering Officer is responsible for the following actions:

- Receiving inputs from staff and making suspicious transaction reports to the financial intelligence unit and regulatory authority.
- Developing and maintaining the anti-money laundering and counterterrorist financing policy and internal procedures of the company in line with regulatory requirements.
- Assisting the management in developing and maintaining an effective anti-money laundering and counterterrorist financing compliance culture.
- Ensuring adequate documentation of the Iris Global FZCO risk management policies regarding prevention of money laundering and terrorist financing, risk assessments, and their application.
- Determining and updating, in consultation with the senior management, a risk-based approach regarding money laundering and terrorist financing and the risk assessment of the Iris Global FZCO customers, products, services, delivery channels, and geographic reach.
- Ensuring that all internal suspicious activity reports received are investigated without delay.
- Submitting suspicious transaction reports to the financial intelligence unit (FIU)through goAML System
- Providing initial and updated training for all relevant staff, including all staff who handle transactions, and customer receipts and payments transactions.
- Providing awareness training to the staff and the senior management.
- Ensuring that the staff are aware of and complying with their obligations under the law and the Iris Global FZCO policies and procedures and that the basis for the risk-based approach to managing money laundering and terrorist financing risks is understood and applied.
- Presenting reports to the Owner, making recommendations, if any, for action to remedy any deficiencies in the policies, procedures, systems, or controls and following up on those recommendations.

4. AML/CFT GUIDELINE AND PROCEDURES:

4.1. Customer Due Diligence Process.

Iris Global FZCO as dealers in precious metals and stones should carefully consider the following factors while conducting any business relationship with a natural person/Individual, legal entity, or a corporate customer such as;

- Customer Risk:
  Whether the counterparty or customer is a physical person, a legal person, or a legal arrangement, if a legal person or arrangement, whether part of a larger, more complex group; and whether there is any association with a Political Exposed Person (PEP)—particularly in relation to whether the party appears to be acting on their own or at the behest of a third party, and whether their knowledge and experience level in regard to the product or service and transaction type is appropriate.

- Geographic Risk:
  Country of origin of the product, particularly in relation to whether the country is a known production or trading hub for the type of precious Metals and Stone; has adequate regulations and controls (for example, is a participant in the Kimberley Process Certification Scheme (KPCS) for rough diamonds); is a High-Risk Country (e.g., is subject to international financial sanctions, has a poor transparency or corruption index, or is a known location for the operation of criminal or terrorist Organization's).

  Country of origin or residence status of the counterparty or customer (whether a UAE national or a foreign customer, and in the case of the latter, whether associated with a High-Risk Country).

- Channel Risk:
  Channel by which the counterparty/customer is introduced (e.g., referrals versus walk-in, international versus domestic, in-person or via the internet or other media) and communicates (e.g., remote, or personal contact, direct or indirect through a proxy).

All the above factors to be assessed while onboarding a customer as part of Risk Assessment factors.
PEP checks on its customers to include verifying details related to

- Close relatives: these include any individual who is identified to be the PEP's parent, parent-in-law, stepparent, spouse, ex-spouse, children, stepchildren, adopted children and their spouses, siblings, step-sibling, adopted sibling and their spouses, spouse's siblings and their spouses.
- Close associates include: a natural person who is closely connected to the politically exposed person, either socially or professionally.
- A person who has an account relationship with the PEP and who is not an immediate family member of the PEP.
- A person appointed to advise the PEP in matters of public policy (e.g., political adviser, national security adviser etc.).
- A person in a position to influence a PEP.
- A person who is given the mandate to act on behalf of the PEP.
- A joint beneficial owner of a legal entity or legal arrangement with the PEP, excluding those who are merely providing advisory services in a professional capacity.
- A sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for the benefit of the PEP, excluding those who are merely providing advisory services in a professional capacity.
- Prominent members of the same political party, civil organization, labor or employee union as the PEP.

- Person who is connected with the PEP e.g., through joint membership of a company board.
- For all PEPs and close relatives or associates of PEPs, the compliance team will ascertain the impact of the political connection on the client's Source of Funds, the corruption risk of the country where the PEP held his / her PEP appointment (with reference to the corruption perception index and other adverse media reports), the probability of criminal proceedings and the potential impact on the company's reputation.
- If a customer, or a UBO, is a PEP the company will:
- Classify the PEP as high risk
- Conduct a thorough risk assessment ton the PEP taking into consideration the following for the PEP:
  Source of Wealth (SOW) & Source of Funds (SOF).
- Obtain the approval of the Client Acceptance Committee to commence or continue the business relationship with the customer.
- Increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious.

The Enhanced Due Diligence (EDD) Measures asper AML/CFT Decision point number 6.4 the Articles 4.2(b), 7.2, 15, 22, 25) of AML/CFT and illegal Organizations Guidelines for Designated Non-Financial Businesses and Professions of March 2021 provides guidelines for undertaking appropriate measures related to EDD, Wherein EDD shall be conducted on high risk customers and transactions including PEP related transactions

The EDD measures involve a more rigorous application of CDD measures, including elements such as:

1. Increased scrutiny and higher standards of verification and documentation from reliable and independent sources with regard to customer identity.
2. More detailed inquiry and evaluation of reasonableness in regard to the purpose of the Business Relationship, the nature of the customer's business, the customer's source of funds and source of wealth, and the purpose of individual transactions.
3. Increased supervision of the Business Relationship, including the requirement for higher levels of management approval, more frequent monitoring of transactions, and more frequent review and updating of customer due diligence information.

   EDD means that DNFBPs should intensify their measures & specific measure related to involvement of any cash related transactions or virtual/digital currency-based transactions if going to be conducted, specifically by obtaining further evidence and supporting documentation. DNFBPs should obtain additional information and evidence from high-risk customers such as:

   o Source of funds (revenue) and source of wealth;
   o Identifying information on individuals with control over the customer (legal person or arrangement), such as signatories or guarantors;
   o Occupation or type of business;
   o Financial Statements;
   o Banking references;
   o Domicile;
   o Description of the customer's primary trade area and whether international transactions are expected to be routine;
   o Description of the business operations & the anticipated volume of currency and total sales, and a list of major customers and suppliers; and Explanations for changes in business

activity. Obtaining senior management written approvals for all high risk and cash related transactions

In addition, DNFBPs should also apply specific EDD measures in case there are doubts about the accuracy or appropriateness of a customer's ML/FT risk classification in order to determine the appropriate risk classification. EDD should also be applied when there are red- flag indicators of potentially unusual or suspicious transactions or activities. In all cases in which EDD is applied, DNFBPs should ensure that they take reasonable measures to obtain adequate, substantiated, information about the customer, commensurate with the level of the risks identified

Following documents to be collected as part of Due Diligence & Enhanced Due Diligence Process:

1. KYC Registration Form (Refer Annexure)
2. National ID of an Individual and all Partner/Shareholders/Owners/UBO.
3. Passport copy of an Individual and all Partner/Shareholders/Owners/UBO.
4. Aliases or "aka" names or any other known names for natural/ legal entities to be checked, if any
5. Business Registration License Copy with Online Verification QR code or in absence attested by UAE Embassy from the respective country.
6. Permanent Residential Address of an Individual and all Partner/Shareholders/Owners/UBO.
7. Tax Certificate if any in case of a Legal Entity.
8. Memorandum of Association / Articles of Association in case of legal entity.
9. Annual Audited Financial Statement to understand business volumes and turnover of the company if the volumes are more than the usual transactions.
10. Collecting, identifying, and verifying UBO's/Ownership details in any other business activities to assess risk of Proliferation Financing Risks and dealing into dual goods/technologies which may be used for dealing in WMD (Weapons for Mass Destruction)

Procedure to onboard a Customer

Following documents to be collected as part of Due Diligence & Enhanced Due Diligence Process:
UBO's means .,as per Articles (5) of Cabinet Decision No.(58) of 2020 & article (9) of the cabinet decision No (10) of 2019, beneficial owner of the legal person shall be whoever person that ultimately owns or controls, whether directly through a chain of ownership or controller by other means of control such as the right to appoint or dismiss the majority of its Directors , 25% or more of the shares or 25% or more of the voting rights in the legal Person)

4.2. Name Screening & Targeted Financial Sanctions (TFS) & PF Measures:

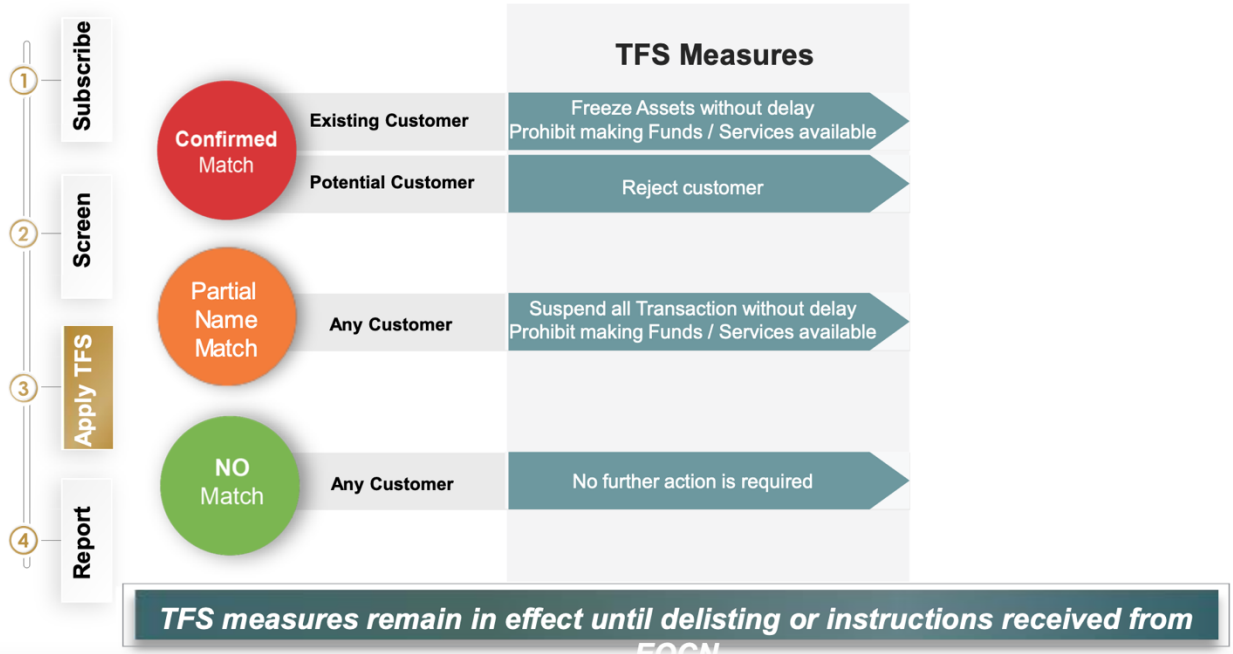
Iris Global FZCO is registered for the updates at https://www.uaeiec.gov.ae/ for Local Terrorist List and UN Consolidated list.

