GUIDELINES FOR DEVELOPERS ON PREVENTION OF MONEY LAUNDERING, PROLIFERATION FINANCING AND TERRORISM FINANCING

Version Control Record

Version	Release Date	Key Changes
1.0	10 March 2023	• First release
1.1	17 April 2023	• Updated para 1.3 to state that the URL https://go.gov.sg/ura-amltf can be accessible from 28 June 2023 onwards • Updated the FATF URL on countries subject to counter measures or ECDD, and countries subject to increased monitoring at paragraphs 2.1, 4.2.3ii, Annexure 2 item 2.4a, • Updated paragraph 6.3.6c – MAS website on Regulations under the United Nations Act 2001 ("UN Act") • Updated paragraphs 9, 10 and 11- included SCDD as one of the allowable measures • Updated paragraph 13.1 – Included "Prescribed form to notify purchasers of the information/documents required for CDD checks" and "records of CDD conducted" as one of the documents for record keeping
1.2	21 January 2025	• Included definition of "Relevant Person" • Updated Section 4.2 on "How to Perform Risk Analysis" • Updated Section 6 on "Customer Due Diligence (CDD)" • Updated Section 7 on "Enhanced CDD" • Inserted new Annexure 1 on "Suggested Risk Analysis Template" • Updated Annexure 2 on "Checklist for Conducting Customer Due Diligence" • Updated CDD Forms and Inserted a new CDD Form D
1.3	30 June 2025	• Updated Definitions of Terms Used in Guidelines • Updated para 3.2 to include Proliferation Financing • Inserted References to Proliferation Financing, where relevant • Included key areas to be included in the IPPC under Section 5 • Updated Section 6.3 on "How to Perform CDD" • Updated Section 7.3 on "Requirements of ECDD" • Updated Section 12 on the timeline to file an STR

		• Updated Section 14 on “Additional Measures Relating to Targeted Financial Sanctions” • Updated Annexure 2 on “Checklist for Conducting Customer Due Diligence” • Updated Forms C to G
1.4	07 July 2026	• Inserted definition of “International Organisation” • Updated paragraph 5.1.3a on the appointment and role of the compliance officer • Updated Section 6 on “Customer Due Diligence (CDD)” • Updated Section 7 on “Enhanced CDD” • Updated Section 11 on “Ongoing Monitoring of Transactions” • Updated Section 12.1 on “Submitting a Suspicious Transaction Report” • Shifted Section 14 on “Additional Measures Relating to Targeted Financial Sanctions” to Section 6.4 to consolidate Guidelines relating to the Sanctions List • Updated Annexure 1 on “Suggested Risk Analysis Template” • Inserted new Annexure 3 on “Flow chart for CDD/ECDD Checks Prior to Property Transactions”

Table of Contents

1 Introduction 6

2 Definition of Terms Used in Guidelines 7

3 Money Laundering, Proliferation Financing and Terrorism Financing 10
- 3.1. What is Money Laundering
- 3.2. What is Proliferation Financing
- 3.3. What is Terrorism Financing
- 3.4. Implications of ML, PF and TF for Singapore

4 Risk Analysis 11
- 4.1. Risk-Based Approach
- 4.2. How to Perform Risk Analysis

5 Programmes and Measures to Prevent Money Laundering, Proliferation Financing and Terrorism Financing 13
- 5.1 Governance on Prevention of ML/PF/TF
- 5.2 Training of Employees
- 5.3 Audit Function

6 Customer Due Diligence ("CDD") 15
- 6.1 What is CDD
- 6.2 When to Perform CDD
- 6.3 How to Perform CDD
- 6.4 Screening and Targeted Financial Sanctions Obligations
- 6.5 Failure to Satisfactorily Perform or Complete CDD Measures

7 Enhanced Customer Due Diligence ("ECDD") 20
- 7.1 What is ECDD
- 7.2 When to perform ECDD
- 7.3 Requirements of ECDD
- 7.4 How to perform ECDD

8 Simplified Customer Due Diligence ("SCDD") 24
- 8.1 When to perform SCDD
- 8.2 Requirements of SCDD
- 8.3 How to perform SCDD

