# **Annex A Sample Risk Assessment Form**

Note: The following template contains examples which the regulated dealers may consider using in their risk assessments, and should be adapted to suit their business context. Regulated dealers should include relevant risk factors and ensure that the measures listed to manage the ML/TF/PF risks identified are aligned to their IPPC.

The ultimate responsibility and accountability for ensuring compliance with the PSPM Act and PMLTF Regulations rest with the regulated dealers’ directors and senior management. As part of AML/CFT/CPF oversight and governance, regulated dealers’ risk assessments must be seen and/or evaluated and signed off by the most senior member of the senior management or whoever he/she designates in the senior management team. The directors and senior management should have a good understanding of the risks that the business is exposed to, and ensure that the risk mitigating measures adopted are adequate, robust and effective.

|  |  |
| --- | --- |
| Name of regulated dealer: | Date of risk assessment: |

* + - 1. **Customer Profile**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Background** | **Low**  **risk** | **Medium**  **Risk** | **High**  **risk** | **Measures to address risk**  [Note: The examples provided below are not exhaustive and they should at minimum contain the ECDD measures in the IPPC if risk factor is assessed to be high] |
| E.g. New customers transacting in cash above S$X,000. |  |  |  | E.g. Obtain compliance officer’s pre-approval before completing transaction  E.g. Request customer to pay in non-cash mode  E.g. Enquire on the customer’s occupation or business |
| E.g. Regular and existing customers transacting in cash above S$X,000. |  |  |  | E.g. Obtain compliance officer’s pre-approval before completing transaction  E.g. Request customer to pay in non-cash mode  E.g. Check if transaction amount is within the same range as previous transactions. If no, to enquire on customer’s reason for transacting above usual transaction range |
| E.g. Politically-Exposed Persons, and their family/close associates |  |  |  | E.g. Conduct ECDD measures in accordance with Section XX of IPPC  E.g. Request customer to pay in non-cash mode |
| Etc. |  |  |  |  |

* + - 1. **Customer’s countries or territories of origin**

| **Country or territory**[[1]](#footnote-2) | **Low**  **risk** | **Medium**  **Risk** | **High**  **risk** | **Measures to address risk** |
| --- | --- | --- | --- | --- |
| E.g. Higher risk jurisdiction (refer to FATF listing:  <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html> as at DDMMYYYY)   * Country A * Country B * Country C etc. * <Regulated dealer to populate the list and keep it updated. To refer to Registrar’s Notices on Jurisdictions under Increased Monitoring> |  |  |  | E.g. Conduct ECDD measures in accordance with Section XX of IPPC |
| Overseas buyer from higher risk jurisdiction (refer to FATF listing:  <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>)  Democratic People’s Republic of Korea (DPRK)  Iran |  |  |  | E.g. Conduct ECDD measures in accordance with Section XX of IPPC  E.g. Enquire and observe if customer is buying products for own consumption in Singapore |

* + - 1. **Products/ Services/ Delivery channels/ Mode and value of transactions**

| **Products** | **Low**  **risk** | **Medium**  **Risk** | **High**  **risk** | **Measures to address risk** |
| --- | --- | --- | --- | --- |
| E.g. Gold bullion |  |  |  | E.g. Conduct all transactions through bank transfers  E.g. Conduct CDD on bullion customers even if payment through non-cash mode |
| E.g. Loose diamonds |  |  |  | E.g. Conduct all transactions through bank transfers  E.g. Conduct CDD on loose diamond customers even if payment through non-cash mode |
| E.g. Jewellery/ watch/ apparel/ accessory/ ornament or other finished product that is priced above S$20K. |  |  |  | E.g. Conduct all transactions through bank transfers  E.g. Conduct CDD on respective customers even if payment through non-cash mode |
| Etc |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Services, Delivery Channels, and Mode and Value of Transactions** | **Low**  **risk** | **Medium**  **risk** | **High**  **risk** | **Measures to address risk** |
| E.g. Payment for gold jewellery using gold bars |  |  |  | E.g. Conduct CDD on customers making payment in gold bars  E.g. Conduct CDD on customers even if payment through non-cash mode |
| E.g. Payment for precious stone jewellery using digital payment tokens | ☐ | ☐ | ☒ | E.g. Conduct CDD on customers making payment in digital payment tokens  E.g. Conduct CDD on customers even if payment through non-cash mode |
| E.g. Online Platform transactions above S$X,000 |  |  |  | E.g. Payment for online transactions using credit cards to rely on the banks’ CDD process. |
| E.g. Transactions conducted by the customer’s representative (i.e. not the customer’s employee) |  |  |  | E.g. Ensure that the customer’s representative is authorised and conduct CDD (including screening) on representative, customer and BO of customer  E.g. Understand the relationship between the customer and his representative  E.g. Limit cash transaction amount to S$XXXX |
| Etc. |  |  |  |  |

# **Annex B Sample IPPC Document**

Note: The following IPPC template is a document which regulated dealers may consider adopting. However, regulated dealers should adapt the IPPC to suit their business context and ensure that the IPPC meets the requirements of the PSPM Act and PMLTF Regulations.

The ultimate responsibility and accountability for ensuring compliance with the PSPM Act and PMLTF Regulations rest with the PSMD’s directors and senior management. As part of AML/CFT/CPF oversight and governance, the IPPC must be approved by the senior management, and directors and senior management are responsible for ensuring that:

a. Enhanced measures are taken to manage and mitigate risks, where higher risks are identified;

b. An ongoing programme to train employees on the IPPC is put in place; and

c. The IPPC is implemented, monitored for effectiveness and enhanced if necessary.

**Cover Page**

Document title: Internal Policies, Procedures and Control (“IPPC”)

Name of regulated dealer:

**Version Control Record**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Release Date** | **Key Changes** | **Author** | **Approved by Senior Management** |
| 1.0 |  |  |  |  |
| 2.0 |  |  |  |  |

**Content Page**

Page

* + 1. Aim …………………………………………………………………………………………………... 2
    2. Assessment of risks …………………………………………………………………………... 4
    3. Etc. …………………………………………………………………………………………………… xx