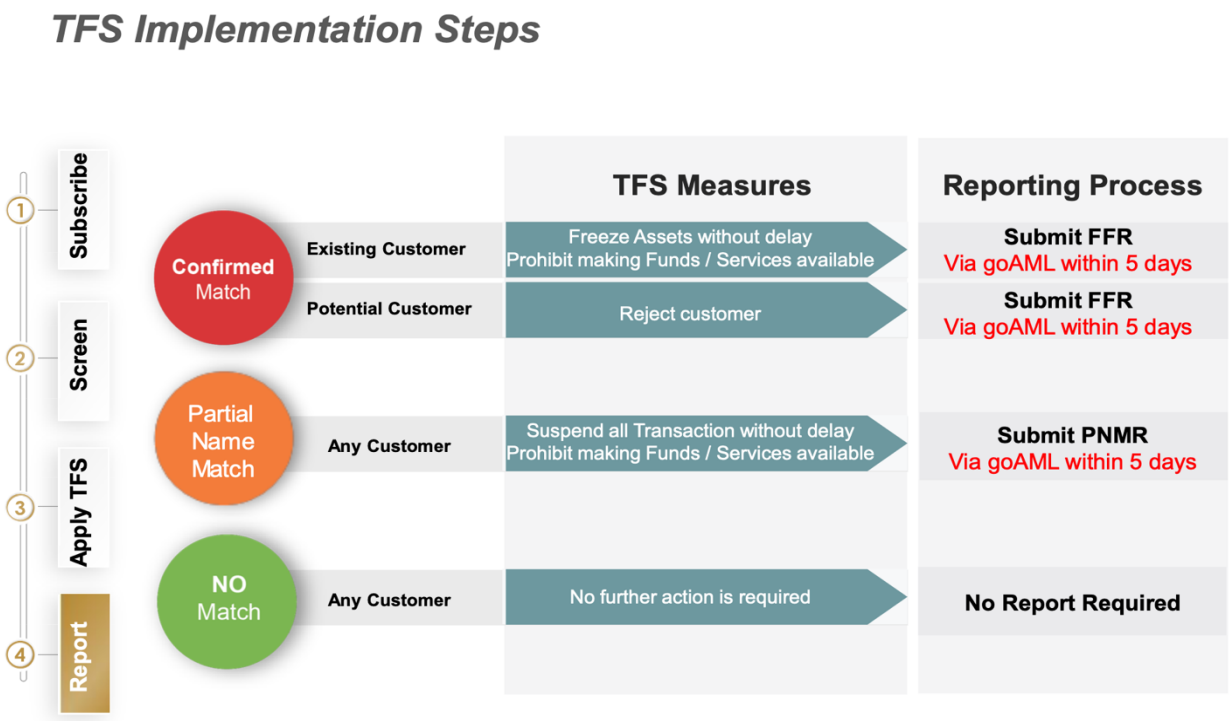
As a DNFBP, Iris Global FZCO owes a responsibility towards the screening names and addresses against UN Consolidated Sanctions and Local list which is compiled and updated on a regular basis and kept in records for the purposes of identifying designated and prohibited individuals and entities, PEPs and other high-risk entities who may pose a threat to the international community at large. Name screening should be done for all the customers of the organisation and for all the onboarding of the relations and related parties.

There are four main obligations on all persons, natural or legal in the UAE to implement Targeted Financial Sanctions (TFS)

TFS Implementation Steps

Depending on the type of match, the following TFS measures should apply:





4.2.1. Requirements:

- Iris Global FZCO should follow the strict adherence to the name screening on each transaction and ensure that no transaction is done with the customer's name that appear in any list (of known specially designated nationals (SDN) or suspected terrorists or terrorist organizations or any blacklist or posing risk of Proliferation Financing provided by the UAE Regulatory Authorities.
- Iris Global FZCO ensures that the Name Screening is done on a regular and transactional basis, including on aliases names "aka", which means other known names
- Iris Global FZCO has an automatic name screening system which can be integrated with the core system for a real time basis, scans, and filters names of each customer and beneficiary against the sanctioned list.
- In the event that there is a possible match of a customer name with that of the blacklist, there is a provision to put the transaction on hold.
- The details of the name match on the SDN list are checked against details of the customer and beneficiary.
- In the event of an exact match i.e., it is determined that the name is on the blacklist or on TFS list, the transaction is withheld and immediately reported to the Financial Intelligence Unit & EOCN with FFR (Fund Freeze Report) and if Potential match is identified then the transaction is suspend and PNMR is reported via GoAML system to the regulatory authority, if any other matches on any other list STR/SAR is reported via GoAML system following the internal risk controls without tipping-off the customer.
- Iris Global FZCO understand that the failure to report the same could result in fines, penalties, reputational and commercial loss.
- In the event the details of the customer do not match with the SDN list, the transaction and onboarding is released for further processing.
- The blacklists should be updated on a regular basis to avoid omission of names which may be recently added or deleted by the above-mentioned authorities.
- It is recommended to subscribe for alerts from OFAC, UN, EU, and other relevant paid sources.
- Iris Global FZCO maintains its internal watch list for addition and deletion of the persons with whom the company does not want to deal with according to the risk he/she may expose the company to

any risk, also conduct searches on google to check adverse or negative news on its customers as a part of its EDD process and take due senior management approval in such cases.
- Any name screening that Identifies as PEP or on sanctioned list is escalated for the approval of the owner with the detailed EDD on the customer.
- The Logs related to the screening of the transactions should be kept for 5 years from the date of transaction for records.

4.3. ISTR and SAR/STR Procedures:

As a primary requirement of submitting Suspicious Transaction Reports (STR), Iris Global FZCO has obtained access to goAML, the online STR reporting portal of the Central Bank. The Licensed Person may contact the FIU or the AML Department at Ministry of Economy for appropriate guidance to obtain access to the STR reporting portal.

All employees of the Iris Global FZCO are obliged personally to report, when there are reasonable grounds to suspect that the funds are proceeds from criminal activity or to be used for money laundering, terrorism or terrorist act or terrorist financing, to the compliance officer. The compliance officer will conduct proper investigations and update the highest authority and raise suitable STR/SAR's. (SARs are generally reported for attempted transactions in case of any suspicion)

A single Suspicious Transaction Report (STR) can help stop the flow of illegal money and help prevent the repercussions of financial crime. Further, these reports are an essential contribution to the development of the financial intelligence resources that are used by country's law enforcement, revenue, and national security agencies. Thereby, we file STRs to ensure that the Iris Global FZCO is not used to aid the transfer of illegal money for money laundering and terrorism financing.

4.3.1. Procedures:

- All employees are required to report any potentially suspicious or unusual transactions.
- The reporting must be done with full facts of the case within reasonable time.
- It is company`s obligation to investigate the background and purpose of transactions deemed to be 'unusual' and to set forth our findings in writing, even in the event, it is not considered necessary to report the transactions to FIU as suspicious. As is the case of other documents these findings should also be maintained for inspection by the competent authorities for a period of at least five years.
- The Compliance Officer shall conduct in depth investigation and take an appropriate action before reporting such transactions to Financial Intelligence Unit.
- It is important to note that the "time factor" in reporting suspicious transactions remains crucial; if we are able to retrieve / submit the relevant information, it will help regulatory authority and Law enforcement authorities to effectively review and take effective measures to combat money

laundering, terrorism financing or any other illegal activity.

- Attempted Transactions are obliged to report transactions through GoAML system, which appear as an attempt to launder money and / or finance a terrorist organization and / or a terrorist activity, Terrorism Financing.

In case of doubt that a transaction might be meant for terrorism or terrorist organizations or for terrorism purposes, we should freeze the transaction / account and inform the financial intelligence unit in writing immediately.
All Employees should strictly comply with the following if a transaction created at your end / found in the system seems suspicious to you:

a. Do not inform the customer of your suspicions about his/her transaction(s), and action being taken by you.
b. Hold the transaction and report immediately to your Compliance Officer.
c. Forward copy of Customer identity and transaction copy to Compliance Officer
d. Hold or block the transaction and do not proceed.

Institutions which fail to report unusual and suspicious transactions shall be penalized in accordance with the prevailing laws and regulations, such incidents should be immediately reported to the authorities through the proper systems.

4.3.2. Tipping Off:

All suspicious transactions must be kept fully confidential, and no one should inform any person or customer that his/her transaction is being reported as a suspicious transaction to the FIU.

