

## IMAS Guidance to Assessing Money Laundering and Financing of Terrorism (ML/FT)

### Risk

Please note that this template is intended only to provide general guidance to assessing ML/FT risk. It is not meant to be mandatory nor definitive. Companies should adjust the template accordingly to their own specific circumstances. IMAS accepts no liability for any errors or omissions in this template, or for any actions or decisions taken or not taken as a result of using this template.

### **Risk Assessment**

To conduct the risk assessment, first assess your company's risk score in the various components in Appendix 1 and 2. Then adjust the risk weight accordingly to your company specific conditions, and enter the risk scores in the table below to arrive at the Risk Assessment Score. (Please refer to the next page for an example on how to carry out the risk assessment)

- a) A Risk Score (1-Lower risk, 5-Higher Risk) is assigned to each individual factor based on its relative importance in identification of ML/TF risks.
- b) Each Risk Score is then weighted according to its level of risk exposed by the Company based on the individual factors. A weighted summation of the Risk Scores gives an overview of the risk exposure on an enterprise-wide basis. Refer to Appendix 2 and 3 for possible approaches and considerations in deriving the Risk Scores.

Risk Factors	Risk Weight	Risk Score	Weighted Risk Score
<b>I. ML/TF Risk Internal Governance Framework</b>			
I.1 Compliance programme			
I.2 Management support			
I.3 Documentary process			
I.4 Risk assessment conduct			
I.5 Frequency of assessment			
<b>II. ML/TF Risk Factor Assessment</b>			
II.1 Client risk			
II.2 Country risk			
II.3 Products, services and delivery channels			
II.4 Higher risk business activities			
<b>III. ML/TF Risk Mitigation Assessment</b>			
III.1 Vulnerabilities to ML/TF risks			
III.2 Appropriate EDD process			
III.3 Customers' risk mitigation assessment			
III.4 Customer transaction assessment			
III.5 Customer screening procedures			
III.6 Business activities review			
III.7 Periodic ML/TF audits			
<b>IV. ML/TF Training and Coordination</b>			
IV.1 Communication of new regulations			
IV.2 Staff training			
<b>Risk Assessment Score</b>			

### Risk Assessment (Example)

In this example, risk weights of 20%, 40%, 30% and 10% has been allocated to I. ML/TF Risk Internal Governance Framework, II. ML/TF Risk Factor Assessment, III. ML/TF Risk Mitigation Assessment and IV. ML/TF Training and Coordination respectively. Note that the summation of the risk weights must be 100%.

The risk score was obtained in Appendix 1 and 2 and then inserted under the 'risk score' column. The 'weighted risk score' was then derived by multiplying the risk weight and risk score.

Risk Factors	Risk Weight	Risk Score	Weighted Risk Score
<b>I. ML/TF Risk Internal Governance Framework</b>	<b>20%</b>		
I.1 Compliance programme	3%	2	0.06
I.2 Management support	8%	2	0.16
I.3 Documentary process	3%	3	0.09
I.4 Risk assessment conduct	3%	4	0.12
I.5 Frequency of assessment	3%	3	0.09
<b>II. ML/TF Risk Factor Assessment</b>	<b>40%</b>		
II.1 Client risk	10%	2.3	0.23
II.2 Country risk	10%	2.19	0.22
II.3 Products, services and delivery channels	5%	2.41	0.12
II.4 Higher risk business activities	15%	2	0.3
<b>III. ML/TF Risk Mitigation Assessment</b>	<b>30%</b>		
III.1 Vulnerabilities to ML/TF risks	6%	1	0.06
III.2 Appropriate EDD process	5%	2	0.1
III.3 Customers' risk mitigation assessment	4%	2	0.08
III.4 Customer transaction assessment	5%	3	0.15
III.5 Customer screening procedures	5%	3	0.15
III.6 Business activities review	2%	4	0.08
III.7 Periodic ML/TF audits	3%	2	0.06
<b>IV. ML/TF Training and Coordination</b>	<b>10%</b>		
IV.1 Communication of new regulations	4%	1	0.04
IV.2 Staff training	6%	2	0.12
<b>Risk Assessment Score</b>	<b>100%</b>	<b>5</b>	<b>2.23</b>

a) Risk Assessment score:

- 1.0 – 2.0: ML/TF risk on an enterprise-wide basis is low
- 2.0 – 3.0: ML/ TF risk on an enterprise-wide basis is moderate
- >3.0: ML/ TF risk on an enterprise-wide basis is high

b) Results of Assessment:

A summation of the numbers indicates a Risk Assessment Score of **2.23** and hence the Company's enterprise-wide ML/ TF risk is assessed to be **moderate**.