1. **Aim**
   1. Employees of <**Name of regulated dealer**> or the “regulated dealer” play an important role in protecting against money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk. The following IPPC will equip you to do so, and ensure that the business is in compliance with the Precious Stones and Precious Metals (Prevention of Money Laundering, Terrorism Financing and Proliferation Financing) Act 2019 (“PSPM Act”).
   2. Reference should also be made to the PSPM Act and Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Regulations 2019 (“PMLTF Regulations”) as well as Guidelines from the Ministry of Law and relevant government agencies.
2. **Assessment of risks** 
   1. The regulated dealer shall conduct a risk assessment of its business to identify, assess and understand its ML/TF/PF risks in relation to:
3. the profile of its customers;
4. the customers’ country or territory of origin;
5. the countries or territories where the regulated dealer has operations; and
6. the regulated dealer’s products, services, transactions, delivery channels, etc.
   1. The regulated dealer shall develop measures (internal rules, processes, etc.) to address the identified risks, and ensure that all employees follow and implement such measures.
   2. The regulated dealer shall ensure that its risk assessment is up-to-date by regularly reviewing it every <**X months**>, before launching a new product or a new business practice or before using a new or developing technology for any new or existing product.
   3. The assessment must be seen and/or evaluated and signed off by the most senior member of the senior management of the regulated dealer or whosoever he/she designates in the senior management team.
   4. <**Additional item(s) to be decided by the regulated dealer**>
7. **Group Policy** (*Applicable to regulated dealers with branches or subsidiaries*)
   1. The regulated dealer with one or more branches or subsidiaries (whether located or incorporated in Singapore or in a foreign country or for territory), shall implement a group policy consistent with the internal controls and measures in this document for preventing ML, TF and PF; and for managing and mitigating the risk of ML, TF and PF, that apply to, and are appropriate for:
8. every such branch; and
9. every such subsidiary where more than 50% of the shares or other equity interests are owned by the regulated dealer.
   1. If the regulated dealer has a branch or subsidiary in a foreign country or territory having laws for the prevention of ML, TF or PF that differ from Singapore, the more stringent law shall be applied to that branch or subsidiary, to the extent that the law of the foreign country or territory permits. The regulated dealer shall report to the Registrar of Regulated Dealers (Registrar) if the more stringent law cannot be fully applied to the branch or subsidiary and:
10. perform appropriate additional measures to manage the ML, TF and PF risks; and
11. comply with any directions given by the Registrar.
    1. For the purpose of conducting customer due diligence or managing the risk of ML, TF and PF, the regulated dealer shall have measures to share information among the branches and subsidiaries, if there are adequate safeguards to protect confidentiality and use of information that is shared, including safeguards to prevent tipping-off, and to the extent permitted by the law of the foreign country or territory that the dealer’s branch or subsidiary is in.
    2. Such measures to share information shall include the provision, to the regulated dealer’s group-level compliance, audit, and AML/CFT functions, of customer, account, and transaction information from its branches and subsidiaries within the group, when necessary for AML/CFT purposes. The information to be shared within the regulated dealer’s group should include information and analysis of transactions or activities which appear unusual.[[2]](#footnote-3)
    3. Similarly, branches and subsidiaries shall receive such information from group-level compliance, audit, and/or AML/CFT functions when relevant and appropriate to risk management.
    4. <**Additional item(s) to be decided by the regulated dealer** >
12. **Appointment of a Compliance Officer** 
    1. The regulated dealer shall appoint a management level employee who is fit and proper to be the Compliance Officer for all anti-money laundering/countering the financing of terrorism/countering proliferation financing (“AML/CFT/CPF”) efforts, including the design and execution of the IPPC. In the case of a sole proprietorship, the sole proprietor is the designated Compliance Officer. The responsibilities of the Compliance Officer shall be as follows:
13. Trained/be familiar with the PSPM Act, PMLTF Regulations, relevant regulations and Guidelines issued by the Ministry of Law and relevant government agencies;
14. Ensure that the regulated dealer is in full compliance with the PSPM Act and its regulations;
15. Be responsible for day-to-day operation of the regulated dealer’s AML/CFT measures;
16. Be the main point-of-contact with the Registrar of Regulated Dealers under the Ministry of Law and law enforcement authorities. The compliance officer shall ensure that he/she is reasonably contactable and should appoint a covering officer (in writing to the covering officer), where possible;
17. Ensure that remedial actions are taken in a timely and effective manner when there are instances of non-compliance;
18. Regularly conduct internal audits of all compliance procedures/processes related to AML/CFT/CPF of the regulated dealer (if applicable, refer to section 11); and
19. <**Additional item(s) to be decided by the regulated dealer**>
20. **Conduct employee checks when hiring employees (Not applicable to sole proprietorships)**
    1. The regulated dealer shall check each employee before hiring, against the following information sources:
21. Ministry of Home Affairs Inter Ministry Committee-Terrorist Designation (“IMC-TD”) webpage for listings on terrorist designation (persons designated as terrorists) : <https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism>;
22. Monetary Authority of Singapore (“MAS”) webpage for sanctions listings on designated individuals: <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities>;
23. Public sources like the internet, or against commercial databases, to check if a prospective employee has any adverse/negative news which may pose an ML/TF/PF risk to the dealer, e.g. history of dishonest behaviour;
24. Declaration made by potential employee that such a person:
25. was not convicted of any offence involving fraud or dishonesty; and
26. is not an undischarged bankrupt.
27. <**Additional item(s) to be decided by the regulated dealer**>
28. **Customer Due Diligence (“CDD”)** 
    1. CDD is the process of obtaining your customer’s identifying information, recording the information and verifying who they are before transacting with them. The objective is to help regulated dealers determine the ML/TF/PF risks and take appropriate measures to address them.
    2. The regulated dealer must perform CDD measures in any of the following circumstances:

a. before entering into a designated transaction;

b. where the regulated dealer has reason to suspect ML/TF/PF;

c. where the regulated dealer has reason to doubt the veracity or adequacy of information from earlier CDD measures;

d. under the following prescribed circumstances:

i. before entering into a transaction involving payment in gold (except in the form of jewellery) exceeding S$20,000;

ii. before entering into a transaction involving payment in digital payment tokens exceeding S$20,000.

1. **Procedures to conduct CDD** 
   1. Employees of the regulated dealer shall follow the following procedures when conducting CDD:
2. The employee shall complete the CDD forms as in [**Annex E**](#_Annex_E_Sample)for the following customer types:

| **Customer Type** | **CDD Forms** |
| --- | --- |
| Individual acting for himself | * Customer (Individual) – Form A1 * Documentation of Screening Conducted – Form B |
| Individual acting on behalf of another individual | * Customer (Individual) – Form A1 * Person on behalf Customer is Acting On (Cash Owner **–** Individual) – Form A2 * Documentation of Screening Conducted – Form B |
| Individual acting on behalf of another corporate/ legal arrangement | * Customer (Individual) – Form A1 * Particulars of Person on behalf Customer is Acting On (Cash Owner **–** Corporate / Legal Arrangement) – Form A3 * Particulars of BO(s) of Corporate / Legal Arrangement – Form A4 * Documentation of Screening Conducted – Form B |

1. The documents which the employee can use to verify the identity of the customer are:

| **Customer Type** | **CDD document used to verify customer identity** |
| --- | --- |
| Individuals (customers and BOs of corporate/ Legal arrangement) | * National Identity Card * Passport * <**Additional item(s) to be decided by the regulated dealer**> |
| Corporate/ Legal arrangement | * Records in an independent company registry on ownership and directorship * Certificate of incumbency, certificate of good standing, share register, as appropriate * Certificate of incorporation * <**Additional item(s) to be decided by the regulated dealer**> |
| <**Additional item(s) to be decided by the regulated dealer**> | <**Additional item(s) to be decided by the regulated dealer**> |

1. Where the employee obtains data, documents or information from the customer, he should ensure that such data, documents or information is current and valid at the time they are provided to the regulated dealer.
2. The employee who sighted and took copies of the identification document, should sign and date the copy of the document to document the verification process.
3. If the customer is unable to produce an original document, the employee may consider accepting a copy of the document that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant).
4. Where a document is in a foreign language, appropriate steps should be taken by the regulated dealer to be reasonably satisfied that the document does in fact provide evidence of the customer’s identity. The employee should ensure that any document that is critical for the performance of any measures required under the Regulations is translated into English by a suitably qualified translator. Alternatively, a translation of such a document by an employee who is conversant in that foreign language may be relied upon. This is to allow all employees of the regulated dealer involved in the performance of any measures required under the Regulations to understand the contents of the documents, for effective determination and evaluation of ML/TF/PF risks associated with the customer.
5. The employee should ensure that documents obtained for performing any measures required under the Regulations are clear and legible. This is important for the establishment of a customer’s identity, particularly in situations where business relations are established without face-to-face contact.
   1. Employees of the regulated dealer shall adhere to the following procedures when conducting screening of their customers:

a. The employee shall check each customer before entering into a transaction against the following information sources:

i. Ministry of Home Affairs: IMC-TD website (<https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism>);

ii. UN sanctions lists from the Monetary Authority of Singapore website (<https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities>); and

iii. Financial Action Task Force (“FATF”) list of high-risk countries (https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html).