9 Customer Due Diligence on Existing Purchasers 25

10 Performance of Customer Due Diligence Measures by Third Parties 25

11 Ongoing Monitoring of Transactions 26

12 Reporting of Suspicious Transactions 27
12.1 Submitting a Suspicious Transaction Report

13 Record Keeping 27

14 Identifying Risks from New Technologies 27

15 Managing and Mitigating Risks from New Technologies 28

Annexures

Annexure 1: Risk Analysis Template 29

Annexure 2: Checklist for Conducting Customer Due Diligence 32

Annexure 3: Flow Chart for Customer Due Diligence / Enhanced Customer Due Diligence Checks Prior to Property Transactions 41

CDD Forms

Form A1: Purchaser's Particulars Form for Natural Persons 43

Form A2: Purchaser's Particulars Form for Entities 46

Form A3: Purchaser's Particulars Form for Legal Arrangements 49

Form B: Details of Person(s) Acting on Behalf of Purchaser 53

Form C: Details of Beneficial Owner(s) of an Entity or Legal Arrangement Purchaser 55

Form D: Details of Natural Person(s)/Entity/Legal Arrangement on whose behalf the Purchaser (who is a Natural Person) is Acting 56

Form E: Details of Politically Exposed Person(s) 64

Form F: Screening of Purchasers for Money Laundering, Proliferation Financing and Terrorism Financing Risks 66

Form G: Ongoing Monitoring of Transactions 72

1 Introduction

1.1 All developers are subject to regulatory requirements[1] under the following legislation:

a. Housing Developers (Control and Licensing) Act 1965 ("HDCLA") and its Rules; and

b. Sale of Commercial Properties Act 1979 ("SCPA") and its Rules.

1.2 This set of guidelines aims to provide guidance to developers of residential and non-residential properties on the requirements pertaining to prevention of money laundering, proliferation financing and terrorism financing under the HDCLA, Housing Developers (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Rules, SCPA and Sale of Commercial Properties (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Rules ("the Acts and Rules"). Developers regulated under the HDCLA and SCPA will be subject to these requirements.

1.3 The guidelines are not meant to be exhaustive and may be amended from time to time. Developers are advised to refer to the latest version of the guidelines on https://go.gov.sg/ura-amltf .

1.4 It is the responsibility of developers to ensure that they are in compliance with all regulatory requirements.

[1] Developers are also subject to other laws (e.g. Terrorism (Suppression of Financing) Act 2002, United Nations Act 2001 and Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992).

2 Definition of Terms Used in Guidelines

2.1 The following table summarises some key terms used in this set of Guidelines. Please refer to the Acts and Rules for the full definition of these terms.

Terms	Definitions
Beneficial Owner (BO)	In relation to an entity or a legal arrangement, refers to an individual: a) who ultimately owns or controls the entity or legal arrangement; b) who exercises ultimate effective control over the entity or legal arrangement; or c) on whose behalf the entity or legal arrangement conducts any transaction with a developer. For example, if a company purchases a property in a building project, the individual who meets the above criteria is referred to as the BO. Whether an individual exercises ultimate effective control depends on the ownership structure of the entity or legal arrangement may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).
Close Associate of a PEP	Means: a) a partner of the PEP; b) a person accustomed or under an obligation, whether formal or informal, to act in accordance with the directions, instructions or wishes of the PEP; c) a person whose directions, instructions or wishes the PEP is accustomed or under an obligation, whether formal or informal, to act in accordance with; or d) a person with whom the PEP has an agreement or arrangement, whether oral or in writing and whether express or implied, to act together.
Domestic Politically Exposed Person ("Domestic PEP")	Means an individual who is or has been entrusted with any prominent public function in Singapore
Family Member of a PEP	Means a spouse, a child, an adopted child or a stepchild, a sibling, an adopted sibling or a stepsibling or a parent or step-parent, of the PEP.

