SUPERVISORY GUIDANCE
AML/CFT Guideline for Dealers in Precious Metals and Stones
2025

This Guideline is designed to assist Dealers in Precious Metals and Stonds (DPMS) in understanding and fulfilling their obligations under Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws of Kuwait. It provides sector-specific guidance on identifying, assessing, and mitigating ML/TF risks and implementing the necessary policies, procedures, and internal controls to comply with AML/CFT regulatory requirements and supervisory expectations. This Guideline aligns with international best practices, including recommendations from the Financial Action Task Force (FATF). It provides practical measures to promote a robust AML/CFT compliance culture within the DPMS industry. By following this Guideline, DPMS professionals will be better equipped to:

- Identify and assess ML/TF risks specific to DPMS sector, including high-risk clients, jurisdictions, and transaction types.
- Implement effective customer due diligence (CDD) measures, including identifying beneficial owners and verifying the source of funds.
- Identify and report suspicious transactions to the KwFIU in a timely manner.
- Strengthen internal controls and compliance frameworks to ensure adherence to AML/CFT laws and regulatory obligations.
- Enhance awareness and training among employees to detect and prevent ML/TF activities within the DPMS.

This guideline applies to all DPMS licensed by MOCI.

ML/TF Risks Associated with DPMS Sector

DPMS are recognized by the FATF as a high-risk sector for money laundering (ML), terrorism financing (TF), and proliferation financing (PF) due to the high-value, portable, and easily transferable nature of precious metals and stones. Criminals exploit this sector to store, move, and integrate illicit funds into the legitimate economy, often taking advantage of weak regulatory oversight and informal trading practices. The key risks associated with DPMS include:

1. High Value and Liquidity of Precious Metals and Stones
    a. Precious metals (gold, silver, platinum) and stones (diamonds, rubies, emeralds, etc.) are highly valuable and can be easily converted into cash, making them an attractive vehicle for laundering illicit proceeds.
    b. Large transactions can take place outside formal financial channels, reducing transparency and traceability.
2. Ease of Transportability and Cross-Border Movement
    a. Precious metals and stones can be easily concealed and transported across borders without detection, making them an ideal means of transferring illicit wealth internationally.
    b. Criminals can exploit weak customs controls to move these assets undetected.
3. Use of Cash Transactions and Informal Markets
    a. The DPMS sector is often cash-intensive, particularly in regions where gold and diamonds are traded informally, making it difficult to verify the source of funds.

b. Transactions conducted outside regulated financial institutions pose a higher risk of money laundering and terrorism financing.

4. Exploitation of Complex Supply Chains
    a. The global nature of the precious metals and stones trade means that supply chains often involve multiple intermediaries, dealers, and refiners in different jurisdictions.
    b. Criminals can use shell companies, front businesses, and informal networks to disguise the illicit origin of assets.
5. Links to Terrorism Financing (TF) and Sanctions Evasion
    a. Terrorist organizations may use the trade of gold, diamonds, and other high-value assets to finance their operations, particularly in conflict zones and high-risk regions.
    b. Sanctioned entities and proliferators may use precious metals and stones to bypass financial restrictions and move assets across borders.
6. Dealers may lack awareness or fail to conduct proper due diligence, allowing criminals to exploit loopholes in verification and record-keeping.

Based on the National Risk Assessment of Kuwait, DPMS has been assessed as having medium-high ML risk. Although cash transactions exceeding KWD 3,000 have been prohibited in Kuwait since 2016, the regulatory framework was further strengthened in 2025, when all cash transactions in the DPMS sector were fully banned, regardless of their value.

This legal prohibition significantly reduces cash-related risks for the sector. However, DPMS professionals must remain vigilant and strictly comply with the regulation by refusing to process any transaction involving cash, regardless of the amount. This absolute ban must be enforced as part of DPMS's internal controls and procedures.

Risk-Based Approach

Recommendation 1 of the FATF focuses on assessing risks and applying a risk-based approach. The implementation of a risk-based approach (RBA) is a dynamic process that involves identifying, assessing, and mitigating risks associated with money laundering (ML) and terrorist financing (TF). A risk-based approach necessitates the development of procedures that are proportionate to the assessed risk. Higher-risk areas should be subjected to enhanced procedures as determined through risk assessments. This involves implementing measures like enhanced customer due diligence and transaction monitoring. Areas identified as having a higher risk, such as specific customer segments such as politically exposed persons or high net worth individuals or types of transactions, should be subjected to enhanced measures and controls. This ensures that the level of scrutiny aligns with the identified risk level.

The RBA is flexible and should be tailored to the size, type, and complexity of the DPMS's business. The aim is not to eliminate all risk, but to manage it effectively. DPMS should consider multiple risk categories to identify and assess ML/TF risks.

AML/CFT Controls for DPMS

Business Risk Assessment

As part of their AML/CFT obligations, DPMS must assess their inherent risks—that is, the level of money laundering (ML) and terrorist financing (TF) risk that exists in their business before any internal controls or mitigating measures are applied. This includes evaluating risks related to products, services, customers, transactions, delivery channels, and geographic exposure.

DPMS must establish and document a clear and justifiable methodology for determining both inherent and residual risks. The residual risk is the level of risk that remains after the application of mitigating measures and internal controls. The risk assessment methodology must be:

- Proportionate to the size and complexity of the business,
- Aligned with the risk-based approach,
- Reviewed and updated regularly, and
- Available for inspection by supervisory authorities.