* + 1. The employee shall update the supervisor (if any) and/or managerial-level employee (if any) and/or compliance officer if there are any matches of the names of customer (individual), person(s) on whose behalf the customer is acting or corporate customer and BO(s) of corporate customer to lists in paragraph 6.2(a)(i) and (ii). The regulated dealer must stop the transaction and report to the police if the match is assessed to be a true match.

c. The employee shall update the supervisor (if any) and/or managerial-level employee (if any) and/or compliance officer if the customer, the person on whose behalf the customer is acting, or a BO of the corporate customer is a Politically-Exposed Person (“PEP”) or if they are from countries in list in paragraph 6.2(a)(iii). The regulated dealer shall continue with ECDD measures (refer to paragraph 9).

d. The employee shall document the results of the screening and assessment.

* 1. In the case that CDD in regulations 5 to 6 of the PMLTF Regulations cannot be completed, the regulated dealer shall terminate the transaction, consider if the circumstances are suspicious so as to warrant the filing of a suspicious transaction report (“STR”) and document the basis for its determination, including where the customer is reluctant, unable or unwilling to provide any information requested by the regulated dealer.
  2. Where the regulated dealer forms a suspicion of ML/TF/PF and reasonably believes that performing any of the measures as required in regulations 5 to 6 of the PMLTF Regulations will tip-off a customer, the person on whose behalf the customer is acting, or a BO of that person, the regulated dealer may stop performing those measures. The regulated dealer shall document the basis for assessment and file an STR.
  3. <**Additional item(s) to be decided by the regulated dealer**>

1. **Procedures to complete a Cash Transaction Report (“CTR”)**
   1. The following procedure shall apply for the regulated dealer and employees when completing a CTR:
2. The regulated dealer shall designate an employee e.g. Compliance Officer or employee/s to complete a CTR.
3. The employee who is communicating with the customer and/or conducting CDD shall inform the supervisor on the necessity to lodge a CTR.
4. The designated employee tasked with completing the CTR shall submit Form NP 784 at the Suspicious Transaction Reporting Office (“STRO”) Online Notices And Reporting Platform (“[SONAR](http://www.police.gov.sg/sonar)”) at <http://www.police.gov.sg/sonar> within 15 business days.
5. The designated employee shall check all the inputted information to ensure accuracy. Submitting an incomplete or inaccurate CTR without reasonable excuse constitutes as an offence under the PSPM Act.
6. <**Additional item(s) to be decided by the regulated dealer**>
7. **Enhanced Customer Due Diligence (“ECDD”)** 
   1. Where the ML/TF/PF risks are identified to be higher, the regulated dealer is expected to take ECDD measures to mitigate and manage those risks.
   2. The regulated dealer must conduct ECDD measures in any of the following circumstances where the customer, the person on whose behalf the customer is acting, or a beneficial owner of the customer (where the customer is an entity or legal arrangement):

a. is a PEP, a family member or a close associate of a PEP;

b. is a resident of or originates from a country on the FATF list of high-risk countries ([www.fatf-gafi.org/countries/#high-risk](http://www.fatf-gafi.org/countries/#high-risk)); and

c. is assessed to have higher ML/TF/PF risks.

* 1. A customer, the person on whose behalf the customer is acting, or a beneficial owner of the customer (where the customer is an entity or legal arrangement) is assessed to be of higher ML/TF/PF risk when he is:
  2. a resident of or originates from a foreign country or territory that the FATF has placed under increased monitoring or the Registrar has notified to be with inadequate measures to prevent ML/TF/PF;
  3. in higher risk business/ activities <**to be decided by the regulated dealer**>
  4. exhibits the following behaviour or transaction pattern <**to be decided by the regulated dealer. Regulated dealer can consider the red flag indicators in Annex D**>
  5. from countries or territories which have relatively higher levels of corruption and/or organised crimes, as identified by credible bodies (e.g. reputable international bodies such as Transparency International).
  6. <**Additional item(s) to be decided by the regulated dealer**>

1. **Procedures to conduct ECDD**
   1. The ECDD measures to be conducted include:

a. obtaining the approval of a person holding a senior managerial or executive position in the regulated dealer before —

(i) in the case of a new customer, entering into a transaction with the customer; or

(ii) in the case of an existing customer, continuing to transact with the customer.

b. taking reasonable measures to establish the income level, source of wealth, and the source of funds, of the customer and, if the customer is an entity or a legal arrangement, of the beneficial owner or owners of the customer **<regulated dealer should elaborate on the “reasonable measures”>;**

c. conducting enhanced ongoing monitoring of the transactions entered into with the customer so as to identify suspicious transactions, including transactions or patterns of transactions that are inconsistent with the customer’s profile.

d. <**Additional item(s) to be decided by the regulated dealer**>

* 1. Employees of the regulated dealer shall follow the following procedure when conducting ECDD:

1. The employee shall complete the ECDD form as shown in [**Annex F**](#_Annex_F_Sample).
2. The employee shall update the supervisor (if any) and managerial-level employee (if any) if ECDD cannot be completed.
3. <**Additional item(s) to be decided by the regulated dealer**>
   1. The regulated dealer shall assign an employee to conduct enhanced and regular (the time-frame to be decided by the regulated dealer) checks of higher risk customers.
   2. <**Additional item(s) to be decided by the regulated dealer**>
4. **Ongoing Monitoring**
   1. The regulated dealer must conduct ongoing monitoring of transactions for regular customers and for cases where the money laundering, terrorism financing or proliferation financing risk are assessed to be high.
   2. The regulated dealer shall conduct ongoing monitoring of transaction by reviewing on an annual basis the information and documents obtained as a result of the CDD measures for regular customers and also in cases where there is a higher risk of money laundering, terrorism financing or proliferation financing.
   3. The following procedures shall apply when the regulated dealer and employees are conducting annual reviews on the customers:
5. The employee shall review the transactions with the customer and assess if the transactions are consistent with its knowledge of the customers, customers’ income and risk profile and customers’ source(s) of funds. Where transactions are inconsistent with the known profile, the employee should check with the customer if its profile and business have changed.
6. The employee should review the identifying documents collected to ensure that they are still valid and current. Where the documents are outdated, the employee should request an updated document from the customer.
7. The ongoing monitoring procedures performed should be properly documented.
8. **Procedure to complete an STR**
   1. The following procedure shall apply for the regulated dealer and employees when completing an STR:
9. The regulated dealer shall designate an employee e.g. Compliance Officer or employees tasked to complete an STR;
10. The employee who is communicating with the customer and/or conducting CDD or ECDD shall inform the supervisor on the necessity to complete an STR (a discussion may be necessary);
11. The designated employee tasked with completing a STR shall submit it via [SONAR](http://www.police.gov.sg/sonar) as soon as possible; and
12. The designated employee shall check all the inputted information to ensure accuracy and/or get clearance from the compliance officer.
13. <**Additional item(s) to be decided by the regulated dealer**>
    1. The employee is reminded that under Section 57 of the CDSA, it is an offence to disclose a STR that was filed or to tip off the customers.
14. **Record keeping** 
    1. The Regulated Dealer shall keep copies of documents with the following information for a period of **5 years**:

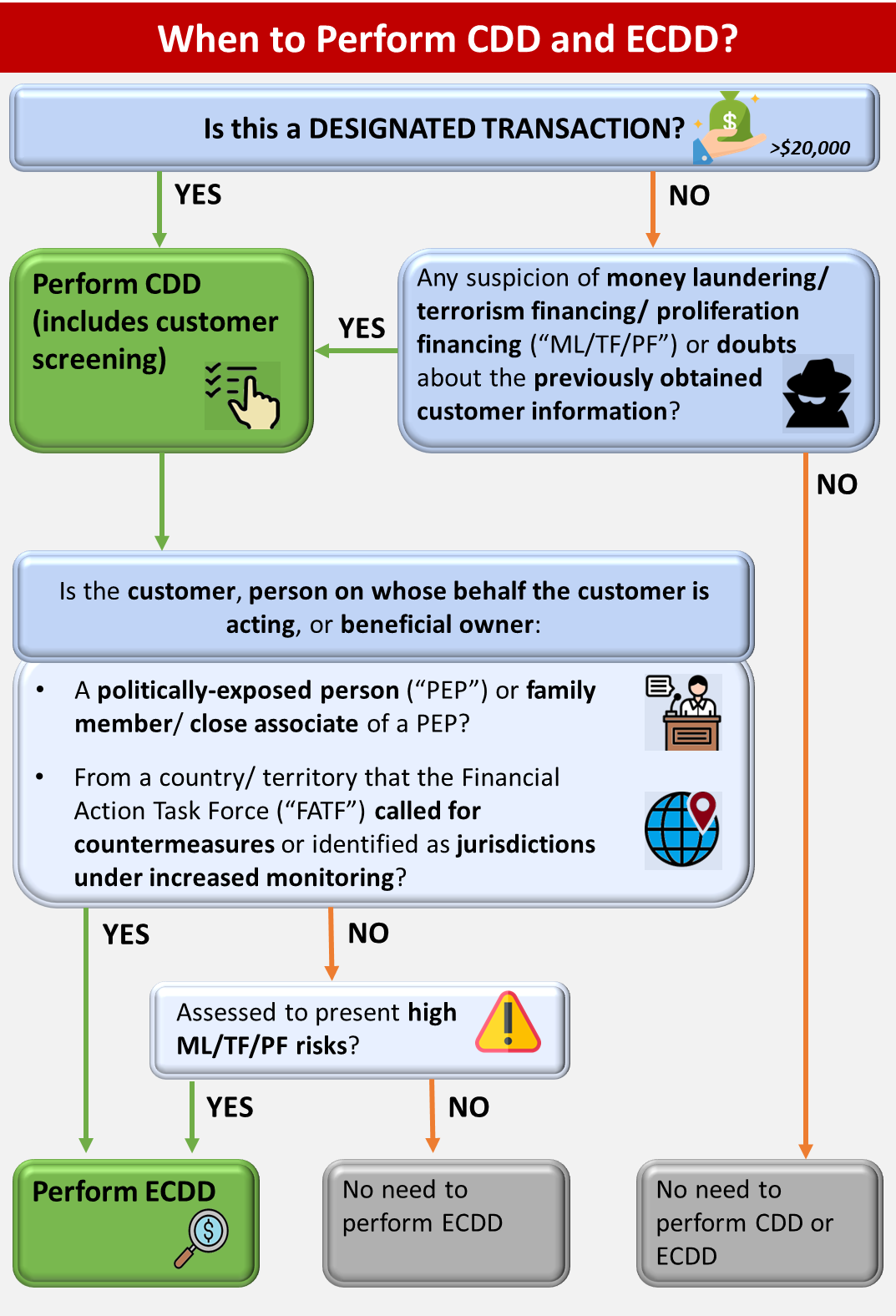
*For all customers*

1. Customer’s identifying information;
2. A copy of the supporting document that was relied upon for the customer’s identifying information (e.g. NRIC, passport);
3. Whether the customer is the owner of the cash or cash equivalent received from the customer, owner of the PSPM purchased or redeemed from the customer or acting on behalf of another person;
4. Identifying information of the person the customer is acting on behalf of, if the customer is not the owner mentioned in paragraph 12.1(c);
5. Proof that the customer is authorised to act on behalf of that other person, if the customer is not the owner mentioned in paragraph 12.1(c);
6. Date of transaction or intended transaction;
7. Amount of transaction or intended transaction;
8. Description of the PSPMs sold, purchased or redeemed under the transaction or intended transaction;
9. Address where the transaction was carried out, or would have been carried out;
10. Name and designation of the individual who carried out (or would have carried out) the transaction on behalf of the regulated dealer; and
11. The reason why the regulated dealer was unable to or chose not to complete any CDD measures;
12. Supporting documents relied on in making a CTR;
13. Where ECDD or SCDD was carried out, the name and designation of the person holding the senior managerial or executive position in the regulated dealer who approved the transaction with the customer.
14. A copy of all CTRs.

*For customers acting on behalf of a legal person*

1. the name of the legal person;
2. the legal form of the legal person;
3. proof of the legal person’s existence (e.g. ACRA BizFile search);
4. the place under which the legal person is incorporated, registered or otherwise constituted;
5. the documents that regulate and bind the legal person (e.g. the corporate constitution of a company);
6. if the legal person is incorporated or registered in Singapore, its unique entity number (UEN No.);
7. if the legal person is incorporated or registered outside Singapore, its foreign incorporation or registration number;
8. if the legal person is an entity, the identity of each individual having a senior management position in the legal person;
9. the address of the legal person’s registered office and its principal place of business.
10. if the legal person is an entity:
    * 1. the identifying information of each individual who ultimately has a controlling ownership interest in the legal person;
      2. if it is doubtful whether all or any of the individuals who ultimately have a controlling interest in the legal person are its beneficial owners, or where no individual exerts control through ownership interests, the identifying information of each individual (if any) exercising control of the legal person through other means; or
      3. if no individual is identified under sub-paragraphs (i) and (ii), the identifying information of each individual having a senior management position in the legal person.
11. if the legal person is a trust, the identities of:
12. the settlor;
13. each trustee;
14. the protector (if any);
15. each beneficiary or class of beneficiaries; and
16. any other individual exercising ultimate effective control over the trust.
17. if the legal person is a legal arrangement that is not a trust, the identity of each person holding a position equivalent or similar to any position in paragraph (y).
    1. A registered dealer may also be asked to keep relevant documents and information for a prescribed period after ceasing to be a registered dealer. If the registered dealer is found to have dispose records during the period of the registration, the registered dealer will be liable for enforcement action against them.
18. **Staff training on AML/CFT/CPF**
    1. The regulated dealer shall ensure that its employees attend on-going training on AML/CFT/CPF matters. The training can be conducted internally or through the engagement of external training providers.
    2. The regulated dealer shall record the names of the employees who have undergone training and the courses attended (with date/s of courses attended).
    3. <**Additional item(s) to be decided by the regulated dealer**>
19. **Audit of IPPC** (*Applicable to regulated dealers who conduct designated transactions*)
    1. The regulated dealer shall conduct an independent audit of its IPPC to assess the effectiveness of measures taken to prevent ML/TF/PF. This includes the following:
20. Determine the adequacy and relevance of the IPPC;
21. Assess employees’ compliance with the IPPC; and
22. Assess whether instances of non-compliance are reported to senior management on a timely basis.
    1. The regulated dealer shall state that the frequency of such audits is every **X** month.
    2. The auditing unit must be adequately independent of the business arm.
    3. <**Additional item(s) to be decided by the regulated dealer**>
23. **Tipping-off and Confidentiality**
    1. Employees of the regulated dealer are reminded that it is an offence[[3]](#footnote-4) to disclose the fact that an STR was filed.
24. **Additional procedures (deemed necessary by the regulated dealer)**
    1. XXX