Foreign Country	Means a country, territory or jurisdiction other than Singapore.
Foreign Politically Exposed Person ("Foreign PEP")	Means an individual who is or has been entrusted with a prominent public function in a foreign country.
Identifying Information	Means all of the following information: a) full name, including any alias used; b) date of birth, for an individual; c) place of birth, for an individual; d) address, which must be — (i) for an individual, the address of the individual's usual place of residence; or (ii) for a body corporate or unincorporate, the address of its registered office and principal place of business; e) contact number or numbers; f) nationality, for an individual, or place of incorporation or registration, for a body corporate or unincorporate; g) identification number, which must be — (i) for an individual, an identity card number, a passport number, a taxpayer identification number, or the number of any other document of identity issued by a government as evidence of the individual's nationality or residence and bearing a photograph of the individual; or (ii) for a body corporate or unincorporate, a registration number, or the number of any other document issued by any government certifying the incorporation, registration or existence of the body corporate or unincorporate; h) the type of identifying document mentioned in paragraph (*g*) and the expiry date (if any) of the identifying document; and i) the occupation, for an individual, or the nature of the business, for a body corporate or unincorporate.
International Organisation	International Organisations are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organization for Security and Cooperation in

	Europe and the Organization of American States; military international organisations such as the North Atlantic Treaty Organization and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.
International Organisation Politically Exposed Person	Means an individual who is or has been a member of the senior management of an international organisation (including a director, deputy director or member of a board of the international organisation, or an equivalent appointment in the international organisation).
Politically Exposed Person (PEP)	Means a domestic politically exposed person, a foreign politically exposed person or an international organisation politically exposed person.
Prominent Public Function	Includes the role held by — a) a head of state; b) a head of government; c) a government minister; d) a senior politician; e) a senior civil or public servant; f) a senior government, judicial or military official; g) a senior executive of a state-owned corporation; h) a senior political party official; or i) a member of the legislature;
Relevant Country	Means a foreign country that is subject to a call made by the FATF through a public statement, notice or directive published on its official website at: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html for countermeasures or enhanced customer due diligence measures.
Relevant Person	Means a purchaser, a beneficial owner of a purchaser, a person on whose behalf a purchaser is acting or a beneficial owner of that person.

3 Money Laundering, Proliferation Financing and Terrorism Financing

3.1 What is Money Laundering

3.1.1 Money laundering ("ML") is a process intended to mask the benefits derived from criminal conduct so that they appear to have originated from a legitimate source. Singapore's primary legislation to combat ML is the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("CDSA").

3.1.2 There are 3 stages involved in ML:

a. **Placement** – Placement occurs when the proceeds from illegal activities are first introduced into the economy and financial system. This can be done by splitting the money into smaller amounts and depositing them into a bank account, by investing the monies in different ways such as purchasing financial instruments, valuable goods or real estate.

b. **Layering** – Layering refers to separating illicit/criminal proceeds from their source by creating layers of transactions designed to disguise the source of money and to obscure the audit trail. The funds might be channelled through the purchase and sale of investment instruments/properties or be wired through multiple bank accounts. For example, after the property bought is resold, a money launderer could use the illicit funds to pay for renovations to increase the value of the property.

c. **Integration** – Integration means placing the laundered funds back into the economy and financial system with the appearance of being legitimate funds. For example, cash obtained from the sale of properties are banked into accounts, or the money launderer may rent the property to get income from the investment before selling it.

3.2 What is Proliferation Financing

3.2.1 Proliferation financing ("PF") refers to the raising, moving, or making available of funds, other assets or other economic resources, or financing, in whole or in part, to persons or entities for purposes of weapons of mass destruction proliferation, including the proliferation of their means of delivery or related materials (including both dual-use technologies and dual-use goods for non-legitimate purposes).

3.2.2 Singapore gives effect to the United Nations Security Council Resolutions ("UNSCR") which prohibit specified transactions with individuals and entities designated as being involved in the proliferation of weapons of mass destruction and its financing.

3.3 What is Terrorism Financing

3.3.1 Terrorism financing ("TF") involves providing services, supplies, materials and assets to support terrorist organisations and their activities. Terrorism seeks to influence, compel, or intimidate governments or the general public through threats, violence, or damage to property. The Terrorism (Suppression of Financing) Act 2002 ("TSOFA") was enacted in Singapore to combat this threat.

3.3.2 TF may be financed using legitimate funds (e.g. business or charitable funds/donations) or illegitimate funds (e.g. from extortion or drug trafficking). While TF may not always involve large sums of monies, the methods used, particularly by terrorist organisations, to raise, move, or conceal funds for their activities can be similar to those used by criminal organisations to launder their funds.