In conducting their risk assessments, DPMS should refer to reliable and relevant sources of information to inform their understanding of ML/TF threats and vulnerabilities. These sources may include:

High-Level sources DPMS professionals can use for conducting Business Risk Assessment

- International guidance & typologies
- Country-level evaluation reports
- Black lists & grey lists
- Sanctions lists
- Topical risk assessments
- Kuwait National Risk Assessment
- Sectorial risk assessments
- Threat & risk assessments of other jurisdictions/ regions
- Communications by competent authorities
- Guidance published by MOCI
- Information from professional sectorial bodies
- Reports from media

Internal Sources for BRA

- Data on customers: numbers, residence, value of activity
- Data on beneficial ownership of customers
- Results of analyses of unusual & suspicious transactions
- Findings of internal or external auditors
- Volume of transactions
- Product range and characteristics
- Reports from compliance
- Exposure to customers active in higher-risk industries/sectors
- Size of the business
- Use of third parties
- Extent of non-face-to-face business

DPMS should ensure they apply a structured and documented process when incorporating external sources into their risk assessments, and the information used must be current, relevant, and periodically reviewed.

When conducting a Business Risk Assessment, DPMS must evaluate the specific money laundering (ML) and terrorist financing (TF) and proliferation financing (PF) risks to which their business is exposed. This includes an assessment of the following core risk categories:

A. Country or Geographic Risk

Geographic risk considers whether any part of a transaction involves a country or region with a higher exposure to ML/TF. This can include:

- Origin of the product (e.g., where gold or gemstones are mined or refined).
- Location of the buyer, seller, or delivery destination.
- Source or destination of funds involved in the transaction.

Higher risk may be present if the country:

- Has limited AML/CFT regulation or enforcement.
- Is subject to international sanctions, embargoes, or trade restrictions.
- Has a high level of corruption or organized crime.
- Hosts terrorist groups or is known for conflict financing.
- Has limited financial infrastructure and relies heavily on cash or informal remittance systems like hawala.
- Is not a participant in the Kimberley Process (for rough diamonds).

Remote mining areas with little regulatory oversight or security, especially those controlled by non-state actors, may also present significant TF risks.

B. Customer and Counterparty Risk

DPMS must understand who they are dealing with. Both retail customers and business counterparties may present higher risks depending on their behavior or profile.

Retail Customers may raise red flags if:

- They insist on paying large sums in cash.
- They involve unrelated third parties in payment or delivery.
- There is an effort to avoid recordkeeping or anonymity.

Dealers should exercise increased caution when counterparties display one or more of the following characteristics. These may indicate elevated money laundering (ML) or terrorist financing (TF) risks at any stage of the value chain examples of the indicators include:

Lack of Business Legitimacy or Knowledge

- Unfamiliar with the industry, trade practices, or standard financial terms.
- Lacks a physical business presence, relevant equipment, or adequate financial capacity.

Unusual or Illogical Transaction Behavior

- Proposes transactions that are excessive or economically irrational (e.g., disproportionate profit, quantity, or quality).
- Makes frequent, unexplained changes in bank accounts or banking relationships.
- Seeks anonymity or refuses to disclose beneficial ownership when it would be commercially expected.

Geographic and Banking Risk

- Based in a location with no clear commercial connection to the trade or dealer.
- Uses unfamiliar or unrelated banks, or money service businesses, without valid justification.
- Engages in cross-border transactions where parties (sender/receiver) do not match the importer/exporter.

Use of Third Parties Without Justification

- Involves third parties to make or receive payments or deliver products without a legitimate business reason.
- Third-party involvement in deposits or payments not aligned with trade norms (e.g., rough or polished diamond transactions).
- Uses intermediaries (e.g., accountants or lawyers) to conduct ordinary business activities.

Payment and Transaction Risk

- Uses cash in non-standard ways or in large amounts.
- Returns advance payments from third parties unrelated to the transaction.
- Conducts payments or receives funds through unrelated or higher-risk sectors (e.g., real estate, automotive, construction, tourism).

C. Product and Service Risk

Certain products and services may present higher risk due to their value, portability, and potential for anonymity:

- High-value, portable items like gold bars or polished diamonds can be easily transported and concealed.
- Gold is of particular concern due to its global liquidity, standardized pricing, and use as a currency alternative.
- Scrap gold, gold dust, or alluvial gold (often mined informally) may carry heightened risk due to lack of oversight and difficulty in valuation.
- Fraudulent or stolen items (e.g., synthetic diamonds misrepresented as natural, or misdeclared gold purity).
- Used jewellery traded in bulk may be harder to trace, especially through pawn shops or informal buyers.

Metal accounts, where gold is stored and transferred like money, and other bank-like services may present less risk if conducted within regulated environments, but their misuse is still possible and must be assessed on a case-by-case basis.

D. Transaction and Financing Risk

The way a transaction is financed and executed also affects its risk level:

- Multiple smaller transactions (structured payments) to avoid reporting thresholds.
- Third-party payments without a clear link to the transaction.
- Use of unrelated or offshore bank accounts, especially from jurisdictions not involved in the trade.
- Payments through money remitters or exchange houses without economic justification.

Even when the customer or product appears low risk, unusual or complex financing methods may indicate attempts to obscure the origin of funds.

Each of these risk categories must be assessed based on the specific context of the DPMS's operations. The assessment should be clearly documented, regularly reviewed, and used to inform internal controls, customer due diligence, and monitoring processes in line with a risk-based approach.