# **Annex C Guide on When to Perform CDD and ECDD Measures**



# **Annex D Red Flag Indicators for Regulated Dealers**

**General Comments**

Any person, who in the course of business, employment, trade or profession, knows or has reasonable grounds to suspect that any property is linked or intended to be used in connection with criminal conduct or drug dealing (or generically referred to as “crime”), shall disclose the knowledge or suspicion or the information to the Suspicious Transaction Reporting Office (“STRO”). This must be done as soon as is reasonably practicable after it comes to his attention. Please refer to the STRO’s website on how to lodge a Suspicious Transaction Report (“STR”) with STRO.

The red flag indicators that follow are meant to help PSMDs to identify some of the circumstances that could be suspicious in nature. They could indicate that property may represent proceeds of money laundering (“ML”) or terrorism financing (“TF”) or proliferation financing (“PF”) or used/intended to be used in connection with ML or TF.

While each individual indicator may not be sufficient by itself to suggest ML or TF or PF, a combination of the indicators may indicate a suspicious transaction.

The list is not exhaustive. It may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Please refer to STRO’s website for the latest list of red flags.

A customer’s declarations regarding such transactions should be checked for plausibility. Not every explanation offered by the customer can be accepted without scrutiny.

It is reasonable to suspect any customer who is reluctant to provide normal information and documents required routinely by the PSMD before entering into a designated transaction. PSMDs should pay attention to customers who provide minimal, false or misleading information.

**Red Flag Indicators: Customers**

A “customer” in this context means a person with whom a regulated dealer enters into or intends to enter into a transaction. Precious stones, precious metals and precious products are collectively referred to as “PSPM” in the red flag indicators.

**Transaction Patterns**

i) Transactions that are not consistent with the expected or known profile of the customer:

(a) Transactions that appear to be beyond the means of the customer based on his/her stated or known occupation or income, experience in the industry or known share capital or period of incorporation

(b) Transactions that appear to be more than the usual amount or quantity for a typical customer of the business; or

(c) Transaction purposes that are not in line with the known or expected operations of the business.

ii) Unusually large amounts of cash, traveller’s cheques, cashier's cheques or precious metals, e.g. gold bars or precious stones, e.g. diamonds, digital payment tokens involved in the transactions.

iii) Unusually large or frequent transactions that are made in a foreign currency.

iv) Transactions in which third parties are involved, either as payers or recipients of payment or PSPM, without apparent legitimate business purpose. For example:

(a) Payments received from a third party, who is not the owner of the funds, without legitimate business purpose;

(b) Payments received from multiple third parties for the same transaction;

(c) Payments of proceeds made to third parties overseas, although the transaction is between a domestic buyer and seller, and without apparent legitimate business purpose;

(d) PSPM delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose; or

(e) Refunds paid to a third party, who is not the owner or payer of funds, without legitimate business purpose.

Note: Payments may be in the form of third-party cheques, a third-party credit card, precious metals, e.g. gold bars or precious stones, e.g. diamonds and digital payment tokens.

v) Transactions with no apparent business purpose among associates or trading accounts for PSPM and asset-backed tokens traded using bullion, investment or asset-backed token.

vi) Large transactions which are cancelled shortly after deposits or full payment are made, resulting in the refunds. For example, the customer may pay for the transaction in cash and request the refund be issued in the form of a cheque. Conversely, the transaction may be made with a credit card and the customer request for the refund to be in cash or other means.

vii) Overpayment of transactions with a request to refund excess in cash or to a third party.

viii) Transactions involving virtual assets, especially where ownership of the virtual assets cannot be easily traced to the customer.

ix) Transactions involving the use of stolen or fraudulent payment instruments, for example a payment card that appears stolen or altered or not issued in the customer’s name. Some other possible indicators of suspicious online payment ‘card-not-present’ transactions could include:

(a) Same shipping address, but different payment cards: Multiple online orders with mismatched payment card information could signify a criminal attempting to use a series of stolen or fraudulent payment cards while the cards are still active.

(b) Same payment account, but different shipping addresses: Some criminals may share stolen payment card information with accomplices, or order PSPM for them and ask for the PSPM to be shipped to various different shipping addresses.

(c) Same Internet Protocol address (IP address): Online orders made from the same IP address, especially at or around the same time, but with different payment cards could signify criminals attempting to use fraudulent payment cards.

(d) Reattempting with smaller transaction amount: When an online order is flagged as a potential fraud and declined, criminals may attempt to quickly purchase another item that cost less. This may indicate a form of card testing to try identifying the card’s limit and available balance of the account.

x) Transactions involving unusual or complex payment arrangements, without apparent legitimate business purpose.

**Customer Behaviour**

i) The customer appears to be structuring amounts to avoid customer identification or reporting threshold. For example, numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial (e.g. below the regulatory threshold for CDD), but the cumulative total of which is substantial.

Note: especially if just below S$20,000 cash reporting threshold.

ii) The customer makes enquiries about refund policies and requests for large refunds subsequently.

iii) The customer is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes, e.g. the customer presents identification documents with recent issue dates.

iv) The customer is unusually concerned with the PSMD’s anti-money laundering, countering the financing of terrorism and countering proliferation financing (“AML/CFT/CPF”) policies.

v) The customer fails to provide sufficient explanation and/or documents for the source of funds for his transaction. For example, the customer attempts to use a third-party cheque or credit card in which the source of funds or underlying ownership cannot be easily traced to the customer or is questionable.

vi) The customer attempts to maintain a high degree of secrecy with respect to the transaction, for example:

(a) To request that normal business records not to be kept; or

(b) The customer is unable or unwilling to provide information for due diligence and record keeping purposes.

(c) The customer is unable or unwilling to identify beneficial owners or controlling interest, where this would be commercially expected.

(d) The customer is vague or refuses to provide information on the reason for buying or selling PSPM, or about the origin of the items.

vii) The customer or the declared owner of the funds is traced to negative news or crime. For example, the person is named in a reliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity, or detected when screened against UN Security Council Resolutions (UNSCRs).

viii) The customer appears to be related to a high-risk country or territory or entity that is associated with money laundering or terrorism activities or a person that has been designated as terrorists.

ix) The customer dramatically increases purchases of PSPM for no apparent reason or is willing to sell PSPM at a rate significantly lower than their typical sale value.

x) The customer is employed by a PSMD but is dealing in his personal capacity.

xi) The customer uses alternative addresses for delivery such as a General Post Office (GPO), private service provider mailbox or third parties to receive purchases.

xii) The customer appears to be in a hurry to complete the transaction.

xiii) The customer purchases PSPM without consideration for the value, size and/or colour of the PSPM or other costs (e.g. the extra expense of rush shipping) in the transaction.

xiv) The customer is accompanied by others who appear suspicious (e.g. lurking outside the premise and closely monitoring the customer) and is in doubt when asked for further details.

xv) The customer requests to alter the transaction after being asked for identity documents.

xvi) The customer makes unnecessary self-disclosure that his funds are clean and not involved in any money-laundering activities.

xvii) The customer pays excessively for an item beyond its expected selling price in an auction.

xviii) The customer insists on using cash to pay for excessively high value transactions when there was no apparent economic reason.