3.4 Implications of ML, PF and TF for Singapore

3.4.1 ML, PF and TF pose serious risks to Singapore's safety and security as they enable harmful criminal activities to go undetected. Due to the trans-border nature of ML, PF and TF, they also threaten Singapore's reputation as a trusted international financial and trading centre. Disrupting and preventing these terrorism-related financial flows and transactions help to fight terrorism. It is therefore critical for all stakeholders to play an active role in addressing these threats.

4 Risk Analysis

4.1 Risk-Based Approach

4.1.1 The purpose of the prevention of money laundering, proliferation financing and terrorism financing (ML/PF/TF) regulatory and supervisory regime is to manage and effectively mitigate the ML/PF/TF risks faced by developers.

4.1.2 Developers are required to perform, in relation to each purchaser, an adequate analysis of the ML/PF/TF risks associated with the purchaser, assess the ML/PF/TF risks faced by developers' businesses and adopt a risk-based approach to address these risks.

4.1.3 Under the risk-based approach, developers must:

a. identify, assess and understand the ML/PF/TF risks in their business;

b. take reasonable steps to manage and mitigate those ML/PF/TF risks; and

c. ensure that programmes and measures to manage and mitigate ML/PF/TF risks commensurate with the level of ML/PF/TF risks identified.

4.2 How to Perform Risk Analysis

4.2.1 Before launching any project for sale, developers must take appropriate steps to identify, assess and understand the ML/PF/TF risks in relation to:

a. their purchasers[2];

b. the countries and jurisdictions which their purchasers are from or in;

c. the countries and jurisdictions in which developers have operations; and

d. their services, transactions and delivery channels.

4.2.2 In performing the risk analysis, developers must consider all relevant risk factors for each project regulated under the HDCLA and SCPA, before determining the developer's overall risk level. Thereafter, developers must:

a. document their risk analysis;

b. implement risk mitigating measures that are commensurate with the overall risk level and size of the developer's business;

c. keep their risk analysis up to date. For example, developers could consider reviewing their risk analysis once every 2 years, or when material trigger events occur, whichever is earlier. Material trigger events include, but are not limited to, acquisition of new customer segments etc; and

d. have appropriate mechanisms to provide their risk analysis to the Controller of Housing, as appointed under Section 3(1) of the HDCLA.

4.2.3 Developers may refer to the risk analysis template in Annexure 1 to guide them in performing their risk analysis.

4.2.4 Developers should consider all the following when determining if the purchaser presents a higher risk of ML, PF or TF:

a. whether the relevant person is a resident of or originates from[3]:

i. a relevant country;

[2] To understand the ML/PF/TF risks of purchasers, developers can refer to the Monetary Authority of Singapore's website for the lists of designated individuals and entities whom developers must decline to enter into any transaction or terminate any transaction entered into with the purchaser, and file a Suspicious Transaction Report (STR), if there is a match. (http://www.mas.gov.sg/regulations-and-financial-stability/anti-money-laundering-countering-the-financing-of-terrorism-and-targeted-financial-sanctions/targeted-financial-sanctions/lists-of-designated-individuals-and-entities.aspx).

[3] Refers to the relevant person's current citizenship.

ii. a foreign country that the FATF, by a public statement, notice or directive published on its official website at https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html, identifies as a foreign country subject to increased monitoring. As defined by FATF, these are countries that are actively working with FATF to address strategic deficiencies in their regimes to counter ML, PF or TF; or

iii. a foreign country that the Controller has notified the developers to be a foreign country with inadequate measures to prevent ML, PF or TF.

b. whether the transaction with the purchaser is complex or unusually large or is part of an unusual pattern of transactions which have no apparent economic or visible lawful purpose[4].

c. whether the relevant person or any person acting on behalf of the purchaser is suspected of, or at risk of, facilitating ML, PF or TF, as notified by the Controller or other relevant authorities.

5 Programmes and Measures to Prevent Money Laundering, Proliferation Financing and Terrorism Financing

5.1 Governance on Prevention of ML/PF/TF

5.1.1 The commitment, participation and authority of the developer is important to a sound risk management framework to prevent ML/PF/TF. Developers should ensure that their risk mitigating measures are adequate, robust, and effective. The successful implementation of a risk-based approach to prevent ML/PF/TF requires developers to have a good understanding of the ML/PF/TF risks they are exposed to.