DPMS Business Risk Assessment Table – Examples of the Risk Indicators per Risk Category

Risk Category	Example Risk Indicators	Low Risk	Medium Risk	High Risk
Country/Geographic Risk	Transactions involve high-risk jurisdictions, conflict zones, or sanctioned countries.	Well-regulated, low-risk jurisdictions.	Occasional exposure to moderate-risk countries.	Frequent dealings with high-risk or sanctioned countries.
Customer/Counterparty Risk	Customer is a PEP, has complex ownership, or uses unexplained third parties.	Long-standing, transparent customers with simple structures.	Limited documentation or occasional third-party involvement.	PEPs, anonymous clients, or complex structures without clear purpose.
Product/Service Risk	Dealing in high-value, portable, or untraceable products (e.g., loose diamonds, gold bars).	Low-value, traceable, and regulated products (e.g., certified jewelry).	Moderate-value or semi-traceable products (e.g., scrap metals).	High-value, bulk, or portable products from informal or unregulated sources.
Transaction/Financing Risk	Frequent large cash payments, third-party funding, or use of offshore accounts.	Bank transfers from verified customers; no third-party involvement.	Mixed payment methods (cash + wire); occasional third-party activity.	unrelated third-party funding or delivery.

Customer Risk Assessment

Customer Risk Assessment (CRA) is a key part of the Risk-Based Approach. DPMS professionals must identify and manage risks arising from customer relationships, especially with higher-risk clients. A clear and categorical CRA helps classify customers by risk level and apply appropriate measures to reduce those risks. Key risk factors in a CRA include:

- Geographic Risk: Customers linked to higher-risk countries (e.g., through citizenship, residence, or business) may pose greater ML/TF risks.
- Customer Risk: Clients like Politically Exposed Persons (PEPs) or High Net Worth Individuals often require enhanced scrutiny.
- Product Risk: products that are more vulnerable to misuse for money laundering or financing of terrorism.
- Transaction Risk: Cash payments, third party payments, anonymous methods.

By categorizing customer risks effectively, DPMS professionals can focus resources on high-risk customers and apply appropriate controls to mitigate potential ML/TF/PF threats.

Examples of High-Risk Customer Profiles for DPMS

Politically Exposed Persons (PEPs)

- Individuals holding or having held prominent public positions (e.g., heads of state, ministers, judges, military leaders), including their family members and close associates.
- PEPs are higher risk due to the potential misuse of public funds or influence.

Non-Resident and Cross-Border Clients

- Customers operating from jurisdictions known for high ML/TF risks, secrecy laws, or poor AML/CFT compliance.
- Clients with no clear business or economic link to the country of the DPMS.

Customers Using Unusual Payment Methods

- Transactions involving large amounts of cash, third-party payments, or payments through offshore or unrelated accounts.
- Use of money remitters or non-bank financial institutions without clear rationale.

Customers Seeking Anonymity or Using Intermediaries

- Customers who avoid face-to-face interaction, use lawyers, accountants, or proxies to conduct routine business, or refuse to identify beneficial owners.
- Use of unnecessary third-party delivery or payment instructions.

Customers Involved in High-Risk Activity

- Real estate
- Construction
- Mining and extraction
- Tourism and hospitality
- Automotive trade
- Art and antiquities

New or Unknown Counterparties in Wholesale Trade

- First-time counterparties proposing large or complex transactions, particularly in bulk purchases of gold, diamonds, or other high-value goods.
- Buyers or sellers lacking basic knowledge of the trade or market conditions.

Customers with Complex or Opaque Ownership Structures

- Legal entities with multiple layers of ownership, especially those registered in offshore financial centers or trust jurisdictions.
- Entities unwilling or unable to clearly disclose beneficial owners or controllers.

Customers Involved in Informal or Unregulated Markets

- Buyers or sellers of alluvial gold, gold dust, or scrap metal from informal mining areas with no licensing or regulatory oversight.
- Customers dealing in recycled goods (e.g., pawned or second-hand jewellery) in large quantities without proper documentation.

Customers Making Structuring Transactions

- Individuals or entities breaking up large purchases into smaller amounts to avoid identification thresholds or reporting obligations (e.g., under EUR/USD 15,000 cash limits).

Customers from or linked to Sanctioned or High-Risk Countries

- Any entity or person listed on the UN and domestic sanctions lists.
- Transactions involving goods or payments linked to embargoed territories.

Customer risk should be assessed for all customers with whom the DPMS professional establishes a business relationship or conducts transactions above the specified threshold KWD 3000. This threshold applies to either a single transaction or to several transactions which appear to be linked.

DPMS Customer Risk Matrix Example

This matrix provides examples of customer risk levels (Low, Medium, High) across key factors relevant to DPMS. It is designed to support the risk-based approach to customer due diligence and the identification of higher-risk customer profiles.

Risk Factor	Low Risk Example	Medium Risk Example	High Risk Example
Political Exposure	Private individual with no political connections.	Relative of mid-level public official.	Foreign PEP or their close associate/family member.
Geographic Risk	Customer based in well-regulated FATF member country.	Customer based in country with moderate AML/CFT controls.	Customer located in high-risk or sanctioned jurisdiction.
Payment Method	Bank transfer from personal/business account in same country.	Combination of bank transfer and small cash payments.	Large cash payments or third-party offshore funding.
Use of Intermediaries	Customer deals directly with DPMS and provides full ID.	Use of accountant/lawyer with clear mandate and documentation.	Customer insists on using proxy or refuses to disclose agent.
Sector Association	Employed in low-risk sectors (e.g., education, retail).	Self-employed in loosely regulated trade sector.	Linked to high-risk sectors (e.g., mining, real estate, arms).
Business Relationship	Long-standing client with consistent transaction history.	New customer referred by existing client, limited history.	Unknown/new customer with large one-off transaction.
Ownership Structure	Simple ownership structure with clearly identified owners.	Legal entity with multiple shareholders, all disclosed.	Opaque structure with trusts, shell companies, or offshore links.
Market Type	Deals only in regulated markets with documented sourcing.	Occasional trade in partially regulated markets (e.g. local gold buyers).	Operates in informal/unlicensed markets (e.g., alluvial gold).
Transaction Behavior	Single transaction with clear purpose and documentation.	Transactions slightly structured or split across accounts.	Deliberate structuring to avoid reporting thresholds.
Sanctions	No match to any sanctions or watch lists.	Customer operates in proximity to high-risk regions.	Links with a listed individual/entity on the UN sanctions list.