**Red Flag Indicators: Suppliers**

**Transaction Patterns**

i) Transactions that are not consistent with the usual profile of a supplier:

(a) Over or under-invoicing, structured, complex, or multiple invoice requests, and high-dollar shipments that are over or underinsured; or

(b) Transactions which are excessive, given the amount or quality, or potential profit from the sale of PSPM; or

(c) Consignment size or type of PSPM shipped appears inconsistent with the capacity of the exporter or importer. For example, the shipment or transhipment that does not make economic sense.

(d) Misclassification of gold purity, weight, origin and value on customs declaration forms.

(e) The transaction involves the use of front or shell companies, which have no real operating activity. For example, the entity’s ownership structure appears to be doubtful or obscure or the entity refuses to provide additional information when requested.

ii) Transactions in which third parties are involved, either as payers or recipients of payment or PSPM, without apparent legitimate purpose.

(a) Funds paid to a third party who is not related to the supplier, without legitimate business purpose; or

(b) PSPM delivered from a third party who is not related to the supplier, without legitimate business purpose.

iii) Transaction involving virtual assets, especially where ownership of the virtual assets cannot be easily traced to the regulated dealer and supplier.

**Supplier Behaviour**

i) The supplier is unable to provide information for due diligence and record keeping purposes.

ii) The supplier is suspected to be using forged, fraudulent or false identity documents for due diligence and record keeping purposes.

iii) The supplier’s origins of the PSPM appear to be fictitious, doubtful or cannot be explained. For example, the supplier sells a large amount of PSPM that originate or are known to be traded from areas not known for their production i.e. trading centres.

iv) The supplier is unusually concerned with the PSMD’s AML/CFT/CPF policies.

v) The supplier attempts to maintain a high degree of secrecy with respect to the transaction, for example –

(a) Request that normal business records not to be kept; or

(b) Unwillingness to identify beneficial owners or controlling interests, where this would be commercially expected; or

(c) Request for payments to be made through money services businesses or other non-bank financial institutions for no apparent legitimate business purposes.

(d) Is vague or refuses to provide information on the reason for selling or buying PSPM, or about the origin of the items.

vi) (For diamonds only) Rough diamonds are not accompanied by a valid Kimberley Process (KP) certificate. For example:

(a) No KP certificate attached to the shipment of rough diamonds; or

(b) The KP certificate is or appears to be forged; or

(c) The KP certificate has a long validity period.

vii) The supplier is traced to negative news or crime. For example, the person is named in a reliable source (which can include a media or other open sources) that the person is suspected of being involved in illegal activity, or detected when screened against UN Security Council Resolutions (UNSCRs).

viii) The supplier appears to be related to a high-risk country or territory or entity that is associated with risk for money laundering or terrorism activities or a person that has been designated as terrorists.

ix) The supplier transports the PSPM through a country or territory that is designated as ‘high risk for money laundering or terrorism activities’ for no apparent economic reason.

x) The location to which the PSPM are moved directly to or from storage, is different from the supplier’s listed address.

xi) The supplier uses alternative addresses as a General Post Office (GPO), private service provider mailbox which appears to be concealing its whereabouts.

xii) The supplier appears to be in a hurry to complete transaction or is willing to sell PSPM at a rate significantly lower than their typical sale value.

xiii) The supplier does not appear to understand the PSPM industry, or lacks the appropriate equipment or finances to engage in regulated activity in the PSPM industry.

xiv) The supplier appears to be uninterested in or uninformed about the structure or transactions of their PSPM business.

xv) Other indicators that may warrant closer scrutiny. For example, the supplier offers products such as loose diamonds that retain their wholesale value because they can be easily liquidated. The supplier may insist on offering products through non-face-to-face means (telephone, mail internet). These delivery channels may pose higher risks, as it may make it more difficult to identify the supplier.

**Red Flag Indicators: Proliferation Financing[[4]](#footnote-5)**

The following are some of the red flag indicators that could alert PSMDs to customers and transactions that are possibly associated with PF-related activities:

* + - * 1. The customer is vague and resistant to providing additional information when asked.
        2. The customer’s activity does not match its business profile or the end-user information does not match the end-user’s business profile.
        3. The transaction involves designated individuals or entities.
        4. The transaction involves higher risk countries or jurisdictions, or involves other entities with known deficiencies in AML, CFT or countering of proliferation financing controls, or involves possible shell companies.
        5. The transaction involves containers whose numbers have been changed or ships that have been renamed.
        6. The shipment of goods takes a circuitous route or the financial transaction is structured in a circuitous manner.
        7. The transaction involves the shipment of goods inconsistent with normal geographic trade patterns or consumer patterns (e.g. the country involved would not normally export or import such goods).
        8. There are inconsistencies in the information provided, including in trade documents and financial flows (e.g. in the names, companies, addresses, ports of call and final destination).

The FATF has also provided guidance on measures to combat PF and PSMDs may wish to refer to the [FATF website](http://www.fatf-gafi.org/) for additional information.

**Red Flag Indicators: Misuse of Shell and Front Companies[[5]](#footnote-6)**

Shell companies are companies (also known as “Legal Persons”) with no operations, assets or business activities. Although all companies start as shell companies, many become fully operational and carry out legitimate business activities. Others may remain as shell companies serving legitimate purposes such as transaction vehicles for corporate mergers or to protect names from being used by others. Generally, a company can only be determined as being used for illegitimate or illicit purposes after its incorporation.

Not all companies that are being misused for money laundering are shell companies. Front companies with a portfolio of businesses, comprising a mix of legitimate and illicit activities, are often used. This makes it challenging to identify the true nature of companies.

When carrying out transactions with Legal Persons, PSMDs should watch out for the following signs of illicit activities.

|  |
| --- |
| **Pass-Through Transactions**  Pass-through transactions create additional layers in attempts to mask the proceeds from illicit activities. Transactions that pass through Legal Persons with no real economic purpose or plausible explanations are risk indicators that the Legal Person may be misused for money laundering. |
| **Round-Tripping Activities**  Round-tripping activities are a series of transactions where original funds are passed through entities but eventually returned to original entity, with the pass-through activity serving no apparent economic purpose. The objective is to create the impression that money is derived from legitimate commercial activities. |
| **Hidden Relationships**  Relationships between Legal Persons may be hidden using nominee shareholders/ directors with complex structures involving listed companies. Such relationships are usually not apparent and PSMDs should be alert to the need for such overly complex relationships or the mixed used of personal and corporate funds in the purchase of PS/PM/PP. |
| **Use of Similar Name Entities**  Front companies may be set up, without significant assets or business activity, using similar names to establish entities. The purpose is to give an impression of legitimacy through association, and fake documents may be produced to allow transfer of funds through these front companies. |

**Red Flag Indicators: GST Missing Trader Fraud (“MTF”) Involving Precious Metals[[6]](#footnote-7)**

IRAS has observed MTF arrangements involving Investment Precious Metals (“**IPM**”) gold bars that are exempted from GST. Syndicates will transform the IPM gold bar into scrap gold by melting, cutting or defacing them for onward sale to businesses down the supply chain. A supplier fails to account for or pay the GST charged on his sales (this supplier is referred to as the “**Missing Trader**”), while businesses along the supply chain continue to claim credit of input tax or refund of GST on their purchases. We have listed the following non-exhaustive warning signs and the due diligence checks below for you to protect your business from any involvement or association with such MTF arrangements.