5.1.2 The ML/PF/TF risks are not static as criminals will modify their ML/PF/TF methods to avoid detection and overcome measures put in place to manage ML/PF/TF risks. To encourage proper governance and a culture of compliance to prevent ML/PF/TF, developers and the Senior Management in the developers (e.g. a director, Chief Executive Officer) should:

a. obtain sufficient information to form an accurate picture of the ML/PF/TF risks, including emerging or new ML/PF/TF risks;

b. obtain sufficient and objective information to assess whether the developers' controls are adequate and effective to prevent ML/PF/TF;

[4] Complex transactions include attempts to disguise the BO(s) involved in the transaction, use of unnecessarily complex transaction structures designed to obscure the true nature of the transaction or involving the use of multiple intermediaries for the transaction. Unusually large transactions could include a transaction priced at more than the usual or expected amount for a similar typical transaction. Transactions with no apparent economic or lawful purpose could include using trust and company service providers to set up a number of corporate structures in multiple jurisdictions for the transaction without any apparent purpose.

c. obtain information on legal and regulatory developments and the impact these have on developers' frameworks to prevent ML/PF/TF; and

d. ensure that processes are in place to escalate important decisions that directly impact the ability of developers to manage and mitigate ML/PF/TF risks, especially where controls are assessed to be inadequate or ineffective to prevent ML/PF/TF.

5.1.3 Developers must develop and implement policies, procedures and controls (IPPC), which must be approved by their Senior Management[5], taking into consideration the ML/ PF and TF risks and the size of their business. This is to manage and effectively mitigate the ML, PF and TF risks identified or notified by the Controller in writing. The IPPC should include the following areas:

a. appropriate compliance management arrangements, including the appointment of a compliance officer. The compliance officer must have the necessary authority to ensure that the developer complies with the requirements to prevent money laundering, proliferation financing and terrorism financing, e.g. conduct or arrange for independent audits on the internal policies, procedures and controls, take remedial actions in a timely manner if any non-compliance is noted. The developer should ensure that the appointed compliance officer plays a managerial role and is duly authorised to perform the necessary duties;

b. adequate ML/PF/TF screening procedures when hiring employees; and

c. scope and frequency of developer's training programme for its staff.

5.1.4 For a developer that is a company incorporated in Singapore and has a branch or subsidiary, whether in Singapore or elsewhere, the developer must develop and implement a group-level programme to prevent ML, PF and TF. The programme must:

a. be applicable to all the developer's branches and subsidiaries, whether in Singapore or elsewhere;

b. include the measures mentioned in paragraphs 4.2.1 and 4.2.2;

c. be appropriate to the business of the developer's branches and subsidiaries;

d. be implemented effectively at the level of the developer's branches and subsidiaries;

[5] The policies, procedures and controls must be approved by the Senior Management of the developers. "Senior Management" refers to the persons who are responsible for the management and conduct of the business of the company. They have strategic decision-making authority and hold the highest level of executive responsibility in the developer company, e.g. Director, Chief Executive Officer or Chief Financial Officer, of the developer. Developers may also seek approval from their Board of Directors for the policies, procedures and controls, depending on their internal company policy.

e. include policies and procedures for providing and sharing information required for the purposes of CDD measures and generally for the management of risks relating to ML, PF and TF; and

f. include adequate safeguards on the confidentiality and use of information exchanged between the developer and its branches and subsidiaries.

5.1.5 If the developer has a branch or subsidiary in a country or territory outside Singapore that has laws for the prevention of ML, PF or TF that differ from those in Singapore:

a. the developer must require the management of that branch or subsidiary to apply the more stringent set of laws, to the extent that the law of the host country or territory permits; and

b. if that branch or subsidiary is unable to fully apply the more stringent set of laws, the developer must report this to the Controller and must, in lieu of paragraph (a), comply with the Controller's directions.

5.2 Training of Employees

5.2.1 Developers must have an ongoing programme to train employees on their IPPC. Examples include:

a. roles and responsibilities of developers in combating ML/PF/TF, and in particular, CDD measures, and detecting and reporting of suspicious transactions; and

b. internal policies, procedures and controls to prevent ML/PF/TF.

5.2.2 The scope and frequency of training should be tailored to the specific risks faced by the developer and pitched according to the job functions, responsibilities and experience of the employees and officers.

5.2.3 Employees should have a good understanding of the ML/PF/TF risks inherent in the developer's business.

5.3 Audit Function

5.3.1 Developers must have an independent audit function to test the policies, procedures and controls as mentioned in paragraph 5.1.3, monitor the implementation and enhance the policies, procedures and controls if necessary.