Non-compliance is a criminal offence, and the employee involved shall be terminated, immediately and additionally he/she is personally subject to a fine or imprisonment or both.

It is a criminal offence for an employee to tip off, tell or inform any person including customers that any of their transactions is being scrutinized for possible involvement in suspicious money laundering operations or terrorist financing.

4.4. Red Flags, Unusual, Suspicious Customer and Transactions

The company has a documented list of red-flags indicators for suspicious transaction as required by the Article (16) of Cabinet Resolution No. (10) of 2019.

Few key indicators of suspicious Customers and Transactions are: -

4.4.1. The Business Relationship, Counterparty, or Customer:

- Suddenly cancels the transaction when asked for identification or information.
- Is reluctant or refuses to provide personal information, or the DPMS has reasonable doubt that the provided information is correct or sufficient.
- Is reluctant, unable, or refuses to explain:
    - their business activities and corporate history.
    - the identity of the beneficial owner.
    - their source of wealth/funds.
    - why they are conducting their activities in a certain manner.
    - who are they transacting with?
    - the nature of their business dealings with third parties (particularly third parties located in foreign jurisdictions).
- Is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information (such as allegations of corruption or criminal activity) in reliable publicly available information sources.

- Is a designated person or organization (i.e. is on a Sanctions List).
- Is related to, or a known associate of, a person listed as being involved or suspected of involvement with terrorists or terrorist financing operations.
- Insists on the use of an intermediary (either professional or informal) in all interactions, without sufficient justification.
- Actively avoids personal contact without sufficient justification.
- Is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Is a foreign national with no significant dealings in the country, and no clear economic or other rationale for doing business with the DPMS.
- Is located a significant geographic distance away from the DPMS, with no logical rationale.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate a transaction, or is unfamiliar with the details of the requested transaction.
- Makes unusual requests (including those related to secrecy) of the DPMS or its employees.
- Is prepared to pay substantially higher fees than usual, without legitimate reason.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Is conducting a transaction which appears incompatible with their socio-economic, educational, or professional profile, or about which they appear not to have a good understanding.
- Uses legal persons, legal arrangements, or foreign private foundations that operate in jurisdictions with secrecy laws.
- Requests services (for example, smelting and reshaping of gold into ordinary-looking items, or re-cutting and polishing precious stones) that could improperly disguise the nature of the PMS or conceal beneficial ownership from competent authorities, without any clear legitimate purpose.
- Claims to be a legitimate DPMS but cannot demonstrate a history or provide evidence of real activity.
- Is a business that cannot be found on the internet or social business network platforms (such as LinkedIn or others)
- Is registered under a name that does not indicate that activity of the company is related to PMS, or that indicates activities different from those it claims to perform.
- Is a business that uses an email address with a public or non-professional domain (such as Hotmail, Gmail, Yahoo, etc.).
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have Authorized the transaction.
- Is incorporated or established in a jurisdiction that is considered to pose a high money laundering, terrorism financing, or corruption risk.
- Has a complex corporate structure that does not appear to be necessary or that does not make commercial sense.
- Appears to be acting according to instructions of unknown or inappropriate person(s).
- Conducts an unusual number or frequency of transactions in a relatively short time period.
- Asks for short-cuts, excessively quick transactions, or complicated structures even when it poses an unnecessary business risk or expense.
- Request's payment arrangements that appear to be unusually or unnecessarily complex or confusing (for example, unusual deposit or installment arrangements, or payment in several different forms), or which involve third parties.

- Provides identification, records or documentation which appear to be falsified or forged.
- Requires that transactions be affected exclusively or mainly through the use of cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or other such payment methods), or through virtual currencies, for the purpose of preserving their anonymity, without adequate and reasonable explanation.

4.4.2. Transactions:

- Involves the use of a large sum of cash, without an adequate explanation as to its source or purpose.
- Involves the frequent trading of PMS (especially diamonds and gold) or jewelry for cash in small incremental amounts.
- Involves the barter or exchange of PMS (especially diamonds and gold) or jewelry for other high-end jewelry.
- Appears structured so as to avoid the cash reporting threshold.
- Involves delivery instructions that appear to be unnecessarily complex or confusing, or which involve foreign jurisdictions with no apparent legitimate connection to the counterparty or customer.
- Includes contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Involves payments to/from third parties that do not appear to have a logical connection to the transaction.
- Involves merchandise purchased with cash, which the customer then requests the merchant to sell for him/her on consignment.
- Involves PMS with characteristics that are unusual or do not conform to market standards.
- Involves the unexplained use of powers-of-attorney or similar arrangements to transact business on behalf of a third party.
- Appears to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Involves a person acting in the capacity of a director, signatory, or other Authorized representative, who does not appear to have the required competency or suitability.
- Involves persons residing in tax havens or High-Risk Countries when the characteristics of the transactions match any of those included in the list of indicators.
- Is carried out on behalf of minors, incapacitated persons or other categories of persons who appear to lack the mental or economic capacity to make such decisions.
- Involves several successive transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- Involves recently created legal persons or arrangements, when the amount is large compared to the assets of those legal entities.
- Involves foundations, cultural or leisure associations, or non-profit-making entities in general, especially when the nature of the merchandise or the characteristics of the transaction do not match the goals of the entity.
- Involves legal persons which, although incorporated in the country, are mainly owned by foreign nationals, who may or may not be resident for tax purposes.
- Involves unexplained last-minute changes involving the identity of the parties (e.g., it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction.
- Involves a price that appears excessively high or low in relation to the value (book or market) of the goods, without a logical explanation.
- Involves circumstances in which the parties: – Do not show particular interest in the details of the

transaction; – Do not seem particularly interested in obtaining a better price for the transaction or in improving the payment terms; – Insist on an unusually quick completion, without a reasonable explanation.

- Takes place through intermediaries who are foreign nationals or individuals who are nonresident for tax purposes.
- Involves unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of clients with a similar profile.
- Involves indications that the counterparty does not have or does not wish to obtain necessary governmental approvals, filings, licenses, or other official requirements.
- Involves any attempt by a physical person or the controlling persons of a legal entity or legal arrangement to engage in a fraudulent transaction (including but not limited to over- or under-invoicing of goods or services, multiple invoicing of the same goods or services, fraudulent invoicing for non-existent goods or services; over- or under-shipments (e.g., false entries on bills of lading); or multiple trading of the same goods and services).

4.4.3. The Payments:

- Involves cash, cash equivalents (such as cashier's cheques, gold certificates, bearer bonds, negotiable third-party promissory notes, or similar instruments), negotiable bearer instruments, or virtual currencies, which do not state the true payer, especially where the amount of such instruments is significant in relation to the total value of the transaction, or where the payment instrument is used in a non-standard manner.
- Involves unusual deposits (e.g., use of cash or negotiable instruments, such as traveler's cheques, cashier's cheques, and money orders) in round denominations (to keep below the reporting threshold limit) to pay for PMS. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Is divided into smaller parts or installments with a short interval between them.
- Involves doubts as to the validity of the documents submitted in connection with the transaction.
- Involves third-party payments with no apparent connection or legitimate explanation.
- Cannot be reasonably identified with a legitimate source of funds.

4.5. KYE

Know Your Employee policy should be conducted have the following stages.

a. Pre- Employment Stage
b. Course of employment
c. Employee Conduct

4.5.1. Pre – Employment Stage:

Due diligence in KYE starts at the recruitment stage, to know if the promising candidates are telling the truth.

At the initial stage references should be checked, reference check can be done by the organization or by outsourced agencies.

References of a prospective employee - You can verify if there is any criminal conviction; this can be achieved by getting.

- A police clearance certificate from the police station of the last known residences.
- The relieving letter from the previous employer is taken.
- The past employer can be asked to provide few details like; did they really work for that

company stated on the CV? Employment credentials such as designation, role, compensation, conduct and reason for leaving will be ascertained.
- How was their conduct of the prospective employee?
- References provided by the prospective employee can be requested to provide information which the prospective employee has stated on the resume' or job application.
- The references given by the candidate shall be contacted & affirmed. (First degree relations should not be hired)
- In case the verification or background check services are provided by a vendor, Company must ensure the standards & procedures the organization applies while conducting the check. Are their standards comparable to yours? Are there procedures reviewed by an independent firm.
- Screening of Employee names against the sanctions list

4.5.2. Course of Employment:

Even though the reference checks have been applied, it is advisable to have random checks to ensure that the employee maintains its responsibility to be a trustee of the organization. It is good management practice to monitor your employees' performance and understand what makes them stick, but this routine procedure can also unearth internal threats to your business.

4.5.3. Employee Conduct:

Signs which could raise a signal for verifying the employees conduct and behavior: -

- Staff Behavior: A change in the employee's lifestyle, especially when the spending etc. by an employee sees a drastic change then what an employee at the same level could afford.
- Credit cards/Loans: the employees availing frequent loans and credit cards should pose a question for the employer. Too many approvals and NOCs provided to employees can not only lead to defaults but can also cause the organization to be blacklisted for getting further benefits from banks etc.
- Overzealous nature and relation with select customers; There could be possibilities of Customers offering bribes and commissions to employees for conducting frauds, embezzlements and money laundering, Frequent checks, and controls on the activities of employees can help detect these activities at an early stage.
- Timing: Many a times employees employed in critical areas of operations and accounts have been caught for internal frauds etc. These employees have been reported to have long working hours, coming early before the time to office and sitting till late in office.
- Compromising on data & system integrity: employees who have often been reprimanded for misuse of confidential data and systems should be monitored closely for mitigating any risk of fraud.