## Appendix 1 - Periodic Enterprise-Wide Money Laundering/Terrorist Financing (“ML/TF”) Risk Assessment (Sample)

I. <i>ML/TF Risk Internal Governance Framework Assessment</i>	<u>Yes</u>	<u>No</u>	<u>Risk Score</u>	<u>Comments</u>
1. Does the Company have a legal and regulatory compliance programme that includes a designated officer that is responsible for coordinating, overseeing, reviewing and updating the firm’s ML/TF risk assessment framework conducted on an enterprise-wide level covering all business units, product lines and delivery channels?	√		2	
2. Does the Company’s senior management and Board approve its enterprise-wide ML/TF risk assessment, be apprised of the assessment results and provide full support and adequate resources towards mitigating potential ML/TF risks?	√		2	

<p>3. Does the Company have a documentary process evidencing the conduct of ML/TF risk assessment, implementation of technology systems and procedures to address the deficiencies identified and the management reporting and escalation of such matters to senior management and Board?</p> <p>Does the Company have a process to retain record of and make them available to the Authority upon request?</p> <ul style="list-style-type: none"> <li>▪ What is the local retention period for record keeping for AML documents?</li> <li>▪ Does the local retention period comply with the local regulatory requirement and group policy?</li> </ul>	√		3	
<p>4. Does the conduct of ML/TF risk assessment allow the Company to better understand its overall vulnerability to ML/TF risks and form the basis for its overall risk-based approach?</p>	√		4	
<p>5. Will the Company conduct enterprise-wide ML/TF risk assessment at least once in two years or when material trigger events occur, whichever is earlier? Material trigger events include but are not limited to the acquisition of new customer segments or delivery channels or the launch of new products or services.</p>	√		3	

<b>II. Enterprise-wide ML/TF Risk Factors Assessment</b>	<u>Yes</u>	<u>No</u>	<u>Risk Score</u>	<u>Comments</u>
<p>1. Does the Company consider ML/TF risk factors concerning its customers across its business units, product lines and delivery channels (in and outside Singapore), such as:</p> <ul style="list-style-type: none"> <li>▪ Target customer markets and segments;</li> <li>▪ Profile of existing customers (client segments broken down by number, country of domicile, and AML risk profile); and</li> <li>▪ Volume and size of its transactions and fund transfers, considering the usual activity and risk profile of its customers.</li> </ul>	✓ Please refer to App2 for details		2.30	
<p>2. In relation to its own business activities and the customers assessed in II.1., does the Company consider ML/TF risk factors concerning countries or jurisdictions where there is relatively higher levels of corruption, organised crime or inadequate anti-money laundering and countering of financing of terrorism measures (“AML/CFT”)?</p>	✓ Please refer to App2 for details		2.19	
<p>3. In relation to its products, services, transactions and delivery channels, does the Company consider the following attributes:</p> <ul style="list-style-type: none"> <li>▪ Nature, scale, diversity and complexity of its business activities;</li> <li>▪ Nature of products and services offered;</li> <li>▪ Nature of delivery channels utilised?</li> </ul> <p>Does the Company also consider the following factors:</p> <ul style="list-style-type: none"> <li>▪ Whether reliance is placed on Customer Due Diligence</li> </ul>	✓ Please refer to App2 for details		2.41	

<p>(CDD) conducted by third parties. If so, what are the checks in place?</p> <ul style="list-style-type: none"> <li>▪ What payment processes are utilised? Are payments made to third parties?</li> <li>▪ Whether the firm’s products, services, transactions and delivery channels particularly susceptible to the following higher risk prevailing crime types. <ul style="list-style-type: none"> <li>▪ Unlicensed moneylending</li> <li>▪ Fraud</li> <li>▪ Criminal breach of trust</li> <li>▪ Foreign funding of terrorist activities</li> <li>▪ Corruption</li> </ul> </li> </ul>				
<p>4. Does the Company have business relationships with the following persons or entities identified as potentially presenting higher ML/TF risks:</p> <ul style="list-style-type: none"> <li>▪ Shell banks or shell companies;</li> <li>▪ Persons or private legal entities controlled or influenced by Politically Exposed Persons, their family and close associates, or state-owned entities;</li> <li>▪ Entities that provide correspondent account services; and</li> <li>▪ Higher ML/TF risk entities in certain non-financial sectors identified in Singapore’s National ML/TF Risk Assessment Report (such as, casinos, pawnbrokers, moneylenders and precious stones and metal dealers) or FATF’s Mutual Evaluation Reports?</li> </ul>		√	2	