6 Customer Due Diligence ("CDD")

6.1 What is CDD

6.1.1 CDD refers to the process of identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

6.1.2 There are three levels of customer due diligence – CDD, enhanced CDD and simplified CDD, to be applied to different levels of ML/PF/TF risk.

6.2 When to Perform CDD

6.2.1 Developers are required to perform CDD in any of the following circumstances:

a. before granting to a purchaser an option to purchase a unit, or before accepting any sum of money (including any booking fee) from a purchaser in relation to the intended purchase, whichever is earlier;

b. when a purchaser intends to assign or has assigned to an assignee purchaser all the purchaser's rights, title and interest, under the Sale and Purchase Agreement (S&PA) made between the purchaser and the developer, and when the developer receives written notice from the assignee purchaser requiring the developer to enter into a new S&PA with the assignee purchaser;

c. when the developer has reasons to suspect that a purchaser is engaging in ML/PF/TF; and/or

d. when the developer has reason to doubt the veracity or adequacy of information obtained from earlier CDD measures about the same purchaser.

6.2.2 To fulfil the requirement for CDD at the point of sales (as described in 6.2.1(a) and (b) above), developers are allowed to engage and rely on a third party that is a regulated entity, so long as the engagement and reliance meet the requirements set out in Section 10 "Performance of Customer Due Diligence Measures by Third Parties". For the avoidance of doubt, developers remain responsible for the CDD/ECDD compliance and obligations.

6.3 How to Perform CDD

6.3.1 Developers must perform the following CDD measures in relation to every purchaser:

a. ascertain the identity of the purchaser and obtain the purchaser's identifying information. Please refer to the list of identifying information in Forms A1 to A3. Developers should take reasonable measures to obtain and verify information on the purchaser's current and previous nationalities as well as identities, particularly if the ML/PF/TF risk of the purchaser is determined to be higher.

b. where the purchaser is an entity or legal arrangement:

i. obtain the documents that constitute, regulate and bind the purchaser[6]; and

ii. ascertain the identity of every individual holding a senior management office in the purchaser and obtain the individual's identifying information;

c. understand and obtain information about the purchaser's purpose for purchasing a unit in a building project undertaken by that developer.

d. ascertain whether the purchaser is acting on behalf of any other person (called P), and if so:

i. obtain appropriate documentary evidence (such as an authorisation letter or power of attorney) to verify that the purchaser is authorised to act on behalf of P;

ii. if P is a natural person, perform the CDD measures in sub-paragraphs (a) and (c) in relation to P (as if the references to a purchaser in those sub-paragraphs are references to P; and

iii. if P is an entity or a legal arrangement, perform the CDD measures specified under paragraphs 6.3.1(a), (b) and (c) and 6.3.2 in relation to P (as if the references to a purchaser in those sub-paragraphs are references to P).

e. take reasonable measures, such as screening the relevant person(s) against public sources of information (e.g. UN website lists provided by relevant authorities or third-party commercial screening database), to determine whether the purchaser or a natural person on whose behalf the purchaser is acting, is a politically exposed person or a family member or close associate of a politically exposed person.

6.3.2 For every purchaser or every person that the purchaser is acting on behalf, that is an entity or a legal arrangement, developers must:

a. determine whether the entity or legal arrangement has any BO;

b. take reasonable measures to ascertain the identity and obtain the identifying information of each BO of the entity or legal arrangement, if any;

c. understand the nature of the business of the entity or legal arrangement; and

[6] In the case of a body corporate, the constitution, or the memorandum and articles of association, of the body corporate. In the case of a partnership or limited partnership, the partnership deed or agreement. In the case of an express trust, the trust deed of the trust. In the case of a society or an unincorporated association, the rules of the society or unincorporated association. In the case of any other entity or legal arrangement, the instrument or document that constitutes or establishes the entity or legal arrangement.

d. understand the ownership and control structure of the business of the entity or legal arrangement.

Please refer to the CDD checklist in Annexure 2 for details on how to perform the CDD for purchases by an entity or a legal arrangement.

