

Guidelines on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Internal Controls for Precious Stones and Metals Dealers (PSMDs)

Internal Policies, Compliance, Audit and Training

- 1.1 A PSMD should develop, document and implement adequate internal policies, procedures and controls, taking into consideration its money laundering (ML) and terrorism financing (TF) risks and the size of its business, to help prevent money laundering and terrorism financing, and communicate these to its employees¹.
- 1.2 A PSMD should update its policies and procedures in a timely manner, to take into account new operational, legal and regulatory developments and emerging or new ML/TF risks.

Compliance

- 2.1 A PSMD should appoint an AML/CFT compliance officer at the management level.
- 2.2 The responsibilities of the AML/CFT compliance officer should include —
 - (a) promoting compliance with all relevant AML/CFT regulations¹;
 - (b) taking overall charge of all AML/CFT matters within the organisation;
 - (c) ensuring a speedy and appropriate reaction to any matter in which ML/TF is suspected;
 - (d) reporting, or overseeing the reporting of, suspicious transactions and cash transactions reports referred to under sections 39 and 48J of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Chapter 65A); and
 - (e) advising and training employees and officers on developing and implementing internal controls on AML/CFT.
- 2.3 The AML/CFT compliance officer should consider the set of red flag indicators² which lists circumstances that may warrant STRs to be lodged.

Audit

- 3.1 A PSMD should implement an independent process to independently assess the effectiveness of its internal policies, procedures and controls
- 3.2 In assessing the effectiveness of measures taken to prevent ML/TF, one can consider —
 - (a) determining the adequacy of the PSMD's AML/CFT controls; and
 - (b) reviewing the content and frequency of AML/CFT training programmes, and the extent of employees' compliance with established AML/CFT controls.
- 3.3 The frequency and extent of the assessment should be commensurate with the ML/TF risks presented and the size and complexity of the PSMD's business.

¹ The applicable AML/CFT regulations that a PSMD must comply with include —

- Corruption, Drug Trafficking and other Serious Crimes (Confiscation of Benefits) Act
- Terrorism (Suppression of Financing) Act
- Corruption, Drug Trafficking and Other Serious Crimes (Cash Transaction Reports) Regulations 2014
- United Nations (Sanctions — Democratic People's Republic of Korea) Regulations 2010 (G.N. No. S 570/2010)
- United Nations (Sanctions — Iran) Regulations 2014 (G.N. No. S 633/2014)

² Refer to CAD's website at <http://www.cad.gov.sg/aml-cft/suspicious-transaction-reporting-office/suspicious-transaction-reporting> for the set of red flag indicators for PSMDs.

Employee Hiring

- 4.1 A PSMD should have in place screening procedures to ensure high standards when hiring employees.
- 4.2 The screening procedures applied when a PSMD hires employees can include —
 - (a) background checks with past employers;
 - (b) screening against ML/TF information sources; and
 - (c) bankruptcy searches.

Training

- 5.1 A PSMD should ensure that its employees are regularly and appropriately trained on —
 - (a) AML/CFT laws and regulations, and in particular, the detecting and reporting of suspicious transactions, the cash transaction reporting regime and CDD measures described in Regulation 5 of the Corruption, Drug Trafficking and other Serious Crimes (Cash Transaction Reports) Regulations 2014;
 - (b) the PSMD's internal controls on AML/CFT and the roles and responsibilities of employees in combating ML and TF.
- 5.2 New employees should be trained as soon as possible after being hired or appointed.
- 5.3 Apart from the initial training, a PSMD should also provide refresher training as appropriate, to ensure that employees are reminded of their responsibilities and are kept informed of new developments related to ML/TF.