



Executive Summary

1. Overarching Commitment & Governance

- The Board of Directors and CEO must actively demonstrate commitment to AML/CFT/CPF/Sanctions compliance specifically within the PMS business line, setting the 'tone from the top'.
- Ensure the appointed Compliance Officer has the necessary independence, authority, and resources (including access to all relevant PMS transaction/client information) to effectively discharge their duties related to DPMS compliance.
- The Board/CEO must formally review and approve this PMS-specific AML/CFT/CPF and Sanctions Policy, related procedures, the Sanctions Compliance Program (SCP), and any subsequent amendments.
- Implement and maintain the 'Three Lines of Defense' model for risk management and control within the PMS operations.
- Regularly review the effectiveness of the PMS AML/CFT/CPF framework, including annual audits where applicable.

2. Risk Management

- Conduct a comprehensive Enterprise-Wide Risk Assessment (EWRA) specifically identifying, assessing, understanding, and mitigating ML/TF/PF risks related to MMT's PMS business (gold, palladium, client types, transaction methods, supply chains, geographies involved). Review and update this EWRA at least annually or upon significant changes to the PMS business or risk landscape.
- Consistently apply a Risk-Based Approach (RBA) across all AML/CFT/CPF processes related to PMS activities, ensuring mitigation measures are proportionate to the identified PMS risks.

3. Client Due Diligence (CDD) & Know Your Client (KYC)

- Implement documented, risk-based KYC procedures to identify and verify the identity of *all* clients, suppliers, and counterparties involved in PMS transactions using reliable, independent sources *before* establishing a business relationship or executing any single or series of linked PMS transactions.
- Identify and take reasonable measures to verify the identity of the Ultimate Beneficial Owner(s) (UBOs) for all legal person/arrangement clients involved in PMS activities, understanding their ownership and control structure, strictly complying with Cabinet Resolution No. (109) of 2023.
- Apply appropriate levels of CDD based on the client's risk profile within the PMS context:
 - Simplified Due Diligence (SDD): Only permitted by law and justified by demonstrably low PMS risk.
 - Standard Client Due Diligence (CDD): For normal risk PMS clients/transactions.
 - Enhanced Due Diligence (EDD): For all high-risk PMS clients, including Politically Exposed Persons (PEPs), clients from high-risk jurisdictions involved in PMS trade, complex structures facilitating PMS transactions, high-value PMS transactions, and other relationships deemed high-risk by the PMS EWRA. Obtain senior management/CEO approval before establishing relationships with high-risk PMS clients or PEPs involved in PMS activities.
- Perform ongoing monitoring of PMS business relationships, scrutinizing transactions to ensure consistency with the client's profile, expected PMS activity, and risk assessment. Keep CDD information current through periodic reviews, especially for high-risk PMS clients.



- Implement a clear policy for prohibiting PMS relationships with certain client types (e.g., shell banks, anonymous accounts, sanctioned parties) and an exit strategy for PMS relationships where risks become unmanageable or required CDD cannot be completed.

4. Politically Exposed Persons (PEPs)

- Implement risk-based procedures to determine if a client, UBO, or counterparty involved in PMS transactions is a PEP (domestic or foreign), a family member, or a close associate.
- Obtain senior management/CEO approval before establishing or continuing a PMS business relationship with a PEP.
- Apply EDD measures to all PMS relationships involving PEPs, including establishing the source of wealth and funds related to the PMS activities.
- Conduct enhanced ongoing monitoring of PMS relationships involving PEPs.