5. REGULATORY REPORTING

As a DNFBP and registered Authority Iris Global FZCO has obligation to report transactions in GoAML System for the following transactions:

5.1. Transactions With Individuals

- All **Cash transactions** with individuals equal or exceeding AED 55,000.00 needs to be reported in the GoAML System.
- Exceptions: (Not to Report) – Any Credit Card /Cheque or Bank Transfer transactions of any amount. Only if Suspicious then to be reported through STR Option in GoAML System.

5.2. Transaction with Legal Entities

- All Cash/ International Wire Transfers / Transfers through Exchange Houses or Remittance Companies equal or exceeding AED 55,000.00 need to be reported in the GoAML System.
- All Settlements in USD with following qualifications.
    - Both Entities having accounts in UAE and transfers done for USD payments.
    - USD Settlements done between two Free zones Within UAE, having different bank accounts, and settlements between Free zone and onshore companies registered in the UAE.

Exceptions: (Not to Report)

- AED Settlement where both the parties have accounts in same bank in the UAE.
- AED Settlement where both the parties have accounts in different banks in the UAE.
- USD Settlement where both the parties have accounts in same bank in the UAE.
- Trade between related parties Mainland to Free zone having same bank account transactions and vice versa.
- Barter transaction (Exchange of Gold)
- Intra Company Transactions
- Transaction not routed through the UAE Bank Account.

6. INDEPENDENT REVIEW:

A robust AML Compliance program shall be complete where a periodic review to assess the adequacy the policies & procedures, compliance officer's functions and other controls is performed.

The purpose of independent review is to review and test whether the policies, procedures & controls are in line with the regulatory guidelines and to suggest changes and modifications in procedures to have more effective controls in the fight against money laundering and terrorism financing.

6.1. Guidelines:

Both internal & external audits play an important role in evaluating the procedures of Iris Global FZCO.

a. External Audit: means testing of the internal procedures by an independent party i.e., performed by people not from within the company. The auditors must be sufficiently qualified to ensure that their findings and conclusions are reliable. It is advisable to conduct the independent testing by an external audit firm shall be on an annual basis.

b. Internal Audit: these audits may be performed internally within an organization if there is a provision of an internal audit department or could be outsourced to the efficient partners.
    - There should be a well-defined audit program & checklist.
    - The frequency of such audits may be once in 6 months.
    - The auditor should report directly to the Owner for its findings.

6.2. Scope:

- Examine the adequacy of CDD policies, procedures, and processes, and whether they comply with internal requirements.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations

(products, services, customers, and geographic locations) on sample testing basis.
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program if any.
- Reviewing policies, procedures, and processes for suspicious activity monitoring.
- Determining the system effectiveness for reports, blacklist screening, flagging of unusual transactions and more.
- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures, and processes for referring unusual or suspicious activity from all business lines to the personnel or department responsible for evaluating unusual activity.
- Assess the adequacy of recordkeeping.

7. TRAINING:

The role of AML & CFT training in a dynamic business environment is to be a partner to the employees to help them achieve their objectives. This is achieved by developing the knowledge and skills of the employees. The success of learning, results from its integration with the business plan and the business culture. Hence the prime objectives for Training are:

- To enhance existing knowledge & skills of employees to enable them to successfully accomplish their duties and responsibilities.
- To upgrade the Product Knowledge of Front line / Operations & Sales Staff.
- To adhere to the guidelines of the regulatory authority on employee training.

7.1. Mandatory Teams for Trainings:

7.1.1. New employees – Induction Training

Newly joined employees need to undergo Induction program covering AML/CFT awareness and company`s procedural guide, within fifteen days from joining. This can be conducted internally by the qualified staff from AML/ Compliance Department or through external vendor having expertise in trainings and AML/CFT Knowledge.

7.1.2. Front Line Staff – Induction and Refreshers Training.

All sales staff acts as a first line of defense for AML/CFT program and needs to be trained on an annual basis. These training can be conducted internally by the qualified staff from AML/ Compliance Department or through an external vendor having expertise in trainings and AML/CFT Knowledge.

7.1.3. AML Compliance Department – Continuous Professional Development.

All the employees and members related to AML/Compliance Department shall undergo a Continuous professional development program every year. These trainings can be earned through:

a. AML/CFT conferences or meetings or workshops whether inside or outside the UAE.
b. Face to face training by external agencies whether inside or outside the UAE.
c. Training by industry associations or regulatory bodies; and
d. Web based training

7.1.4. Auditors:

Auditors acts as a third line of defense for AML Program, hence the need to undergo an Awareness and Assessment Training program to audit the operational and AML program implementation of the

company. It is advised to conduct an external training program for auditor's minimum once in a year.

7.1.5. Senior Management – AML Awareness Program.

Senior Management and Owners should undergo AML Awareness, Governance and Risk Framework, Latest updates on laws and regulations, minimum once in a year. These trainings shall be organized through the external agencies.

7.2. Topics:

The topics for AML & CTF training should focus on the different levels of employees, i.e., whether the employee is a customer facing employee, a supervisor, or a clerical employee.

The medium and topics of training should be made available as per the nature of the role an employee is working in. The training mediums may be in the form of classroom sessions, circulars, e-learning modules, corridor specific trainings, role plays.

The topics should include:

7.2.1. General information:

Background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important.

7.2.2. Legal framework:

How the AML Laws apply to institutions and their employees.

7.2.3. Responsibility:

Responsibility of the employees under local laws and regulations for obtaining sufficient evidence of identity, recognizing, and reporting knowledge or suspicion of money laundering and terrorist financing.

7.2.4. Penalties:

For anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment.

7.2.5. Other Topics:

How to react when faced with a suspicious client or transaction & Procedure for reporting of suspicious transactions, how to respond to customers who want to circumvent reporting requirements and Internal policies, such as customer identification and verification procedures and :

- CDD policies.
- What are the legal recordkeeping requirements?
- Red flags.
- Suspicious transaction reporting requirements.
- Duties and accountability of employees.
- Fraud Prevention.
- Tipping off.

8. RECORD KEEPING:

Records should be kept and made available to Regulatory examiners and for investigation for a minimum of 5 years. The objective for records keeping is to ensure that the company can provide the basic information to reconstruct the transaction undertaken, at the request of the relevant authorities.

8.1. Document retention:

The records prepared and maintained by the company must be such that:

- The requirements of the law and expectations of the regulator or the supervisor are fully met; and Auditors, reporting accountants, and regulators or supervisors are able to assess the effectiveness of Iris Global FZCO`s AML/CFT policies and procedures.
- Any transaction or instruction conducted through the NBFI on behalf of any individual customer can be reconstructed.
- Any customer or underlying beneficial owner can be properly identified.
- All suspicious transaction reports received internally, and those submitted to the financial intelligence unit, can be identified; and
- The company can meet, within the required time frame, any inquiries or court orders from the appropriate law enforcement agencies.

8.2. How long should records be retained?

- The minimum periods for which records must be maintained to comply with the requirements of the law are outlined in the following table.

Type of Account	Length of Retention
Account opening records and documentary evidence of identity.	At least 5 years after Account Closure.
Account ledger records.	At least 5 years.
Individual transaction records.	At least 5 years.
Results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, usual large transactions).	At least 5 years after Account Closure.
Information after the account has been closed or after the last transaction.	At least 5 years.
AML Training registers.	At least 5 years.

Records relating to a customer's identity must be retained for at least 5 years from the date of closure of business with the client. The date on which the relationship with a customer end is the date of:

- Carrying out a one-off transaction or the last in the series of transactions; or
- Ending of the business relationship, that is, the closing of an account.

9. FINES AND PENALTIES

As per Federal Decree – Law (20) of 2018;

The Regulator has the authority to impose the following administrative penalties on the financial institutions, designated nonfinancial businesses and professions and non-profit organizations in case they violate the present Decree-Law and its Implementing Regulation:

a) Warning.

b) Fines of no less than AED 50,000 (fifty thousand dirham) and not more than AED 5,000,000 (five million dirham) for each violation.
c) Banning the violator from working in the sector related to the violation for the period determined by the regulatory authority.
d) Constraining the powers of the Board members, supervisory or executive management members, managers or owners who are proven to be responsible of the violation including the appointment of temporary inspector.
e) Arresting Managers, board members and supervisory and executive management members who are proven to be responsible of the violation for a period to be determined by the Supervisory Authority or request their removal.
f) Arrest or restrict the activity or the profession for a period to be determined by the supervisory authority.
g) Cancel the License.

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.

As published in 2024 updated as below:

The list Annexed to Cabinet Resolution No. (71) of 2024 Concerning the Unified List of Violations and Administrative Fines Imposed on Violators of Measures for Confronting Money Laundering and Combating the Financing of Terrorism Subject to the Control of the Ministry of Justice and Ministry of Economy

In all the cases, the Regulatory Authority shall publish the administrative penalties through various means of publication from time to time.