<b>III. Enterprise-wide ML/TF Risk Mitigation Assessment</b>	<u>Yes</u>	<u>No</u>	<u>Risk Score</u>	<u>Comments</u>
1. Does the Company take into consideration the vulnerabilities to ML/TF risks face into assessment and if there are any risk mitigation approaches?	√		1	
2. Does the Company determine the appropriate level of enhanced due diligence necessary for categories of customers it has reason(s) to believe pose a heightened risk of conducting illicit activities?	√		2	
3. Does the Company assess its customers' ML/TF risk mitigation policies or practices, where relevant?	√		2	
4. Does the Company complete a risk-based assessment to understand the normal and expected transactions of its customers?	√		3	
5. Does the Company screen customers against a list of persons, entities and countries issued by governments and competent authorities and against known databases for derogatory information or association to identify changes in customer profile?	√		3	

<p>6. Does the Company conduct a review to assess if existing and new business activities, products and delivery channels would be susceptible to potential abuse and prevailing crime types?</p> <ul style="list-style-type: none"> <li>▪ Have there been any significant changes in the business model or client profile impacting the AML/CTF activities?</li> </ul>	√		4	
<p>7. Is the Company subject to periodical internal audits and annual statutory audits which cover its adherence with regulatory requirements as part of audit scope?</p>	√		2	



<b>IV. Enterprise-wide AML/CFT Training and Coordination Assessment</b>	<u>Yes</u>	<u>No</u>	<u>Risk Score</u>	<u>Comments</u>
1. Does the Company communicate new AML/CFT laws and regulations and their changes, and updates to internal policies or practices to employees?	√		1	
2. Does the Company provide AML/CFT training to its employees that includes, amongst others, these coverage: <ul style="list-style-type: none"> <li>▪ Specific AML/CFT regulatory requirements;</li> <li>▪ Internal policies and procedures on AML/CFT;</li> <li>▪ Examples of different forms of ML/TF and live case-studies; and</li> <li>▪ Identification of ML/CFT red flags and reporting of transactions that must be reported to government authorities?</li> <li>▪ Do all staff undertake AML Training?</li> <li>▪ How often is the training provided?</li> <li>▪ Do all staff receive the same training?               <ul style="list-style-type: none"> <li>▪ If no, describe the differences in training e.g. frequency of training, level of training.</li> </ul> </li> </ul>	√		2	

## Appendix 2 – Risk Scoring

Refer to Appendix 3 – Additional Considerations, Part II - Enterprise-wide ML/TF Risk Factors Assessment when considering the appropriate risk score in your assessment.

### A1.1 Client Risk Assessment for Different Client Types

Risk Level	Risk Score	No. of clients (Retail)	No. of clients (Institutional)	Total No. of Clients	Score	Average Score
Higher Risk	5	5	1	6	30	
High Risk	4	10	2	12	48	
Medium Risk	3	20	3	23	69	
Low Risk	2	25	3	28	56	
Lower Risk	1	30	4	34	34	
<b>Total</b>		<b>90</b>	<b>13</b>	<b>103</b>	<b>237</b>	<b>2.30</b>

Risk Score can be self-assessed by individual companies according to internal policies. Factors to consider may include sensitive Industries, as well as volume and size of transactions.

### A1.2 Client-Country Risk Assessment

Risk Level	Risk Score	No. of clients in Country 1	No. of clients in Country 2	Total No. of Clients	Score	Average Score
Higher Risk	5	5	2	7	35	
High Risk	4	10	4	14	56	
Medium Risk	3	20	6	26	78	
Low Risk	2	30	8	38	76	
Lower Risk	1	40	10	50	50	
<b>Total</b>		<b>105</b>	<b>30</b>	<b>135</b>	<b>295</b>	<b>2.19</b>

Risk Score can be self-assessed by individual companies according to internal policies. Factors to consider may include evidence of adverse news, independent assessment of country's overall AML/CFT regime, AML/CFT laws and regulations, implementation of AML/CFT standards, FATF membership, and contextual factors of concern.