6.3.3 Developers need not ascertain the identity and obtain the identifying information of each BO of an entity that is:

a. an entity listed on the Singapore Exchange and is subject to disclosure requirements by the Singapore Exchange;

b. a financial institution that is listed in Appendix 1 of the direction known as MAS Notice 626 issued by the Monetary Authority of Singapore; or

c. a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of ML, PF and TF, consistent with standards set by the FATF.

6.3.4 Developers must record the basis for determining that the purchaser is an entity specified in paragraphs 6.3.3(a), (b) and (c).

6.3.5 For a person purporting to act on behalf of the purchaser, developers must:

a. ascertain and obtain the identifying information of the person; and

b. ascertain whether the person is authorised to act on behalf of the purchaser, including by obtaining the appropriate evidence in writing of the authorisation and appointment of the person by the purchaser to act on the purchaser's behalf.

Developers may refer to the CDD checklist in Annexure 2 for details on how to perform the CDD.

6.3.6 Developers can also refer to an indicative list of suspicious real estate transactions to look out for during the transactions with purchasers at https://www.police.gov.sg/-/media/SPF/Advisories/STRO/Red-Flag-Indicators-for-Developers-Real-Estate-Agents-and-Salespersons.pdf. This list is not exhaustive, and developers should continue to exercise vigilance and keep abreast of new typologies as well as look out for other suspicious indicators.

6.4 Screening and Targeted Financial Sanctions Obligations

6.4.1 Developers should screen all the relevant persons and persons acting on behalf of the purchaser against the following lists and sources of information (herein referred to as "Sanctions Lists"):

a. First Schedule of the TSOFA at https://sso.agc.gov.sg/Act/TSFA2002;

b. Regulations under the United Nations Act 2001 ("UN Act") available on MAS' website at http://www.mas.gov.sg/regulations-and-financial-stability/anti-money-laundering-countering-the-financing-of-terrorism-and-targeted-financial-sanctions/targeted-financial-sanctions/lists-of-designated-individuals-and-entities.aspx.; and

c. List(s) provided by the Controller or other relevant authorities.

In addition, developers may screen the relevant persons and persons acting on behalf of the purchaser against public sources of information, such as websites or third-party screening database.

6.4.2 Developers should subscribe to MAS' website (by selecting "Anti-Money Laundering" under "Regulation Focus Areas") to receive updates on the latest designations by the United Nations Security Council, and other relevant updates to Singapore's frameworks to prevent proliferation financing or terrorism financing.

6.4.3 Before granting an Option to Purchase ("OTP") or entering into a Sale and Purchase Agreement ("S&PA") with a purchaser or assignee purchaser, developers must take reasonable measures, such as screening the relevant person(s) against the Sanctions Lists and sources of information specified in paragraphs 6.4.1, to assess whether any relevant person or any person acting on behalf of the purchaser is a terrorist or terrorist entity under the TSOFA, a designated person under any regulations made under the UN Act, or a person suspected of or at risk of facilitating ML, PF or TF as specified by the Controller or the relevant authorities in any written notice.

6.4.4 Where screening results in a positive hit against the Sanctions Lists, developers must:

a. not grant an OTP, accept any money (including booking fee) from or on behalf of the purchaser, or enter into a S&PA with the purchaser or assignee purchaser for a unit;

b. file a suspicious transaction report via the Suspicious Transaction Reporting Office Online Notices and Reporting platform (SONAR) at http://www.police.gov.sg/sonar; and

c. cease all dealings with the designated persons and entities and where applicable, freeze without prior delay and prior notice, the funds or assets, including any purchase price paid and not refund any part of it, pending further instructions from the Suspicious Transaction Reporting Office (STRO) and/or relevant law enforcement authorities.

6.4.5 Except for relevant person(s) or any person acting on behalf of the purchaser who are on the Sanctions Lists, for which developers are prohibited from transacting with,

developers may take a risk-based approach to decide whether to transact with a purchaser with higher ML, PF or TF risks, after performing the Enhanced Customer Due Diligence (ECDD) checks. Should there be any suspicion of illicit activities or funds, developers should file a Suspicious Transaction Report with the STRO.

6.5 Failure to Satisfactorily Perform or Complete CDD Measures

6.5.1 Developers may choose not to perform or not to complete the required CDD measures if they have reasons to:

a. suspect that the transaction with or intended with the purchaser involves ML/PF/TF; and/or

b. believe that performing the CDD measures will tip off the purchaser or any other person associated with the purchaser.