| **Warning Signs** | **Due diligence checks** |
| --- | --- |
| * **High-value deals offered by newly established supplier**, with minimal experience in the industry. * **Very quick turnaround of high-volume transactions**, making the business appear unrealistically lucrative. * **Back-to-back purchase to sale arrangement** with a fixed gold price between the supplier and customers, making the business practically risk free with little or no exposure to price volatility. * **Out of the norm credit terms.** For example, supplier delivers the gold to you first, and only requires you to make payment after you receive the payment from the customer. * **Too good to be true deals recommended by unfamiliar introducer.** * **Scrap gold bars in condition or volume that is not ordinarily traded in the market.** For example, buying or selling cut or defaced IPM gold bars or cast scrap gold bars in large quantity. * **Supplier/ introducer is evasive** when being asked about the source of its gold supply. * **Material changes in the transactions with existing suppliers or customers.** For example, significant increase in transaction volume or transaction value, or changes in the nature of goods trade.   Note: The above risk indicators and due diligence checks are not exhaustive. | * **Are your immediate supplier and customer legitimate?** Obtain business incorporation details, perform credit checks, request for trade references and verify whether they are credible, and visit their business premises. * **Is the business arrangement valid?** Understand whether there are valid business reasons for IPM gold bars to be defaced or cut and sold as scrap gold bars, whether there are reasonable explanations for the high volume and/or low price of the scrap gold bars relative to the market price and demand, whether the absence of price volatility risk is in line with commercial practice, and whether there is any value for you to be part of the back-to-back purchase to sales arrangement when the customer could have purchased the goods directly from the supplier. * **Is the payment arrangement highly favourable?**Is there commercial justification for the payment to be made to the supplier only after payment is received from the customer. * **Are the scrap gold bars authentic?**Question the source of the scrap gold bars and whether there is a reasonable explanation for them to be defaced IPM gold bars. * **Is the introducer legitimate and credible?** Obtain more information on the introducer. For example, his/her experience in the trade, and the reason for him/her to offer you the deals instead of carrying out the deals himself/herself. * **Is there a valid reason for material changes in the transactions?** Be alert to unusual changes when transacting with existing suppliers and customers. For example, question whether there is any reasonable explanation for the significant increase in the transaction volume and value. |

# **Annex E Sample CDD Forms**

Note: Regulated dealers may consider adopting the following forms to document the CDD measures taken. Regulated dealers remain responsible for ensuring that the forms meet the requirements of PMLTF Regulations.

|  |  |
| --- | --- |
| **Customer Due Diligence (“CDD”)**  **FORM A1 – Particulars of Customer (Individual)** | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMATION REQUIRED** | | | **Example of Supporting Document** |
|  | Transaction number |  | **Invoice** |
|  | Date/Time of transaction |  |
|  | Transaction value |  |
|  | Description of PSPM sold/purchased |  |
|  | Full name (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |
|  | Is the customer acting on behalf of any other individual? Tick the relevant box:  **\* If customer is acting for another individual, employee to also complete Form A2 with details of the individual who is the cash owner.**  **^ If customer is acting for a corporate (e.g. a company or sole proprietorship)/ legal arrangement, employee to also complete Form A3 with details on the corporate or legal arrangement and A4 on the details of beneficial owners of the corporate or legal arrangement.** | **Customer is acting for himself**  **Customer is acting on behalf of person (cash or PSPM owner is an individual) \* (Go to Form A2)**  **Customer acting on behalf of a corporate or legal arrangement (cash or PSPM owner is a corporate) ^ (Go to Form A3 and A4)** |

|  |  |
| --- | --- |
| **Customer Due Diligence (“CDD”)**  **FORM A2 – Particulars of Person on behalf Customer is Acting On (Cash Owner – Individual)** | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

|  |  |  |  |
| --- | --- | --- | --- |
| **INFORMATION REQUIRED** | | | **Example of Supporting Document** |
|  | Is the customer authorised to act on behalf of the other person or the real owner of the cash or cash equivalent? | **Yes**  **No** | **Letter of authorisation/ document proof** |
|  | Transaction number |  | **Invoice** |
|  | Date/Time of transaction |  |
|  | Transaction value |  |
|  | Description of PSPM sold/purchased |  |
|  | Full name (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |

|  |  |
| --- | --- |
| **Customer Due Diligence (“CDD”)**  **FORM A3 –Particulars of Person on behalf Customer is Acting On (Cash Owner – Corporate / Legal Arrangement)** | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

| **INFORMATION REQUIRED** | | | **Example of Supporting Document** |
| --- | --- | --- | --- |
|  | Transaction number |  | **Invoice** |
|  | Date/Time of transaction |  |
|  | Transaction value |  |
|  | Description of PSPM sold |  |
|  | Is the customer authorised to act on behalf of the other person or the real owner of the cash or cash equivalent? | **Yes**  **No** | **Letter of authorisation/ document proof** |
|  | Full name of entity |  | **ACRA BizFile report or certificate of incorporate or any other corporate documents from reliable and independent sources** |
|  | Date of incorporation or registration |  |
|  | Country or territory of incorporation or registration |  |
|  | UEN/Incorporation no./Registration no. |  |
|  | Date of identification expiry (if applicable) |  |
|  | Main business activity: |  |
|  | Type of legal entity | **Sole proprietorship**  **Partnership**  **Limited partnership**  **Limited liability partnership**  **Company**  **Corporation**  **Others:** |
|  | Proof of legal entity’s existence (e.g. ACRA BizFile search) |  |
|  | Registered office address |  |
|  | Name of senior management of the legal entity | **\* To include all senior management here.** |
|  | Document(s) that regulate and bind the entity (e.g. the corporate constitution of a company) |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Principal address of business (if different from registered office address) |  |
|  | Telephone number |  |
|  | Email address |  |
|  | Nature of business of the legal entity |  |
| **Details of beneficial owners should be filled in Form A4.** | | | |

|  |  |
| --- | --- |
| **Customer Due Diligence (“CDD”)**  **FORM A4– Particulars of Beneficial Owner(s) of Corporate Customer/ Legal Arrangement** | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

| **INFORMATION REQUIRED** <Details for beneficial owners who have control over the corporate/ legal arrangement should be identified and verified> | | | **Example of Supporting Document** |
| --- | --- | --- | --- |
|  | Full name of **BENEFICIAL OWNER 1** (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number: |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |
|  | Full name of **BENEFICIAL OWNER 2** (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |
|  | Full name of **BENEFICIAL OWNER 3** (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |
|  | Full name of **BENEFICIAL OWNER 4** (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |
|  | Full name of **BENEFICIAL OWNER 5** (including any alias) |  | **Copy of original identifying document sighted** |
|  | Date of birth |  |
|  | Residential address |  |
|  | Citizenship |  |
|  | Type of identification document | **NRIC**  **Passport**  **Others:** |
|  | Identification number |  |
|  | Date of identification expiry (if applicable) |  |
|  | Occupation |  | **Customer’s declaration or regulated dealer’s documentation of enquiry with customer** |
|  | Contact number |  |