AML/CFT Governance, Policies and Procedures

Subject to the size, complexity, and nature of their operations, DPMS must appoint a Compliance Officer (CO) responsible for overseeing the implementation and effectiveness of the entity's AML/CFT programme.

The DPMS must ensure that the appointed Compliance Officer:

a) Has full, timely, and unrestricted access to all relevant records, data, and systems necessary to perform AML/CFT duties effectively;
b) Is provided with adequate resources, including time, staff support, and access to training, to fulfil their responsibilities;
c) Receives the full cooperation of all staff, including ownership and senior management, in fulfilling AML/CFT obligations;
d) Possesses the necessary knowledge and expertise, including a clear understanding of the AML/CFT obligations applicable to the DPMS and its staff;
e) Reports directly to the owner or senior management (where applicable), and where applicable, has regular access to and communication with the Board or governing body.

The Compliance Officer should be empowered to challenge decisions, escalate concerns, and ensure AML/CFT risks are properly addressed in accordance with a risk-based approach.

DPMS must establish and implement documented policies, procedures, and internal controls to ensure that all relevant employees understand and comply with their legal obligations under applicable Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) laws and regulations.
These policies and procedures must be:

- Approved by senior management (or the owner, in the case of sole proprietorships);
- Commensurate with the size and complexity of the business;
- Reviewed and updated regularly, in response to changes in the risk environment or regulatory requirements.

Minimum Content Requirements for AML/CFT Policies and Procedures
DPMS must ensure that its written policies and procedures address the following core elements:

1. Risk-Based Approach (RBA)
    - Clear articulation of how the DPMS identifies, assesses, and manages ML/TF risks.
    - Documentation of risk factors considered (e.g., customer, product, geographic, transaction risks).

2. Customer Risk Assessment
    - Having a documented process of Customer Risk Assessment
    - Considering risk indicators for defining risk category of an individual customer
3. Customer Due Diligence (CDD) Measures
    - Procedures for identifying and verifying customers and beneficial owners.
    - CDD requirements for individuals, legal persons, and agents acting on behalf of others.
4. Enhanced Due Diligence (EDD)
    - Definition of high-risk indicators and scenarios that trigger EDD.
    - The nature and extent of additional measures to be taken, including obtaining senior management approval and enhanced monitoring.
5. Identification and Management of Politically Exposed Persons (PEPs)
    - Criteria for identifying domestic and foreign PEPs, including close associates and family members.
    - Risk treatment procedures and documentation requirements.
6. Management of High-Risk Customers
    - Step-by-step process to be followed when a customer is classified as high risk.
    - Requirement for senior management review and approval before establishing or continuing the business relationship.
7. Suspicious Transaction Reporting (STR)
    - Internal procedures for detecting, escalating, and reporting suspicious transactions or attempted transactions.
    - Documentation and confidentiality requirements in line with national law.
8. Targeted Financial Sanctions (TFS)
    - Measures for screening against sanctions lists (e.g., UN, EU, OFAC).
    - Immediate freezing of assets and reporting of matches to the competent authority.
    - Frequency and method of sanctions list updates.
9. Record-keeping
    - List of information/documents to be kept

Structure and Purpose of Compliance Documentation

To promote clarity and accountability, DPMS professionals must distinguish between policies, procedures, and controls:

Component	Purpose	Content Focus	Example
Policies	Define overarching principles, expectations, and AML/CFT obligations.	Strategic intent and ethical standards.	"DPMS commits to identifying and mitigating ML/TF risks through a documented risk-based approach."
Procedures	Provide step-by-step instructions to operationalize policies.	Operational processes and detailed actions.	"Verify customer identity using an official government-issued ID and confirm beneficial ownership before onboarding."
Controls	Serve as checks and tools to enforce compliance.	Monitoring, escalation, and exception handling.	"Transaction over KWD 3000 requires full CDD information."

Implementation and Awareness

- Policies and procedures must be made available to all relevant staff.
- DPMS must ensure ongoing training and communication to support employee understanding and compliance.
- The Compliance Officer is responsible for overseeing the implementation and enforcement of the framework and ensuring alignment with evolving risks and legal requirements.

Customer Due Diligence (CDD)

The outcome of the business risk assessment and customer risk assessment must be used by the DPMS professional sector to determine the extent of measures that are required for CDD purposes. CDD is a crucial element of AML/CFT compliance in the DPMS professional industry.

The Customer Due Diligence (CDD) process consists of two key stages: obtaining information and verifying information. The first step involves collecting specific details from the customer, which will vary based on the type of customer and whether simplified, standard, or enhanced CDD is required, as outlined in paragraph [51]. The second step requires verifying the information obtained, ensuring that appropriate measures are taken to confirm its accuracy. The depth of this verification process depends on the risk level associated with the customer or transaction. For low-risk customers, verification procedures may be less extensive, while for high-risk customers, transactions, or circumstances, a more rigorous and thorough verification process must be undertaken to mitigate potential risks effectively.