No.	Legal Reference	Violation	Administrative Fine Amount (AED)	
			Minimum	Maximum
1	Article (20) of the Executive Regulation.	Failure to set policies, measures and internal controls approved by the top management with the aim to combat committing crimes.	100,000	200,000
2	Article (20) of the Executive Regulation.	Internal policies and procedures are not consistent with the crime risks and the nature and size of the facility, or failure to update them continuously.	50,000	100,000
3	Article (20) of the Executive Regulation.	Failure to apply internal policies, procedures, and controls to a branch of the facility or a subsidiary company in which facility holds a majority stake.	50,000	100,000
4	Article (20) of	Failure to include any of the	50,000	200,000

	the Executive Regulation.	provisions listed in Article (20) of the Executive Regulation in the internal policies, procedures, and controls.		
5	Article (4) Para (1/B) of the Executive Regulation.	Failure of the facility to take necessary measures and procedures to identify, assess, understand, document, and continuously update crime risks in its field, as well as to provide such information upon request.	50,000	500,000
6	Article (4) Para (1/A) of the Executive Regulation.	Failure of the facility to consider all relevant risk factors, such as risks of customer. States, geographical regions, products and services, operations, and delivery channels of services and products before determining the overall risk level and the appropriate level of risk mitigation measures that will be applied.	50,000	500,000
7	Article (4), Clause (2) of the	Failure of the facility to undertake the actions and	50,000	1,000,000

	Executive Regulation.	procedures necessary to mitigate the risks identified based on the results of the National Risk Assessment or the self-assessment process given the nature and scale of the violator's business.		
8	Article (23) of the Executive Regulation.	Failure of the facility to identify and assess the risks that may arise in the violator's field of work when developing the services that the violator offers or when conducting new professional practices through its facility.	50,000	500,000
9	Article (6), Clauses (1, 2, 3, 4 and 5) of the Executive Regulation.	Failure to undertake the necessary customer due diligence measures before establishing the business relationship or performing a casual transaction in favour of the customer that is equal to or more than (AED 55,000), whether it is a sole or multiple transactions that seem connected, or upon making casual transactions in the form	50,000	200,000

		of telegraph transfers equal to or more than (AED 3,500) or when suspicion exists about the crime, data validity or sufficiency to identify the identity of the customer that was previously obtained.		
10	Article (5), Clause (2) of the Executive Regulation.	Failure of the facility to conduct risk management procedures with respect to circumstances where a customer would benefit from the business relationship before the verification process.	100,000	500,000
11	Article (8), Clauses (1) and (2) of the Executive Regulation.	Failure to verify - using documents or data from a reliable and independent source - of the customer identity and the real beneficiary or his deputy before or during the establishment of the business relationship or the account opening, or before conducting a transaction for a customer with whom he has no existing business relationship.	50,000	200,000

12	Article (8), Clauses (3, 4) of the Executive Regulation.	Failure to take necessary measures to understand the purpose, their nature, and nature of the business relationship of the customer and the structure of ownership as well as controlling the customer, or failure to obtain information related to such purpose whenever needed.	50,000	200,000
13	Article (9) of the Executive Regulation.	Failure to take reasonable measures to address crime risks arising from customer and the business relationship to identify and validate the beneficial owner of legal persons and legal arrangements.	50,000	200,000
14	Article (16) of the Decree-Law.	Failure of the facility to keep the information obtained through the execution of due diligence measures.	50,000	200,000
15	Article (4), Clause (2/B) of the Executive Regulation.	Failure to take enhanced due diligence measures to manage high-risk when identified.	100,000	500,000

		owner is foreign or citizen, a politically exposed person or an individual who has previously held a prominent position in an international organization.		
19	Article (7) of the Executive Regulation.	Failure of the facility to conduct ongoing auditing and monitoring of the continuing business relationship to ensure that documents, data, or information obtained under customer due diligence measures are up-to-date and relevant. This occurs through reviewing the registers and books, especially the registers and books of high-risk customer categories.	50,000	500,000
20	Article (19) of the Executive Regulation	Failure to abide by measures and procedures when relying on a third party to conduct customer due diligence measures.	50,000	200,000
21	Article (16) of the Executive	Failure of the facility to develop indicators to detect potential	50,000	500,000

	Regulation.	criminal activity to report suspicious transactions and to continuously update such indicators according to the development and diversification of methods to commit such suspicious transactions, while complying with instructions issued by supervisory authorities or the Unit in this respect.		
22	Articles (15) and (17) of the Decree-Law.	Failure of the facility to promptly submit reports of suspicious transactions and investigations to the Financial Intelligence Unit upon suspicion, based on reasonable grounds or suspicion that a crime was committed, or failure to provide any additional information the Unit requests.	100,000	500,000
23	Article (17), Clause (1), and Article (20), Clause (2) of the Executive	Failure of the facility to register at the electronic system approved at the Financial Information Unit.	50,000	200,000

	Regulation.			
24	Article (21) of the Executive Regulation.	Failure of the facility to appoint a compliance officer who has the appropriate competence and expertise to perform his duties.	50,000	200,000
25	Article (21) of the Executive Regulation.	Failure of the facility to enable the compliance officer to perform any of the duties stipulated in Article (21) of the Executive Regulation.	50,000	500,000
26	Article (24), Clauses (1), (3) and (4) of the Executive Regulation.	Failure of the facility to keep any of the records, documents and data stated in the Decree-Law or the Executive Regulation, or to organize them in a manner that allows re-analysis and reconstruction of individual transactions, data analysis, and tracing financial operations according to the specified periods, or the failure to make the same promptly available for relevant entities upon request.	50,000	200,000
27	Article (16) Para	Failure to promptly apply	100,000	1,000,000

	(1/E) of the Decree-Law. and Article (60) of the Executive Regulation.	decisions issued by the concerned authority in the State with respect to execution of UN Security Council's resolutions issued under Chapter Seven of the UN Charter to prevent and suppress terrorism and its financing, prevention and suppression of mass destruction weapons proliferation and suspension and its financing and other relevant resolutions.		
28	Article (18) of the Executive Regulation.	Disclosing, directly or indirectly, to the customer or any other person(s) that they have reported or are intending to report suspicious transactions, or the information and data relevant to such transactions, or that there is an investigation thereto.	100,000	500,000
29	Article (39) of the Executive Regulation.	Contacting the customer, whether directly or indirectly, to inform the customer with	100,000	500,000

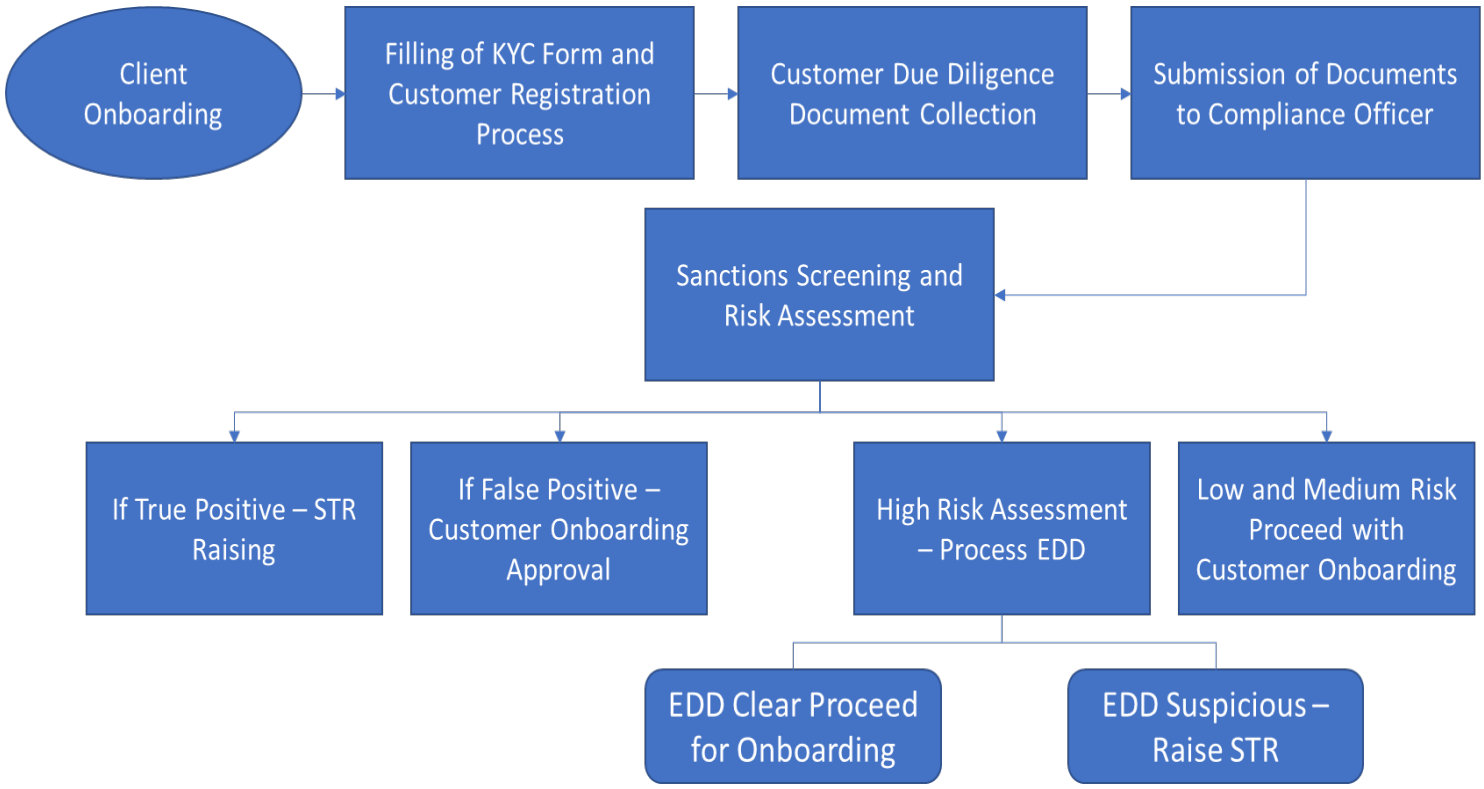
		the procedures that were conducted concerning the latter without a written request from the relevant supervisory entity.		
30	Article (14) of the Executive Regulation.	Dealing with shell banks in any way, whether through opening bank accounts, or accepting funds or deposits from such banks.	200,000	1,000,000
31	Article (14) of the Executive Regulation.	Open or keep bank accounts under nickname, pseudonym or fake name, or with numbers other than their owners names.	200,0000	1,000,000
32	Article (44) of the Executive Regulation.	Failure to comply with the instructions, regulations, and forms concerning crime combating set by supervisory authorities, or failure to respond to request for information regarding the verification of compliance with the provisions of the Decree-Law, the Executive Regulation and the resolutions issued in implementation thereof from	50,000	1,00,000

		the part of the facilities under control.		
33	Article (21) Clause (1) of Cabinet Resolution No. (74) of 2020.	Failure of the facility to register at the website of the Executive Office for Control and Non-Proliferation with the aim of receiving notifications related to the new designation, re-designation as well as updating or de-listing notifications issued by the Security Council, the Sanctions Committee, or the Council of Ministers.	50,000	1,000,000
34	Article (21) Clause (2) of Cabinet Resolution No. (74) of 2020.	Failure to constantly verify databases and transactions and compare them with the names on the lists issued by the Security Council, the Sanctions Committee or the local lists, as well as upon being informed of any changes in any of these lists.	50,000	1,000,000
35	Article (21) Clause (3) of Cabinet Resolution No.	Failure of the facility to freeze funds under the local penalties list and the local lists promptly when any match appears and	500,000	1,000,000