### A1.3 Client-Product-Channel Risk Assessment

Risk Level	Risk Score	No. of clients in Channel 1	No. of clients in Channel 2	Total No. of Clients	Score	Average Score
Higher Risk	5	10	30	40	200	
High Risk	4	15	50	65	260	
Medium Risk	3	20	70	90	270	
Low Risk	2	25	90	115	230	
Lower Risk	1	30	120	150	150	
<b>Total</b>		<b>100</b>	<b>360</b>	<b>460</b>	<b>1110</b>	<b>2.41</b>

Risk Score can be self-assessed by individual companies according to internal policies. Factors to consider may include evidence of adverse news, independent assessment of country's overall AML/CFT regime, AML/CFT laws and regulations, implementation of AML/CFT standards, FATF membership, and contextual factors of concern

## Appendix 3 – Additional Considerations

### I) ML/TF Risk Internal Governance Framework Assessment

#### A. Compliance Programme

Risk considerations for Compliance Programme can include:

- What is the structure of AML/CFT management and how are AML responsibilities are allocated within the organization?
  - *Which team completes CDD?*
  - *Is there oversight/involvement from Compliance/local MLRO?*
  - *Is technology used in the completion of CDD?*
  - *Are there are plans to adopt other technology-based or automated solutions for AML/CFT risk management purposes?*
    - If yes, please elaborate.
  - *What is the current approach with regards to coordination with other functions within the firm in relation to AML/CTF?*
- In order to effectively manage business/operational unit's ML/TF risks, are there:
  - *Sufficient staff resources?*
  - *Fully competent staff resources?*
  - *Adequate systems?*
    - If not, describe the impact of this and how it is intended to manage this situation.
- Is it anticipated that there will be any circumstances which may have a negative impact upon the resource capability over the next 12 months?
- Are there processes in places to ensure effective coordination with regulatory and law enforcement agencies?
- Where there are issues with clients, to whom are these escalated to? Are there clear procedures for escalation?

- In relation to CDD testing,
  - *Does CDD testing include performance of CDD by third parties? (e.g. related entities or distributors )*
  - *How often is it conducted?*
  - *Is the required supporting documentation in place?*
  
- In terms of screening of client relationships and dealing with PEPs
  - *are there processes to:*
    - Screen new client relationships?
    - Screen all existing client relationships regularly to identify if they become a PEP?
    - Assess whether the frequency of the client screening remains appropriate?
      - *If yes, does the screening system capture names in local language/characters?*
  - *Require approval from higher management for newly identified PEP/ high risk client relationships?*
  - *Identify where PEP / high risk client approvals are still outstanding?*
  
- In the area of suspicious Activity reporting,
  - *Are procedures clear for staff to report any suspicions?*
  - *Are there adequate systems to monitor the suspicious activity?*
  - *Have all staff been made aware of their personal obligations regarding the reporting of suspicious transactions?*
  - *Are there procedures in place to ensure that suspicious activity reports are submitted and reviewed in a timely manner?*

## **B. Management Support**

Risk Considerations for Management Support can include:

- In considering the capability and responsibility of senior management in terms of AML risk,
  - *Does the responsibility for oversight of AML identity and verification checks lies with management?*
  - *How capable is senior management in being able to satisfy statutory obligations and ensuring that measures taken against the risks of ML/TF is sufficient and robust?*
  - *Does management communicate AML issues with other business units?*

- Are there requirements to seek approval from senior management onboard new clients?
- Are AML oversight arrangements remain adequately independent of the operational areas of the business?
- Does the company have a Money Laundering Reporting Officer (MLRO) who is tasked with reporting to a fund's board of directors? If yes,
  - *Who is the local MLRO?*
  - *How long they have been the MLRO?*
  - *Provide details confirming their suitability to fulfil the role e.g. training, qualifications, previous roles*
  - *Is the MLRO the focal point for the oversight of all activities relating to the prevention and detection of ML/TF?*
  - *Is the MLRO independent of all operational and business functions; as far as practicable within any constraint of the size of the firm?*
  - *Is the MLRO of a sufficient level of seniority and authority within the institution?*
  - *Is the MLRO provided with regular contact with and direct access to senior management to ensure that senior management is able to satisfy itself that the statutory obligations are being met and the measures against the risks of ML/TF is sufficient and robust?*
  - *How conversant is the MLRO in the local statutory and regulatory requirements and ML/TF risks?*