Step-by-Step Customer Due Diligence (CDD) Process

DPMS must apply Customer Due Diligence measures in accordance with AML/CFT obligations. The steps below outline when and how CDD should be applied:

Step 1: Identify When CDD is Required

CDD must be conducted in the following situations:

- When establishing a business relationship (i.e., ongoing or repeated transactions);
- When there is suspicion of money laundering or terrorist financing;
- When there is doubt about the accuracy, completeness, or adequacy of previously obtained customer information;
- When conducting occasional transactions of 3,000 KWD or more, whether in a single operation or several linked transactions.

Step 2: Determine the Nature of the Relationship

A business relationship in the context of DPMS refers to any ongoing commercial engagement that extends beyond a single, isolated transaction. DPMS must determine if the engagement is occasional or sustained.

Step 3: Collect Customer Identification Information

For Natural Persons, collect:

- Full name;
- Residential address (including country of residence);
- Date of birth;
- Country of citizenship.

Verification: Use a valid government-issued photo ID showing the name and either the residential address or date of birth.

For Legal Entities or Legal Arrangements, collect:

- Full legal name of the entity;
- Registration number (if applicable);
- Registered address and business address (if different);
- Names of all executive directors (e.g., CEO, CFO, COO);
- Names of individuals who own or control 25% or more of the entity.

Verification:

- Obtain documentation from independent and reliable sources, such as company registries, certified documents, or licenses.
- Use public data for well-established companies where applicable.

Step 4: Understand Ownership and Control in case of legal entities/legal arrangements

- If no individual holds 25% or more ownership, DPMS must still understand the ownership and control structure.
- This includes identifying who exercises effective control and documenting the governance arrangements.

Step 5: Identify the Purpose and Intended Nature of the Business Relationship DPMS must understand:

- The purpose of the transaction (e.g., investment, resale, personal use);
- The source of funds and, when relevant, the source of wealth.

This step is particularly critical for high-value or high-risk transactions, where additional information must be requested and documented.

Step 6: What to do when CDD cannot be completed

If the DPMS is unable to complete CDD due to:

- Non-cooperation by the customer;
- Missing or unverifiable documents;
- Refusal to disclose key information;

Then:

- The transaction must not proceed;
- The DPMS must document the attempt and reasons for failure;
- An STR (Suspicious Transaction Report) should be filed if red flags are present, even when the service is denied.
- Non-cooperation itself may be indicative of potential ML/TF activity.

Summary Table: CDD Requirements for DPMS

Requirement Area	Description	Examples / Notes
When CDD is Required	Establishing a relationship, suspicion of ML/TF, doubt about ID, or transaction ≥ 3,000 KWD	Include linked transactions
Natural Person Identification	Full name, address, DOB, citizenship	Use official ID with photo and either address or DOB
Legal Entity Identification	Name, registration number, addresses, directors, UBOs (≥25%)	Obtain certified or official documents
Verification Documents	Independent and reliable sources	Company registry, government websites, certified copies
Ownership & Control	Understand and verify who controls the entity	Apply a risk-based approach for UBO verification
Purpose of Relationship	Establish why the customer is engaging with DPMS and assess source of funds/wealth	Specifically for high-value or unusual transactions
Inability to Complete CDD	Suspend services and consider STR if CDD cannot be completed or customer refuses to cooperate	Non-cooperation = red flag

Examples when CDD should be applied

Scenario	Onboarding Activities
A walk-in customer buys jewelry worth KWD 5,000	Full CDD required: ID verification, address proof, risk classification, screening for PEP and sanctions
A wholesaler wishes to establish a regular trading relationship	Legal entity verification, beneficial owner identification, transaction profile, SoF/SoW checks, account record setup
A one-time buyer of low-value goods under KWD 3,000	May be eligible for simplified due diligence (SDD)"Applying standard due diligence procedures, including verifying the customer's identity through the Civil ID for residents or a copy of the passport for non-residents."

Enhanced Customer Due DiligencEnhanced

In higher risk situations, DPMS professionals are required to implement enhanced customer due diligence (EDD) and ongoing monitoring measures to address money laundering and terrorist financing risks. In line with the risk-based approach, EDD consist of additional measures which the DPMS professional undertakes to address any heightened customer risk factors. It should be noted that EDD is not a substitution for the CDD process. It is applied in addition to CDD measures. Enhanced measures are mandated in specific cases, as provided for in AML/CFT Law and Instructions but also where the DPMS professional has assessed that the risk of ML or TF is higher.

When is EDD Required?

EDD should be applied in the following cases:

- Customers or transactions involving high-risk countries or jurisdictions;
- Customers identified as PEPs, or close associates or family members of PEPs;
- Complex or unusually large transactions without a clear economic or legal purpose;
- High-risk products or delivery channels, including transactions involving significant amounts of cash;
- When the source of funds or wealth is unclear or inconsistent with the customer's profile.

EDD Measures for High-Risk Countries and Transactions

When a customer is linked to a high-risk jurisdiction or transaction, DPMS must take the following steps:

- Obtain additional information about the customer, including purpose and expected nature of the business relationship;
- Collect detailed evidence of the source of funds (SoF) and source of wealth (SoW);
- Perform adverse media screening and assess jurisdictional risks;
- Obtain approval from senior management to establish or continue the relationship;
- Apply enhanced ongoing monitoring of the relationship.

Enhanced Measures for Politically Exposed Persons (PEPs)

Under AML Law No. 106/2013, PEPs include individuals who hold or have held high-level public positions in Kuwait or abroad, such as heads of state, ministers, judges, ambassadors, political party leaders, and senior military officers. The PEP regime in Kuwait applies to both domestic and foreign PEPs, as well as their family members and close associates.