36	Article (21) Clause (4) of Cabinet Resolution No. (74) of 2020.	Failure of the facility to enforce the decision to cancel the freeze, in compliance with the relevant Security Council resolutions or Cabinet decisions regarding the issuance of local lists.	50,000	100,000
37	Article (15) Clause (21) Para (5/1) of Cabinet Resolution No. (74) of 2020.	Failure of the facility to promptly report to the Executive Office for Control and Non-Proliferation with respect to freezing procedures taken.	50,000	100,000
38	Article (15) and Article (21) Para (5/B) of Cabinet Resolution No. (74) of 2020.	Failure of the facility to promptly report to the Executive Office for Control and Non-Proliferation upon determining any match with the designated persons or organizations, details of their data and the actions taken in compliance with the requirements set by the related Security Council Resolutions or Cabinet decisions and the local lists, including transactions that are being attempted.	100,000	1,000,000
39	Article (21) Paragraphs (5/C and D) of Cabinet Resolution No.(74) of 2020.	Failure of the facility to promptly report to the Executive Office for Control and Non-Proliferation if the facility one of its former customers or any occasional customer dealt with is a person or organization included in the Sanctions List or the local lists, or when there is suspicion that a current or former customer, or someone associated with the facility, is listed or has a direct or indirect connection with the listed person.	100,000	1,000,000
40	Article (21) Paragraph (5/E) of Cabinet Resolution No. (74) of 2020.	Failure of the facility to promptly report to the Executive Office for Control and Non-Proliferation upon failure to take any action due to similarity of names and in case removing that similarity has failed through available or accessible information.	50,000	1,000,000
41	Article (21) Clause (6) of Cabinet Resolution No.(74) of 2020.	Failure of the facility to set and apply internal policies, controls and procedures pursuant to provisions of the aforementioned Cabinet Resolution No. (74) of 2020.	100,000	1,000,000

10. ANNEXURE

10.1. Flow Chart - Onboarding of Customer Process



all customers are screened during pre-onboarding & onboarding stages, during every transaction stage, also wherein any changes to the profile of the customer is identified and during any updations to the sanctions list itself

As per the Implementation guide for DNFBP's on Customer Risk-Assessment (CRA) issued in November 2024 Version 0.3.1.1 can be referred in detail:

Below mentioned are few snapshots for understanding & illustration purposes wherein., the compliance team and senior management shall ensure to implement its compliance program to further enhance its Risk Based Approach and Assessment of its institution and customers risk assessments

Customer Risk Assessment vs. Institutional Risk Assessment:

The customer risk assessment focuses on evaluating the risk that individual or corporate clients present in relation to ML/TF/PF. The CRA's include identifying high-risk clients, adjusting monitoring and due diligence procedures accordingly, and mitigating specific risks associated with them. This involves analyzing customer characteristics, behaviors, transaction patterns, and geographic risks to assess the likelihood of involvement in financial crimes. This assessment helps determine the appropriate level of due diligence and monitoring required, especially during customer onboarding and periodic reviews. On the other hand, the Institutional Risk Assessment (IRA), focuses on assessing

the institution's overall risk of exposure to ML/TF/PF (not the individual risks) by taking into consideration a wide range of internal and external factors that may impact the institution's overall performance and stability such as, industry-specific risks, operational processes, internal policies, regulatory Compliance, and the effectiveness of existing AML/CFT policies and procedures. It aims to ensure that the organization can successfully prevent, detect, and respond to threats of money laundering and terrorist funding, the institutional risk assessment seeks to identify and reduce risks at the institutional level. Both CRA and IRA are essential components of an organization's comprehensive risk management framework, but they serve different purposes. While CRA is focused on the customer level, IRA addresses risks at the institutional level. It is important for organizations to regularly conduct both assessments and align them with national risk assessments and sector-specific requirements to ensure an integrated approach to risk management.

This guidance will focus on the customer risk assessment (CRA), for more information about the institutional risk assessment, please refer to the comprehensive Guidance for the DNFBPs available on the website of ministry of economy.

What is CRA:

A CRA is a risk-based assessment that DNFBPs need to undertake for their clients (or prospective clients). This risk assessment must, at minimum, factor in the type of customer (individual or corporate) prior to moving forward through the next steps of your organization's due diligence processes, jurisdiction of the customer, purpose and intended nature of the customer's business, the beneficial ownership transparency (the complexity of the legal structure and controls of the ownership of the customer), the product and/or

service offered, and the delivery channel. The result of the CRA determines the customer's risk rating.

Customer Risk Factors:

The following are the risk factors that must be taken into consideration when conducting a comprehensive CRA

Customer Risk	Geographic Risk	Product/Services Transaction Risk	Delivery Channel Risk	Other Risks, that may be applicable
				

By applying the RBA, DNFBPs can enhance the efficiency of their AML/CFT controls and

ensure that their resources are focused on areas of greatest risk.

Steps for implementing an effective CRA?

Step 1: Define Risk Factors

Establish the factors that will be used to assess risk, this includes, but not limited to (Customer Risk Factors, Geographic Risk Factors, Product/service/transaction type Risk Factors, Delivery Channel Risk Factors, Other Risk Factors.).

Step 2: Establish Risk Levels

Define a scale for assessing the risk levels associated with each factor. A common approach

is to use a scale6 from 1 to 5, where:

- 1 = Low Risk
- 2 = Low- Medium Risk
- 3 = Medium Risk
- 4 = Medium -High Risk
- 5 = High Risk

Example for risk scores given when dealing with Resident & Non-resident customers

Factors under "Geographic Risks"	Risk Score	Factors under "Geographic Risks"	Risk Score
Non-resident from High Risk countries (FATF Black list/ Under UN sanctions)	(5)	Resident customer from high risk countries (FATF Black list)	(4)
Non-resident from Countries Under Increased Monitoring (FATF's Grey ist)	(4)	Resident customer from Countries Under Increased Monitoring (FATF's Grey List)	(3)
Non -resident from low risk countries	(3)	Resident customer from low risk countries	(2)
Non-resident holding UAE nationality	(2)	Resident customer holding UAE nationality	(1)

Step 3: Create the Risk Matrix

Set up a matrix to represent the risk levels. The matrix can have risk factors on one axis (rows) and risk levels on the other (columns)

Step 4: Collecting of Information and documentation

Gather relevant information during the onboarding process, including identification documents, source of funds, and business activities, all al information and documentation related to the transaction.

Step 5: Assess Customer Risk/ Categorize Customers

Classify customers into risk categories based on the identified factors using the completed risk matrix of a risk scoring system.

Step 6: Calculate Overall Risk Score

DNFBPs can calculate an overall risk score by averaging the scores from each risk factor, or by assigning weight to each factor based on its importance to your institution.

Step 7: Update your controls

For higher-risk customers, to conduct EDD and apply suitable risk mitigations measures (examples of risk mitigations measures mentioned here under)

10.2. Risk Assessment Process for Money Laundering - Individual

Customer	Category 1	Category 2	High Risk	Medium Risk	Low Risk
Individual	Residential Status	Resident Local			
		Resident Expat			
		Non Resident			
	Nationality	Low			
		Medium			
		High			
	Income Status	Salaried - Investment Matching to Profile			
		Salaried - Investment Not Matching to Profile			
		Business - Investment Matching to Profile			
		Business - Investment Not Matching to Profile			
Delivery Channel	Cash	Cash Transaction			
	ATM Deposit	ATM Deposit Transaction			
	Bank Transfer	Bank Transfer from Own Account and Customer Risk is Low			
		Bank Transfer from Own Account and Customer Risk is Medium			
		Bank Transfer from Own Account and Customer Risk is High			
		Bank Transfer from Third Party Account			

10.3. Risk Assessment Process for Money Laundering - Corporate

Customer	Category1	High Risk	Medium Risk	Low Risk
	Main Land Formation			
Corporate	Free Zone Formation			
	Off Shore Company			
	Shell Company	Prohibited		
Partner Nationality	High			
	Medium			
	Low			
Representative Nationality	High			
	Medium			
	Low			
KYC & EDD Documentation	Documentation Complete- ID Proof's			
	Not Complete Documentation- ID Proof's			
	Third Party Documentation			
Delivery Channel	Cash			
	ATM Deposit			
	Managers Cheque			
	Bank Transfer Matching Investment Profile			
	Bank Transfer Not Matching Investment Profile			
	Third Party Transfer			

10.4. List of Country Risk Ratings for illustration purposes

As for illustration and example following table can be considered, (Basel AML index 2025 - Public edition): https://index.baselgovernance.org/ranking
in conjunction with latest FATF Country list) the compliance team and senior management will use the latest FATF Country list and might choose country matrix risk tables from other independent credible third-party providers (for e.g., knowyourcountry risk ratings or Basel list of high-risk countries or any such in conjunction with FATF list to derive country -risk ratings table, based on internal risk assessment.
https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-october-2023.html
9b07b7b2.pdf country risk rating table scores and ranking
Weblink for updating: https://www.knowyourcountry.com/country-ratings-table

For illustration purpose - Basel AML index country risk score Basel AML Index 2025- Public Edition

The Basel AML Index is an independent annual ranking assessing the risk of money laundering and terrorist financing (ML/TF) across 177 jurisdictions. Published by the Basel Institute on Governance, it aggregates data from publicly available sources covering AML/CFT frameworks, financial transparency, public sector corruption, financial standards, and rule of law. Scores range from 0 (lowest risk) to 10 (highest risk). This annex forms part of the firm's AML Policy and should be referenced when conducting country risk assessments, onboarding decisions, and enhanced due diligence (EDD) procedures.