|  |  |
| --- | --- |
| **Customer Due Diligence (“CDD”)**  **FORM B – Screen all names and citizenship of customer (individual), corporate customer and beneficial owner(s) of corporate customer obtained from CDD against the lists on:**   * Terrorist designation * Sanctions lists on designated individuals and entities * FATF public list of high-risk and other monitored jurisdictions   \*Note: This form should not be shown to the customer. | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

|  |  |  |
| --- | --- | --- |
| **B1. Check Against Lists on Terrorist Designation and Designated Individuals and Entities** | | |
| 1. | Ministry of Home Affairs (“MHA”)’s website on the Inter-Ministry Committee on Terrorist Designation (“IMC-TD”) on terrorist designation (persons and entities designated as terrorists):  <https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism> | **Any match?**  **Yes/  No**  \*Important: If yes, to stop transaction and lodge a police report. |
| 2. | Monetary Authority of Singapore (“MAS”)’s website on targeted financial sanctions under the United Nations Regulations (“UN Regulations”) for the lists of designated individuals and entities:  <https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities> | **Any match?**  **Yes/  No**  \*Important: If yes, to stop transaction and lodge a police report. |
| **B2. Politically Exposed Person (“PEP”)** | | |
| 1. | Is the customer a PEP? | **Yes/  No**  \*Important: If yes; to proceed with ECDD. |
| **B3. Check against FATF Public List of High-Risk and Other Monitored Jurisdictions** | | |
| 1. | FATF public list on high-risk and other monitored jurisdictions:  <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html> | **Any match?**  **Yes/  No**  \*Important: If yes, to proceed with ECDD. |
| **B4. Higher-Risk Customer Based on Risk Assessment Conducted by Regulated Dealer** | | |
| 1. | Does the customer fit the profile of a higher-risk customer based on their own risk assessment conducted by regulated dealer? | **Yes/  No**  \*Important: If yes; to proceed with ECDD. |

# **Annex F Sample ECDD Form**

|  |  |
| --- | --- |
| **Enhanced Customer Due Diligence (“ECDD”)**  \*Note: This form should not be shown to the customer.  Where ECDD is conducted, to attach completed (1) CDD Form A, (2) CDD Form B and (3) ECDD Form, together with copies of all supporting documents. | |
| Name of regulated dealer: | Date: |
| Name of employee: | Signature of employee: |

|  |  |  |
| --- | --- | --- |
|  | **Income Level, Source of Wealth and Source of Funds** | |
| 1. | Establish the following (by reasonable means e.g. internet scanning and careful enquiries with the customer):   * 1. income level;   2. source of wealth (i.e. source of overall assets); and   3. source of funds (i.e. source of the funds used to pay for the transaction) | **Income level:**  **Source of wealth:**  **Source of funds:**  **Source of information / Documents obtained:**  \*Important:  To consider terminating the transaction if unable to establish source of income and lodge STR. |
|  | **Prior Approval from an Employee of Senior Managerial/Executive Position** | |
| 1. | Obtain prior approval from an employee holding a senior managerial or executive position before establishing/continuing dealings with a higher-risk customer. | **Approve**  **Not approve**  **Reasons for approving / not approving:**  \*Important: To terminate the transaction if approval is not given. |
| **Signature of employee of senior managerial/executive position:** |
| **Name:** |
| **Designation:** |
| **Date:** |
|  | **Enhanced On-Going Monitoring** (To be carried out at later date(s), determined by the regulated dealer) | |
| 1. | Conduct enhanced ongoing monitoring on the transactions performed by that higher-risk customer i.e. consider regularly checking against all sections of CDD and ECDD. | **Date of recheck:** |
| **Remarks:** |
| **Signature:** |
| **Name of employee:** |
| **Designation:** |
| **Date:** |

# **Annex G Guidance on Non Face-to-Face (“F2F”) Identity Verification**

**General Comments**

The Ministry of Law supports the use of technology by regulated dealers for identity verification when carrying out CDD. This could be through using the Singpass app, MyInfo, video conferencing or third-party verification.

Regulated dealers need to ensure that the ML/TF/PF risks are adequately assessed and managed through a risk-based approach. Additional checks should be applied to manage the risk of impersonation. When non F2F identity verification is used, the process should be as robust as measures performed in-person.

Regulated dealers who choose to deploy non F2F identity verification are still required to ensure compliance with record keeping requirements. Where available, technological solutions that can detect possible fraudulent/tampered documents or impersonation should be adopted.

We have listed our guidance below when using non F2F identity verification.

|  |
| --- |
| **Singpass App**  The Singpass app installed and activated on the individual’s mobile device is also considered a government-issued identity document bearing the photograph of a customer. Regulated dealers should view the electronic NRIC on the customer’s Singpass app and retain a copy of the electronic NRIC sighted. |
| **MyInfo**  Regulated dealers may use the MyInfo platform for CDD purposes to verify the individual’s identity, including name, NRIC number, date of birth, nationality and residential address. Regulated dealers should maintain proper records of data obtained from MyInfo. |
| **Video Conferencing**  Real-time video conferencing that is comparable to F2F communication should be used to sight the original identification documents. This is in addition to obtaining electronic or scanned copies of identification documents. Signatures should also be collected through a secure digital signature using a set of Public Key Infrastructure-based credentials issued by a certified Certificate Authority under the Electronic Transaction Act. Where available, biometric technologies should be considered to incontrovertibly link the transaction to the individual. |
| **Third-Party Verification**  Regulated dealers may rely on third-parties (e.g., payment service providers regulated by MAS) to perform CDD measures if all the following conditions are met:   1. Satisfied that the third party to be relied on: 2. is subject to and supervised for compliance with requirements for the prevention of money laundering and the financing of terrorism consistent with standards set by the FATF; 3. has adequate measures in place to comply with those requirements; and 4. is willing and able to provide, without delay, on the regulated dealer’s request, any document acquired by the third party as a result of the customer due diligence measures performed for the regulated dealer; 5. the third party is not precluded from acting as such by the Registrar; 6. appropriate steps are taken to identify, assess and understand the risks of money laundering and the financing of terrorism in the countries or territories that the third party operates in (if applicable); 7. the third party is not relied upon to conduct ongoing monitoring; and 8. basis of the assessment for (a) is documented and all the CDD documents acquired by third party is obtained.   Regulated dealers remain responsible for compliance with the obligations to conduct CDD, even if they rely on third parties for the performance of CDD measures. |

1. Regulated dealers should check against the FATF public lists of high-risk and other monitored jurisdictions at https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html

   <https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html> periodically as the lists are updated. [↑](#footnote-ref-2)
2. Subject to section 57 of the CDSA and section 10B of the TSOFA on tipping-off, information shared may include an STR, the underlying information of the STR, or the fact that an STR was filed. [↑](#footnote-ref-3)
3. Please note section 57 of the CDSA and section 10B of the TSOFA on tipping-off. [↑](#footnote-ref-4)
4. Red flag indicators compiled from MAS’s Guidelines to MAS Notice 626 on Prevention of Money Laundering and Countering the Financing of Terrorism, and Sound Practices to Counter Proliferation Financing. [↑](#footnote-ref-5)
5. Red flag indicators complied from MAS’s Risk of Misuse of Legal Persons and ABS’s Legal Persons – Misuse Typology and Best Practices. [↑](#footnote-ref-6)
6. Red flag indicators compiled from IRAS’s Beware of GST Missing Trader Fraud Involving Precious Metals. [↑](#footnote-ref-7)