For PEPs, DPMS must:

- Implement risk management systems to identify whether a customer or beneficial owner is a PEP;
- Screen customers using internal questionnaires and automated or manual AML/CFT databases;
- Conduct background checks, including open-source reviews, subscription tools, or compliance databases;
- Obtain senior management approval to onboard or maintain a relationship with a PEP;
- Verify source of funds and source of wealth using documentary evidence (e.g. bank statements, payslips, contracts);
- Apply enhanced monitoring to detect unusual patterns of transactions.

❗ Note: PEP status must be assessed at onboarding and reviewed regularly during the business relationship. A self-declaration form may assist identification but is not sufficient on its own.

Understanding Source of Funds vs. Source of Wealth

Concept	Description	Examples
Source of Funds (SoF)	The specific origin of the money used for a particular transaction.	Salary, bank loan, sale of property, business transaction receipts.
Source of Wealth (SoW)	The overall origin of the customer's total assets or net worth over time.	Ownership of companies, long-term investments, inheritance, real estate holdings.

In high-risk cases, both SoF and SoW must be verified using appropriate documentation, and findings must be recorded and assessed in relation to the customer's profile.

Summary of Key EDD Measures

EDD Requirement	Application
Identify high-risk scenarios	High-risk countries, PEPs, complex/large transactions
Collect additional customer information	Nature of business, expected activity, occupation
Verify SoF and SoW	Use documentary evidence (e.g., bank records, payslips, contracts, inheritance docs)
Perform PEP screening and background checks	Internal declaration forms, automated databases, open-source checks
Obtain senior management approval	Mandatory before onboarding or continuing high-risk or PEP relationships
Apply enhanced monitoring	Set frequency and parameters based on risk; flag unusual activity

Examples of Scenarios That Trigger Enhanced Due Diligence (EDD) for DPMS

Scenario	Why EDD is Required	EDD Measures to Apply
Customer is a Politically Exposed Person (PEP)	PEPs pose a higher risk of involvement in corruption or abuse of position	Identify whether the customer or beneficial owner is a PEP Obtain senior management approval before onboarding Verify source of wealth (e.g., payslips, asset sales) Verify source of funds used in the transaction Apply ongoing enhanced monitoring
Customer is from or linked to a high-risk country (e.g. sanctioned or FATF-listed jurisdiction)	Countries with weak AML/CFT controls are associated with greater ML/TF risk	Obtain additional information on the customer's identity, business background, and purpose of transaction Request explanation and documentary proof of links to the country Intensify monitoring of transactions
Complex ownership structure with unknown UBOs	Customers may attempt to obscure identity	Identify all layers of ownership and verify beneficial owners

	through shell companies	Request corporate registration documents, organograms Conduct background checks on UBOs Request justification for the complex structure
Customer exhibits suspicious behavior or transactions inconsistent with their profile	Behavioral red flags signal possible illicit activity	Ask for additional explanation Conduct independent background checks Escalate internally for review File an STR if reasonable grounds for suspicion exist
Customer is a new business with no history but proposes a large transaction	Lack of background or trading history increases uncertainty	Request business license, tax registration Verify financial capacity (bank statements, capital documentation) Request references from partners or suppliers
Involvement of third parties in payment or delivery without clear reason	Use of third parties may be a technique to obscure illicit activity	Identify and verify the third party Confirm the business relationship between customer and third party Assess the purpose and legitimacy of third-party involvement

Ongoing Monitoring and Suspicious Transaction Reporting

DPMS professionals must continuously monitor customer relationships and transactions beyond the initial identification. Ongoing monitoring serves a dual purpose: firstly, to ensure the information and documents are up-to-date; secondly, to scrutinize transactions throughout the relationship, aligning them with the DPMS professional's understanding of the customer's risk profile. Through monitoring client transactions and activities, DPMS professionals can:

a) Identify behaviors or transactions that deviate from the usual pattern, do not match the client's profile, or are inconsistent with what is normally expected.
b) Detect suspicious activity that may require filing a Suspicious Transaction Report (STR) with the relevant authority.
c) Assess whether the initial client risk assessment needs to be updated based on new information or unusual activity.

DPMS professionals have a critical responsibility in identifying and reporting suspicious transactions as part of their AML/CFT compliance obligations. They must remain vigilant in detecting potential money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks by conducting thorough customer due diligence (CDD), verifying source of funds and source of wealth, and assessing unusual transaction patterns that may indicate illicit activity. If a transaction appears suspicious, DPMS is required to file a Suspicious Transaction Report (STR) with KwFIU. This process must be conducted promptly and confidentially, ensuring that the client is not tipped off (tipping-off prohibition) about the report. Additionally, brokers must maintain records of suspicious transactions, including supporting documents, to facilitate potential investigations. They are also expected to cooperate with authorities, provide further information when required, and stay informed about emerging ML/TF typologies through regular training. DPMS Responsibilities for ongoing monitoring and STR Reporting include:

Ongoing Monitoring of Customers and Transactions

Once a customer has been onboarded, DPMS professionals must continue monitoring the business relationship. This helps to:

- Keep customer information up to date (e.g. identification documents, business status, ownership);
- Review whether customer transactions make sense based on what is known about the customer;
- Spot any suspicious activity that may require reporting.

Examples of what to watch for in DPMS business:

- A customer who normally buys small jewelry suddenly starts purchasing large amounts of gold bars;
- A client begins paying through a third party without explanation;
- Payments are coming from or sent to high-risk countries or regions under sanctions;
- A legal entity changes its ownership without notice, especially if ownership becomes unclear.