Risk Classification

Score Range	Risk Band	Description	EDD Trigger
7.00 – 10.00	High Risk	Severe ML/TF vulnerabilities. Weak AML frameworks, high corruption, limited rule of law.	Mandatory EDD
5.00 – 6.99	Medium-High	Notable AML deficiencies, governance concerns or FATF grey-listing.	EDD Required
3.50 – 4.99	Medium-Low	Moderate risk. Some structural weaknesses but functional AML frameworks in place.	Discretionary
0.00 – 3.49	Low Risk	Strong AML/CFT frameworks, high transparency, robust governance and rule of law.	Standard CDD

2025 Index – Key Statistics

Total	High Risk (≥7.0)	Medium-High (5.0–6.99)	Medium-Low (3.5–4.99)	Low Risk (<3.5)	Avg Score
177	12	89	68	8	5.28

#	Country	Score	Risk	#	Country	Score	Risk	#	Country	Score	Risk
1	Myanmar	8.18	HIGH	61	El Salvador	5.65	MED-H	121	Japan	4.73	MED-L
2	Haiti	8.12	HIGH	62	Türkiye	5.65	MED-H	122	Singapore	4.73	MED-L
3	Democratic Republic Of The Congo	7.63	HIGH	63	Pakistan	5.63	MED-H	123	Mauritius	4.65	MED-L
4	Chad	7.56	HIGH	64	South Africa	5.63	MED-H	124	Moldova	4.64	MED-L
5	Equatorial Guinea	7.55	HIGH	65	Bangladesh	5.62	MED-H	125	Canada	4.61	MED-L
6	Venezuela	7.55	HIGH	66	Malaysia	5.60	MED-H	126	Seychelles	4.60	MED-L
7	Lao Pdr	7.50	HIGH	67	Bolivia	5.58	MED-H	127	Saint Lucia	4.58	MED-L
8	Gabon	7.46	HIGH	68	Timor-Leste	5.58	MED-H	128	Samoa	4.56	MED-L
9	Central African Republic	7.44	HIGH	69	Bosnia And Herzegovina	5.54	MED-H	129	Netherlands	4.53	MED-L
10	Guinea-Bissau	7.30	HIGH	70	Indonesia	5.52	MED-H	130	Korea, South	4.51	MED-L
11	Republic Of The Congo	7.27	HIGH	71	Mexico	5.52	MED-H	131	Taiwan (Chinese Taipei)	4.49	MED-L
12	China	7.26	HIGH	72	Tanzania	5.51	MED-H	132	Poland	4.49	MED-L
13	Djibouti	6.93	MED-H	73	Bhutan	5.49	MED-H	133	Switzerland	4.47	MED-L
14	Niger	6.84	MED-H	74	Philippines	5.48	MED-H	134	Belgium	4.46	MED-L
15	Algeria	6.82	MED-H	75	Azerbaijan	5.46	MED-H	135	Argentina	4.44	MED-L
16	Madagascar	6.77	MED-H	76	Saint Kitts And Nevis	5.46	MED-H	136	Ireland	4.40	MED-L
17	Turkmenistan	6.73	MED-H	77	Cape Verde	5.45	MED-H	137	Slovakia	4.38	MED-L
18	Cambodia	6.72	MED-H	78	Guatemala	5.44	MED-H	138	Albania	4.36	MED-L
19	Vietnam	6.69	MED-H	79	Malawi	5.44	MED-H	139	Montenegro	4.33	MED-L
20	Comoros	6.67	MED-H	80	Brazil	5.40	MED-H	140	Georgia	4.32	MED-L
21	Nicaragua	6.61	MED-H	81	Ukraine	5.38	MED-H	141	Austria	4.28	MED-L
22	Papua New Guinea	6.61	MED-H	82	Hong Kong, Sar, China	5.37	MED-H	142	Chile	4.28	MED-L
23	Kenya	6.60	MED-H	83	Senegal	5.36	MED-H	143	Oman	4.25	MED-L
24	Angola	6.55	MED-H	84	Zambia	5.31	MED-H	144	Spain	4.24	MED-L
25	Eswatini	6.51	MED-H	85	Uzbekistan	5.27	MED-H	145	Uruguay	4.23	MED-L
26	Tajikistan	6.44	MED-H	86	Qatar	5.25	MED-H	146	Brunei Darussalam	4.22	MED-L
27	Togo	6.44	MED-H	87	Egypt	5.22	MED-H	147	North Macedonia	4.20	MED-L
28	Guinea	6.43	MED-H	88	Serbia	5.21	MED-H	148	Croatia	4.18	MED-L
29	Suriname	6.42	MED-H	89	Kazakhstan	5.18	MED-H	149	Dominica	4.17	MED-L
30	Cameroon	6.41	MED-H	90	Bahrain	5.16	MED-H	150	Australia	4.13	MED-L
31	Sierra Leone	6.41	MED-H	91	Cuba	5.16	MED-H	151	Botswana	4.12	MED-L
32	Mozambique	6.38	MED-H	92	Guyana	5.16	MED-H	152	Trinidad And Tobago	4.12	MED-L
33	Benin	6.33	MED-H	93	Hungary	5.16	MED-H	153	Liechtenstein	4.11	MED-L
34	Solomon Islands	6.31	MED-H	94	Sri Lanka	5.16	MED-H	154	Belize	4.06	MED-L
35	Mauritania	6.29	MED-H	95	Malta	5.15	MED-H	155	Israel	4.06	MED-L
36	Liberia	6.26	MED-H	96	Ghana	5.13	MED-H	156	Saint Vincent And The Grenadines	4.05	MED-L
37	Mali	6.22	MED-H	97	Bahamas	5.08	MED-H	157	United Kingdom	4.04	MED-L
38	Nigeria	6.18	MED-H	98	Dominican Republic	5.08	MED-H	158	Lithuania	4.03	MED-L
39	Kuwait	6.13	MED-H	99	Colombia	5.05	MED-H	159	Latvia	4.01	MED-L

#	Country	Score	Risk	#	Country	Score	Risk	#	Country	Score	Risk
40	United Arab Emirates	6.11	MED-H	100	Morocco	5.04	MED-H	160	France	3.99	MED-L
41	Côte D'Ivoire	6.05	MED-H	101	Bulgaria	5.00	MED-H	161	Greece	3.99	MED-L
42	Lesotho	6.04	MED-H	102	Costa Rica	4.97	MED-L	162	Antigua And Barbuda	3.98	MED-L
43	Zimbabwe	5.99	MED-H	103	Germany	4.97	MED-L	163	Armenia	3.98	MED-L
44	Thailand	5.98	MED-H	104	Vanuatu	4.97	MED-L	164	Luxembourg	3.97	MED-L
45	Kyrgyzstan	5.96	MED-H	105	Mongolia	4.96	MED-L	165	Nauru	3.88	MED-L
46	Sao Tome And Principe	5.96	MED-H	106	Barbados	4.91	MED-L	166	Portugal	3.83	MED-L
47	Lebanon	5.93	MED-H	107	Ecuador	4.91	MED-L	167	Czech Republic	3.82	MED-L
48	Iraq	5.90	MED-H	108	Paraguay	4.91	MED-L	168	New Zealand	3.76	MED-L
49	Nepal	5.88	MED-H	109	Marshall Islands	4.89	MED-L	169	Norway	3.73	MED-L
50	Saudi Arabia	5.87	MED-H	110	Peru	4.88	MED-L	170	Slovenia	3.49	LOW
51	Panama	5.83	MED-H	111	Grenada	4.85	MED-L	171	Andorra	3.48	LOW
52	Gambia	5.76	MED-H	112	Jordan	4.85	MED-L	172	Sweden	3.48	LOW
53	Burkina Faso	5.75	MED-H	113	United States	4.83	MED-L	173	Estonia	3.25	LOW
54	Uganda	5.72	MED-H	114	Romania	4.81	MED-L	174	Denmark	3.18	LOW
55	Rwanda	5.71	MED-H	115	Jamaica	4.78	MED-L	175	San Marino	3.08	LOW
56	Belarus	5.70	MED-H	116	Namibia	4.78	MED-L	176	Iceland	3.04	LOW
57	Ethiopia	5.68	MED-H	117	Cyprus	4.77	MED-L	177	Finland	3.03	LOW
58	Tonga	5.67	MED-H	118	Italy	4.76	MED-L				
59	Honduras	5.66	MED-H	119	Tunisia	4.75	MED-L				
60	India	5.66	MED-H	120	Fiji	4.73	MED-L				

For detailed Country List Kindly refer to the link below:

As for illustration and example following table can be considered, (Basel AML index 2025 - Public edition): https://index.baselgovernance.org/ranking

https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2026.html

Bulgaria	Burkina Faso - Removed as of 25th Oct 2025	Cameroon	Croatia	Democratic Republic of Congo	Haiti
Venezuela	Mali	Mozambique- Removed as of 25th Oct2025	Nigeria – Removed as of 25thOct 2025	Philippines – Removed from Grey List as of 21st February 2025	Senegal - Removed from Grey List as of 25th Oct 2024
South Africa- removed as of 25th oct 2025	South Sudan	Syria	Tanzania	Monaco	Vietnam
Angola	Bolivia	Kuwait	Lao people's democratic Republic	Cot d'Ivoire	Lebanon
Papua New Guinea	Venezuela	Virgin Islands (UK)	Yemen		
Yemen	Algeria	Haiti	Nepal & Laos – added under grey List as of 21st February 2025		
Kenya	Namibia	Monaco & Venezuela added under Grey List as of 28th June 24 Lebanon, Algeria, Angola, Cote d'Ivoire added under Grey List as on 25th Oct 2024 Bolivia, Virgin Islands (UK), Yemen under Grey List as of 25th Oct 2025 Kuwait & Papua New Guinea added under Grey List as of 13th February 2026 Blacklist High risk jurisdiction subject to call for action under FATF: Democratic People's Republic of Korea, Iran, Myanmar.			
UAE	Uganda	Gibraltar	Barbados	Countries exited from Grey List as June 28th, 2024 – Jamaica & Turkey	

KYC (Know Your Customer) Form/KYS (Know Your Supplier or Vendor)

Section 1 - General Information

Full Company Name:				
Your Business Address:	Office No.			
	Building Name:			
	Street Address:			
	City:		State:	
	Country:		Pin/Zip/Code/P.O.Box	
Telephone No.				
Fax No.				
Email address:				
Expected Business Turnover annually with Company				

Section 2 – Ownership Information

Please state below the details of the owners/partners/managers of the Company.

Full Name:	**Nationality:**	**Contact No.**	**Email Address:**	**PEP Y/N**

Group Company Information

Name of Company:	**Nature of Association:**

Section 3 – Regulatory Information

Trade License Details	Issuing Authority		License No.	
	Issue Date		Expiry Date	
Product Registration Details	Reg. No.		Expiry Date	
Commercial Registration Details	Reg. No.		Expiry Date	
Other Registration Status				

Has your business or has any of its Directors, Principals, or Partners been:		
Currently under any legal proceedings or pending judgment in the Court of Law?	Yes☐	No☐
Convicted of or charged with a criminal offense in past 3 years?	Yes☐	No☐
Found liable for negligence, fraud, wrongful trading, or malpractice?	Yes☐	No☐
Subject to any application for, or declaration of, liquidation, bankruptcy, or similar proceedings or subject to an administrative order?	Yes☐	No☐
Refused license or authorization to conduct business has been suspended, withdrawn, or not renewed?	Yes☐	No☐
Censured, fined, disciplined, suspended, or refused membership by any regulatory body?	Yes☐	No☐

Section 4 – Company Legal Information **(please mention details as applicable)**

Company incorporation/Registration Certificate	Date/year of incorporation	☐ PAN No of Co. ☐Trade License No ☐Business Reg Certificate ☐ Cert. of incumbency	Doc No.
	Doc No.		
☐ VAT Registration No. ☐ Tax Reg No ☐ GST Registration No ☐ Other			Valid till
Industry/Association Membership No (Bourse Membership or Diamond Association Membership)		Source of funds: Purpose of transaction:	
☐ Company directors / ☐ Share Holder(s) / ☐ Manager / ☐ Authorized Signatory			
Name-		Email-	
Designation-		Mobile No-	
☐ Emirates ID ☐ Director Identification No ☐ Passport No ☐Other Document (Pl. Specify)		Valid Till Date-	

Section 5- Ultimate Beneficial Owner Name/ declaration

*Attach Latest Govt./Authority/Share certificate for UBO(s)-1st level & identity proof			
Name of the Person	Share %	Identity No. (Attach Doc.)	ID Type: Passport/PAN/Aadhar/Other

Section 6- Bank Details

Bank Name and Address-		Bank Account Number-	
RTGS/SWIFT Code-		IBAN No-	
Account Type/Currency-		Correspondent Bank Name and SWIFT Code	

Section 7- General Information

Does company adhere to KPCS?	☐Yes ☐No ☐NA	Is the company or group sight holder of DTC/Argyle/Associated with any sight holder group?	☐Yes ☐No ☐NA
Comply with DTC Best Practice Principles?	☐Yes ☐No ☐NA	Does company have and follow AML/CFT Policy?	☐Yes ☐No ☐NA

Responsible precious metal supply chain policy (If dealing in precious metal/jewelry)	
1.Did your company establish a responsible supply chain of gold from conflict-effected and high-risk areas policy which is consistent with the standards set forth in the model supply chain policy in Annex II of the OECD Due Diligence Guidance for responsible Supply Chain of Minerals from Conflict-Affected and High-Risk Areas?	
2.Does your company comply or plan to comply with the OECD Due Diligence Guidance for Responsible Supply Chain of Minerals from Conflict-Affected and High-Risk Areas?	
3.Does the company have a risk-based assessment of its precious metal suppliers/customers? (E.g. Low, medium, high)	

4.Does the company perform enhance due diligence for high-risk precious metal suppliers/customers?	
.Is the company complying with any of the following industries initiatives?	
LBMA Responsible Gold or Silver Guidance	
DMCC Risk-Based Due Diligence Guidance for GPM	
RJC Chain of Custody standard	
WGC Conflict Free Gold Standard	
RMI Responsible Gold Standard	
UAE-MOE's Guidelines on CDD measures for responsible sourcing of Precious Metals & Stones and its supply chain	

Encl: Documents Attached for above KYC/KYS

☐ Trade License copy	☐ Company Pan Card copy	☐ Latest Certificate of Incumbency	☐ Business Registration Certificate
☐ VAT Registration Certificate	☐GST Registration Certificate	☐ TAX Registration Certificate	
---Copy of shareholders /Directors/Manager---	☐ Passport	☐ Visa (if applicable)	☐ Emirates ID ☐ Other ID(Pl. specify)
☐ MOA and AOA	☐ Partnership Document (If partnership firm)	☐ Share Certificate	☐ Extract of Company
☐ Certificate of Registration	☐ Certificate of Incorporation		

I/We hereby confirm to the best of my knowledge and belief that the information contained in this form and any attachment hereto is true and correct. I/ We will timely inform the company: _____ in writing of any subsequent material changes to the information provided herein/ attached hereto. Wherein I hereby explicitly agree to abide by all AML/CFT Laws and Regulations of The UAE and shall cooperate further with the company: _____ to provide certified true copies including any further information which may be required during the course or after exiting my/our business relationship if requested for the purpose of regulatory reporting's.

Name		
Position		
Signature		
Date		Company Stamp

Additional – COMMENTS if any:

POLITICALLY EXPOSED PERSON (PEP) DECLARATIONFORM

The information in this form is collected to comply with the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities requirement.

A politically exposed person (PEP) is an individual who is or who has been entrusted with prominent public functions domestically' or by a foreign country.

Prominent public functions include the following profiles:

1. Head of State or of Government

2. Senior politicians

3. Senior government, judicial or military official

4. Member of ruling royal family

5. Senior executive of state-owned corporation / government linked company6. Important political party official

The definition of PEP includes immediate family members, relatives, adviser, close associates, personal adviser or business associate of an individual as set out in FATF's (Financial Action Task Force) Recommendation 12 and 22 and relevant guidance covered under the UAE AML/CFT Laws and Regulations.

1.Are you a PEP? Yes☐ No☐

2. Is you or the entity related to a PEP? Yes☐ No☐
(Please fill the below questions if the first two questions you answered - yes)

3. If you are or related to a PEP, please indicate the profile and relationship to you:

A. Head of State or of Government ☐ B. Senior politician☐ C. Senior government, judicial or military official

☐ D. Member of ruling royal family☐ E. Senior executive of state-owned corporation / Government linked company☐ F. Important political party official☐ G. Other.....

I hereby declare that the details and information given above are complete and true to the best of my knowledge Name:

Designation:

Date & Signature:

Company Stamp

UBO- Declaration

Date:
Dear Sir/Madam,

UNDERTAKING LETTER

I , Mr/Ms ....., ... National having Passport number ..... , owner & UBO of (mention company name) hereby confirm that neither of our entities nor any of our related parties are dealing with sanctioned countries as may be listed by UAE, United Nations, United States, European Union or the UK , nor Owned or controlled by , or operating as agents of the Governments of Cuba, Iran, North Korea, Myanmar, Syria or Venezuela or Resident or domiciled in Iran, Syria, North Korea, Myanmar, Cuba or Crimea.

I hereby further confirm that all our business operations have never dealt with / won't involve a sanctioned countries (at present Crimea, Cuba, Iran, North Korea or Syria) or violate or to cause any economic or financial sanctions or trade embargoes implemented, administered or enforced by the United Arab Emirates, The United Nations, United States, European Union, United Kingdom or other relevant sanctions authorities.

I also confirm that neither I nor any of key person acting as nominee of any person national / residing any of the above sanctioned countries.

Thanking you,

For & on Behalf of :_____

Abbreviations List:

Abbreviation	Full form
DNFPB	Designated Non-Financial Business
PMS	Precious Metal and Stones
ML/TF	Money Laundering/Terrorist Financing
FIU	Financial Intelligence Unit
PEP	Political Exposed Person
KPCS	Kimberley Process Certification Scheme
UBO	Ultimate Beneficiary Owner
EDD	Enhanced Due Diligence
SAR	Suspicious Activity Report
DPMS	Dealers in Precious Metals and Stones
CDD	Customer Due Diligence
NBFI	Non-Banking Financial Institutions
FATF	Financial Action Task Force
BOD	Board of Directors
NOC	No Objection Certificate
AML Def List	AML Deficiency List