## II) Enterprise-wide ML/TF Risk Factors Assessment

### A. Client Risk

Considerations for Client Risk can include:

- What are the total number of clients as at date of assessment?
- Describe the types of clients that the firm has e.g. institutional, retail
- Provide breakdown of different types of client by numbers
- Describe the most common client structures of institutional clients
- What is the extent to which the firm deals directly with individual clients?
- Does the firm have business relationship with clients from the following sectors identified as potentially presenting higher ML/TF risks?
  - *Banks offering retail banking services*
  - *Remittance agents and money changers*
  - *Internet-based stored value facility holders*
  - *Corporate service providers (business entities and people that provide a range of services such as corporate advisory, office hosting, corporate secretarial services and statutory filings for their customer. e.g. lawyers, accountants, chartered secretaries and corporate secretarial agents)*
  - *Pawnbrokers*
- What is the level of ML/TF risks posed by the abovementioned sectors?
- Number (%) of clients identified as high risk:
  - *Clients with nationality or who are domiciled, clients incorporated or operating, in high risk jurisdictions (based on group matrix)*
  - *Clients who have politically exposed persons (PEPs) involvement*
  - *PEP - Direct (individuals)*
  - *State-Owned Entities (SOE)*
  - *Highlight any clients that have had suspicions raised due to adverse media*
  - *Number (%) of clients whereby suspicions have been raised with regard to their transactions and/ or fund transfers*

## **B. Country Risk**

Considerations for Country Risk can include:

- Evidence of adverse news or relevant public criticism of a country or jurisdiction, including FATF public documents on High Risk and Non-cooperative jurisdictions;
- Independent and public assessment of the country's or jurisdiction's overall AML/CFT regime, such as FATF or FATF-Styled Regional Bodies' ("FSRBs") Mutual Evaluation reports and the IMF / World Bank Financial Sector Assessment Programme Reports or Reports on the Observance of Standards and Codes for guidance on the country's or jurisdiction's AML/CFT measures;
- AML/CFT laws, regulations and standards of the country or jurisdiction consistent with those set by the FATF;
- Implementation of the standards (including quality and effectiveness of supervision) of AML/CFT, such as the level of control and/or regulation in the country or jurisdiction consistent with those set by FATF;
- Whether the jurisdiction is a member of FATF; and
- What is the nature of business/ background in country? E.g. distribution office, full functioning office
- List different legal entities in country
- Contextual factors of concern, such as political stability, maturity and sophistication of the regulatory and supervisory regime, level of corruption, financial inclusion, etc.
- Local jurisdiction country risk rating as per group country risk matrix
- Does the firm and/or its branches/subsidiaries operate in in any high risk countries?
  - *If yes, list countries which are rated as high risk in group matrix*
- Which high risk countries is the firm exposed to through its clients, either through place of incorporation/ place of business for non-individual clients or their nationality/ place of domicile for individual clients?
- Are there clients with residence in or connection with high-risk jurisdictions:
  - Countries identified by the FATF as jurisdictions with strategic AML/CFT deficiencies
  - Countries subject to sanctions, embargos or similar measures issued by international authorities
  - Countries that are believed to have strong links to terrorist activities

- Countries identified by the OECD (Organisation for Economic Co-operation and Development) to be an unco-operative tax haven
- Countries identified in the International Narcotics Control Strategy Report (INCSR) to be a “Jurisdiction of Primary Concern”

### **C) Products, Services and Delivery Channels**

Risk Considerations for Products, Services and Delivery Channels can include:

- What are the target client markets and segments?
- What are the different types of products and services offered
- What distribution channels are utilised? E.g. direct client relationships, indirect utilizing third parties such as distributors
- Is reliance placed on CDD conducted by third parties?
  - *If yes, then confirm what checks are in place*
- What payment processes are utilised? Are payments made to third parties?
- Are the firm’s product, services, transactions and delivery channels particularly susceptible to the following higher risk prevailing crime types?
  - *Unlicensed moneylending*
  - *Fraud*
  - *Criminal breach of trust*
  - *Foreign funding of terrorist activities*
  - *Corruption*