If something doesn't match the expected behavior or the customer's profile, investigate further and assess the need to update the customer's risk rating or file a Suspicious Transaction Report (STR).

Suspicious Transaction Reporting (STR)

DPMS professionals have a legal obligation to report any transaction that seems suspicious or may involve money laundering (ML), terrorist financing (TF), or proliferation financing (PF).

Examples of suspicious activity in the DPMS sector:

- A customer wants to buy high-value diamonds and is willing to pay with large amounts of cash;
- The customer insists on keeping their identity secret or refuses to provide verification documents;
- A deal is structured in an unnecessarily complex way (e.g. involves unrelated third parties, off-shore entities, or multiple intermediaries);
- Funds come from countries with weak AML/CFT controls or under international sanctions.

Steps to Follow When Suspicious Activity is Detected

Responsibility	What DPMS Professionals Must Do
Identify Suspicious Activity	Monitor customer behavior for unusual payments, transaction patterns, or inconsistent documentation.
File an STR Promptly	Submit a report to Kuwait Financial Intelligence Unit (KwFIU) as soon as suspicion arises.
Include Key Details	Ensure the STR is accurate, clear, and includes all relevant facts and supporting documents.
Do Not Tip Off the Customer	Never inform the customer or anyone else that a report has been filed—this is illegal.

Keep Proper Records	Retain documents, communications, and the reasons for filing or not filing an STR.
Retain Records for 5 Years	All records relating to STRs must be kept for at least 5 years.

! For detailed guidance on the STR process, DPMS should refer to MOCI's STR Guidance Note for DPMS.

Ongoing Monitoring & STR Scenario Table – DPMS

Scenario	Example	What to Look For	What to Do
Customer transactions deviate from known profile	The customer initially bought low-value items but suddenly purchases high-value diamonds without prior history	Sudden increase in value or frequency of purchases	Ask customer to explain change; verify source of funds – ask what is the origin of funds; update risk assessment
Customer starts using third parties frequently	A customer suddenly requests delivery to a new person every time or uses multiple payers	Inconsistency in delivery/payer info	Identify third party; ask for justification and documents; escalate if suspicious
Use of foreign bank accounts unrelated to customer	Payment comes from a foreign company or account not previously linked to customer	Bank info doesn't match ID or past records	Ask for proof of connection;
Refusal to provide SoF/SoW or other requested info	Customer hesitates or refuses to explain source of funds	Evasive behavior or delays in providing documents	Pause the transaction; document issue; file STR if concerns remain
Customer linked to high-risk country or sanctioned individual	Transaction involves shipping to or receiving payment from a high-risk country	Links to jurisdictions under UN or local sanctions	Screen customer and counterparties; freeze if required; report to Chapter VII committee
Customer shows signs of structuring transactions	Customer breaks up large purchase into multiple transactions under KWD 3,000	Repetitive amounts below the CDD threshold	Record pattern; file STR
Customer changes explanation frequently	First says it's a personal gift, then says it's a resale item	Inconsistent information	Ask follow-up questions; verify purpose with documents

Negative news on customer (adverse media)	News article links customer to financial crimes or political corruption	Public info contradicts declared profile	Conduct deeper screening; reassess customer risk; escalate and consider STR
Attempted transaction by a sanctioned person	Screening system flags customer as being on UN or local TFS list	Match with designation list	Do not proceed; freeze funds if applicable; report immediately to Chapter VII Committee; no tipping off

Targeted Financial Sanctions

DPMS professionals, as Designated Non-Financial Businesses and Professions (DNFBPs), are required to implement Targeted Financial Sanctions (TFS) measures in accordance with legal and regulatory obligations. These measures are essential in preventing the misuse of transactions for money laundering (ML), terrorism financing (TF), and proliferation financing (PF). To ensure compliance with Article 35 of the Ministerial number 5\2020 ، DPMS professionals must undertake the following key actions:

Screen and Monitor Designations

- Continuously monitor updates to the UN Consolidated Sanctions List and the National Special Committee designations.
- Sign up for and use the automatic alert system provided by the Special Committee to stay informed of new or updated designations.
- Regularly (and immediately after any update) screen all customers, beneficial owners, transactions, and business relationships against the updated lists.

Identification and Freezing of Assets

- Immediately identify and freeze any funds, assets, or economic resources belonging to designated persons or entities.
- If a match is found or suspected, report immediately to the Special Committee, whether the individual is a current, former, or attempting customer.
- Do not proceed with the transaction or relationship until the case is assessed.

Confidentiality and Prohibition of Tipping Off

- It is strictly prohibited to notify the customer, beneficial owner, or any third party that a freezing measure is being or will be applied.
- Breaching this obligation is considered a serious offense and may result in enforcement action.

Internal Controls and Cooperation

- Develop and implement internal policies and procedures that ensure compliance with TFS obligations.
- Maintain records of all screenings, matches, and reports filed with the Special Committee.
- Cooperate fully with the Special Committee and supervisory authorities during verifications and inspections.

Summary of Key Responsibilities

Action	Description
Register	Sign up with the Special Committee's automatic alert system to receive real-time updates.
Screen Clients	Use reliable screening tools to regularly screen all customers and beneficial owners against the latest designation lists.
Update Internal Systems	Ensure that internal systems are updated to reflect changes in designations.
Identify and Report	If a customer, beneficial owner, or attempted transaction involves a designated person or entity, report immediately to the Special Committee.
Freeze Assets	Immediately apply a freeze without prior notice and refrain from any transactions involving the person/entity.
Train Staff	Ensure that relevant staff understand TFS obligations and how to apply them.
Maintain Records	Keep detailed records of all screenings, matches, and communications with the Special Committee.

