

ANNEXURE 1: SUGGESTED RISK ANALYSIS TEMPLATE

This template serves to guide developers to perform risk analysis to identify, assess and understand their money laundering and financing of terrorism risks, as required under the Housing Developers (Control & Licensing) Act (HDCLA) and Sale of Commercial Properties Act (SCPA), and should be adapted to suit their business context. Developers should consider the risk factors in this template and any other risk factors that are relevant to their business context before determining the overall level of risk and the appropriate type and extent of mitigation measures. . The type and extent of the mitigating measures must be appropriate to the risk of money laundering and terrorism financing and the size of developer’s business.

The risk analysis should be performed before the launch of each project and updated regularly, e.g. once every 2 years, or when material trigger events (e.g. acquisition of new customer segments) occur, whichever is earlier.

The ultimate responsibility and accountability for ensuring compliance with the HDCLA and SCPA and their respective rules, rest with the developers’ senior management eg directors, CEO etc. As part of AML/CFT oversight and governance, developers’ 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.

Section A: Risk factors to consider before every project launch

S/N	Risk factor to consider	Indicate whether risk factor is met, ie Yes or No. If yes, provide details.
(I) Countries and jurisdictions in which the developers have operations in <i>(Note: If Risk Factor 1 is met, developer should rate itself as “high-risk”.)</i>		
1	High risk countries or jurisdictions subject to a call for action by FATF (“FATF black list”)	
2	Countries or jurisdictions that are subject to increased monitoring by Financial Action Task Force (FATF) (“FATF grey list”)	
(II) Developers’ services, transactions and delivery channels <i>(Note: If Risk Factor 3 is met, developer should rate itself as “high-risk”.)</i>		
3	Target median selling price exceeds \$3 million.	
4	Sole/heavy reliance on online platforms for marketing, without physical face-to-face interactions with purchasers	
(III) Profile of developers’ higher-risk purchasers <i>(Note: The following risk factors should be considered after project is launched and units sold. If any of the risk factors is met, developer should rate itself as “high-risk”.)</i>		

5	≥20% of purchasers who are non-Singapore Citizens (e.g. PRs, foreigners, entities and legal arrangements)	
6	Purchasers buying ≥2 properties within 1 year	
7	Purchasers holding multiple travel documents or possess travel documents issued by countries known to offer citizenship and residency by investment (CBI/RBI) programmes or countries flagged FATF	
8	Purchasers originating from or are residents of : a) high-risk countries or jurisdictions subject to a call for action (“FATF black list”); b) countries or jurisdictions that are subject to increased monitoring (“FATF grey list”)	
IV) Other factors considered by developers, e.g. receipt of unrelated third party payments, foreign PEP purchasers		
9	<i>(Developers to list down relevant risk factors)</i>	
V) Overall risk rating		
10	Developer’s overall risk level	Low/Medium/High

Section B: Size of Developer’s Business

Developer to state its size of business in the table below

Size of Developer’s Business	
Factors considered in determining the size of its business, e.g. gross development value (GDV) of licensed project.	E.g. GDV of licensed project: \$___ mil
Size of business	Small/Medium/Large

Section C: Risk Mitigating Measures

Measures should commensurate with the risk level and size of the developer’s business.

Risk mitigating measures	
<i>(Note: these are examples that developers may consider)</i>	
Implement a system of performing CDD and ECDD checks	
Training of staff	<i>State type of training provided, topics covered (e.g. assessed risk level of project), measures put in place to mitigate risk and when is the training conducted (e.g. before project launch). Where risk level is</i>

	<i>assessed to be high, the developer should consider more rigorous training and increase the frequency.</i>
Review of risk analysis	<i>Where risk level is assessed to be high, developers should consider conducting more frequent review and seeking approval level from the highest level for the risk analysis.</i>
Independent auditor to audit CDD and ECDD process, in addition to audit checks on IPPC	<i>Where risk level is assessed to be high, developers should consider increasing the frequency of audit</i>
Review of transactions	<i>Where risk level is assessed to be high, developers should consider conducting more frequent review of transactions</i>

Section D: Developer's acknowledgement of risk analysis report

Completed by:	
Name	
Designation	
Date	
Approved by:	
Name	
Designation <i>(Note: The Risk Analysis must be approved by the Senior Management eg director or CEO)</i>	
Date	
Date of next review:	
Target date of developer's next risk analysis <i>(Note: The risk analysis should be performed before the launch of each project and updated regularly eg once every 2 years, or when material trigger events (e.g. acquisition of new customer segments) occur, whichever is earlier.)</i>	