5. Sanctions Compliance & Targeted Financial Sanctions (TFS)

- Develop and implement a robust Sanctions Compliance Program (SCP) specifically addressing risks within the PMS supply chain and transaction lifecycle.
- Screen all clients, UBOs, counterparties, and relevant parties involved in PMS transactions against the UAE Local Terrorist list, UNSC Consolidated List, and other relevant sanctions lists (e.g., OFAC, EU) *prior* to onboarding/transaction execution and on an ongoing basis.
- Implement procedures to immediately (without delay - within 24 hours) freeze funds/assets and cease PMS transactions upon identifying a confirmed match with a designated individual/entity.
- Report any confirmed sanctions matches, frozen funds, or attempted PMS transactions involving designated parties to the MOE and the Executive Office for Control & Non-Proliferation (EOCN) immediately (without delay).
- Implement procedures for handling 'partial matches' (suspension) related to PMS transactions pending clarification.
- Stay updated on changes to all applicable sanctions lists relevant to PMS trading.

6. Counter Proliferation Financing (CPF)

- Understand and mitigate risks related to the financing of weapons of mass destruction proliferation potentially linked to PMS trading activities.
- Identify and apply enhanced scrutiny to PMS transactions potentially involving dual-use goods (referencing UAE Control Lists) or entities/countries associated with proliferation risks.
- Comply with specific UNSC resolutions and UAE regulations concerning CPF as they may apply to PMS.



7. Transaction Monitoring & Reporting for PMS

- Implement an effective transaction monitoring system (manual or automated) capable of detecting unusual or potentially suspicious **PMS transactions** based on risk indicators (including DPMS-specific red flags) client profiles, and transaction patterns within the gold and palladium trade.
- Establish clear internal procedures for investigating alerts related to PMS transactions generated by the monitoring system or identified by staff.
- Ensure timely reporting of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) related to PMS activities to the UAE Financial Intelligence Unit (FIU) via the goAML portal whenever reasonable grounds for suspicion exist. Maintain confidentiality.
- Crucially, file Dealer in Precious Metals and Stones Reports (DPMSR) via the goAML portal for all qualifying PMS transactions as required by MOE guidelines and thresholds (e.g., cash transactions $\geq$ AED 55,000).
- File High-Risk Country Transaction/Activity Reports (HRC/HRCA) for PMS transactions involving designated high-risk countries, as required.
- Respond promptly and fully to information requests regarding PMS activities from the FIU or MOE.

8. Training & Awareness

- Develop and implement an ongoing, risk-based training program for the Board, Senior Management, Compliance Officer, and all relevant employees involved in PMS activities. Training must cover AML/CFT/CPF/Sanctions laws, specific DPMS regulations, MMT's PMS policies/procedures, individual responsibilities, PMS-specific red flags, and reporting obligations (including DPMSR).
- Tailor training content to specific roles within the PMS business line.
- Maintain comprehensive records of all PMS-related training provided.

9. Record Keeping

- Retain all relevant records related to PMS activities, including CDD/KYC information, transaction data, risk assessments, DPMSR filings, STR/SAR filings, training records, and correspondence with authorities, for a minimum of **five years** from the end of the business relationship or transaction date.
- Ensure PMS records are readily accessible for competent authorities (MOE, FIU) upon request.

10. Policy Maintenance & Compliance Culture

- Review and update this PMS-specific AML/CFT/CPF and Sanctions Policy and related procedures at least annually, or more frequently if necessitated by regulatory changes, changes in MMT's PMS business/risk profile, or findings from audits/reviews.
- Foster a strong compliance culture emphasizing the specific risks and regulatory requirements associated with the PMS sector.
- Strictly enforce the 'No Tipping Off' policy regarding STR/SAR filings or investigations related to PMS transactions.
- Implement and enforce the 'No Retaliation' policy to protect employees who report suspicions related to PMS activities in good faith.
- Ensure all staff involved in PMS understand the potential penalties for non-compliance with DPMS regulations.



I I. Specific Considerations for PMS

- Implement 'Know Your Employee' procedures for staff involved in PMS activities.
- Assess and mitigate risks associated with new technologies or payment methods used in PMS trading.
- If relying on third parties for CDD elements related to PMS clients/transactions, ensure strict compliance with regulatory requirements. MMT remains ultimately responsible for CDD.