Examples Specific to DPMS

Scenario	What to Do
A customer wants to purchase gold using funds sent from a sanctioned country.	Screen the sender. If matched to a designated person or country, freeze the transaction and report to the Special Committee.
A long-time client becomes listed on the UN or Special Committee list.	Immediately freeze all associated assets and report to the Special Committee. Do not inform the customer.
A third party tries to make a payment on behalf of a customer, and their name appears in adverse media or sanctions alerts.	Screen the third party. If matched, report and freeze any attempted transaction.

Record Keeping

In accordance with the AML/CFT Law and regulatory obligations, DPMS professionals must maintain comprehensive records for a minimum of five (5) years. This applies to both business relationships and occasional transactions and includes customer due diligence (CDD), enhanced due diligence (EDD), and all AML/CFT-relevant activities.

Purpose of Record-Keeping

Maintaining accurate and complete records allows DPMS professionals to:

- Demonstrate compliance with AML/CFT requirements.
- Support investigations by competent authorities.
- Facilitate supervisory reviews.
- Detect and mitigate ML/TF risks through monitoring and follow-up.

Examples of Types of Records to Maintain

Category	What to Maintain
Customer Identification and Verification	- Identification documents (passport, ID, proof of address) - Verification records - Beneficial ownership information - Results of PEP and sanctions screening - Notes or documents related to negative news or inconsistencies
KYC Files	- Internet search records - Customer communications relevant to risk assessment - Information or justifications from the customer - Screening logs and outcomes
EDD Documentation (for high-risk customers)	- All documents collected for verifying Source of Funds (SoF) and Source of Wealth (SoW) - Justifications for high-risk classification - Senior management approvals - Risk scoring and rationale for decisions
Transaction Records	- Invoices, receipts, payment details - Method of payment (e.g. cash, wire transfer) - Dates and values of transactions - Any third-party involvement
Suspicious Transactions	- STRs filed with the Financial Intelligence Unit (KwFIU) - Internal memos or risk analyses - Records of how suspicion was identified

Unreported Suspicious Activity	- Notes on suspicious activity considered but not reported - Reason for not filing STR (e.g. insufficient evidence)
Training Records	- Attendance logs - Training content provided to staff - Dates and topics of AML/CFT sessions
Communication with Authorities	- Correspondence with supervisory bodies or the Special Committee - Records of inquiries or follow-up actions
Monitoring and Reviews	- Records of ongoing due diligence - Monitoring logs - Reviews or updates to customer risk classification

Key Responsibilities of DPMS Professionals

DPMS professionals must:

- Document every step of due diligence and enhanced due diligence (EDD), including the basis for decisions.
- Retain all relevant documentation in organized, retrievable formats.
- Update records regularly, especially when there are changes in customer behavior, business relationship, or risk profile.
- Ensure availability of records for inspection by MOCI.

Training

DPMS professionals must ensure that all relevant employees, especially those involved in customer interactions, compliance functions, or transaction processing, receive regular AML/CFT training that is appropriate to their job functions and risk exposure. The training must be designed to:

- Increase awareness of money laundering (ML) and terrorist financing (TF) risks specific to the DPMS sector;
- Promote understanding of internal AML/CFT policies and procedures;
- Equip staff with practical skills to apply risk-based measures in their day-to-day roles;
- Reinforce the legal and regulatory requirements under national AML/CFT law and ministerial decisions;
- Foster a culture of compliance across the business.

Training Content: Core Topics

Training Topic	Description
ML/TF Risks in the DPMS Sector	- Common typologies and case examples (e.g., bulk cash purchases, trade-based laundering, abuse of third-party payments) - Sector-specific vulnerabilities (e.g., use of cash, international exposure, high-value goods)
Customer Due Diligence (CDD)	- Situations where CDD is required (e.g., transactions >3,000 KWD, suspicion of ML/TF, new business relationships) - Required identification data and documentation for individuals and legal entities - Verification methods and record-keeping
Politically Exposed Persons (PEPs)	- Understanding who qualifies as a PEP (domestic, foreign, international organization officials) - Screening procedures - Reporting and approval process for onboarding PEPs
Enhanced Due Diligence (EDD)	- When and how to apply EDD for high-risk customers (e.g., high-risk jurisdictions, large cash transactions, complex ownership structures) - Documenting source of funds and source of wealth - Role of senior management in approving high-risk relationships
Suspicious Activity and Red Flags	- How to identify red flags (e.g., third-party transactions, inconsistent customer profiles, unusual payment methods) - Steps to take upon identifying suspicious activity - Filing a Suspicious Transaction Report (STR) with the FIU - Tipping-off prohibition

Training Methodology and Frequency

- Training should be tailored to employee roles (e.g., front-line sales, compliance staff, finance and accounting).
- A combination of in-person sessions, virtual webinars, e-learning modules, and practical case studies should be used.
- Training must be delivered at onboarding and refreshed at least annually, or more frequently if there are:
    - Regulatory updates
    - Changes in internal procedures
    - Significant sectoral risks identified by supervisory authorities

DPMS professionals must maintain training logs and attendance records, which should include:

- Date of training
- Topics covered
- Names and roles of participants
- Format (e.g., classroom, online)
- Trainer or provider details

These records should be retained for at least 5 years and be made available during supervisory inspections or audits.

Director of AML-CFT Department :

2025\6\22