6.5.2 Developers are deemed to be unable to complete the CDD if:

a. they are unable to obtain, or to verify, information on the purchaser's identity required as part of those CDD measures; and/or

b. they do not receive a satisfactory response to any inquiry they make in relation to any other information required as part of those CDD measures, e.g. explanations provided is inconsistent or not reasonable.

6.5.3 In the situations highlighted under paragraphs 6.5.1 and 6.5.2, developers must:

a. not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from the purchaser, or enter into a S&PA for a unit with the purchaser or assignee purchaser;

b. determine whether to file a STR; and

c. record the basis of the determination under sub-paragraph (b).

6.5.4 Developers may refer to the summary flow chart on the basis to conduct CDD checks prior to property transactions, as well as the table with examples of scenarios and the required follow-up actions in Annexure 3 to guide them in completing their CDD / ECDD measures.

7 Enhanced Customer Due Diligence ("ECDD")

7.1 What is ECDD

7.1.1 ECDD refers to the process where a higher level of CDD is applied due to a higher ML/PF/TF risk of the customer or transaction. This is performed in addition to the CDD measures in Section 6.

7.2 When to Perform ECDD

7.2.1 Developers are required to perform ECDD in the following circumstances where the relevant person in any transaction is:

i. a foreign PEP, a family member or a close associate of a foreign PEP;

ii. a resident of or originates[7] from a relevant country;

iii. a person that the Controller or other relevant authorities have notified the developer to be a person who presents a higher risk of ML, PF or TF; or

iv. assessed to present a higher risk of ML, PF or TF under paragraph 4.2.4.

7.2.2 For the vast majority of purchasers, including domestic PEPs who are not assessed to be of higher risks, developers are only required to conduct checks as described in paragraph 6.3, instead of ECDD.

7.3 Requirements of ECDD

7.3.1 Where developers are required to perform ECDD, developers must perform the following measures in addition to the CDD requirements in Section 6:

a. obtain prior and special approval from a person holding a senior managerial or executive position in the developer before granting an Option to Purchase (OTP) to a purchaser, or before accepting any sum of money (including any booking fee) from a purchaser, or before entering into the S&PA with the purchaser or assignee purchaser;

b. take reasonable measures to establish the income level, source of wealth (SoW) and source of funds (SoF)[8] of the relevant person;

c. ascertain the identity of the person P on whose behalf the purchaser is acting and obtain P's identifying information, where the developer suspects that the purchaser is trying to conceal the identity of the person P;

[7] Refers to the relevant person's current citizenship.

[8] "Source of Wealth" (SoW) generally refers to the origin of the customer's and BO's entire body of wealth (i.e. total assets). "Source of Funds" (SoF) refers to the origin of the particular funds or other assets which are the subject of the transactions.

d. conduct enhanced ongoing monitoring of the transactions entered into with the purchaser. This is to identify suspicious transactions, including transactions or patterns of transactions which are inconsistent with the purchaser's profile. Where information has been previously provided and remains unchanged, developers are not required to request for the same information again; and

e. take reasonable measures as are appropriate to the risks of ML, PF or TF in relation to the relevant person.

7.3.2 Where a developer is unable to perform or complete any required ECDD measures or has reason to believe that performing such measures risks tipping off the purchaser, the developer should adhere to the requirements and restrictions set out in paragraphs 6.5.1 to 6.5.3.

7.3.3 To conduct the required ECDD checks before issuing OTP or accepting any sum of money, developers are allowed to engage and rely on a third party that is a regulated entity, so long as the engagement and reliance meet the requirements set out in Section 10 "Performance of Customer Due Diligence Measures by Third Parties". For the avoidance of doubt, developers remain responsible for the CDD/ECDD compliance and obligations.

7.4 How to Perform ECDD

7.4.1 Developers must implement appropriate policies, controls and procedures to determine whether the circumstances mentioned in paragraph 7.2 exist. For example, developers could consider increasing the frequency of their checks.

7.4.2 Developers can adopt the following checks, depending on their risk assessment:

a. use the internet and media as sources for determining, verifying and monitoring information;

b. access commercial screening databases to help identify the relevant person and to check against adverse news reports; and

c. refer to the FATF guidance paper on dealing with PEPs.

7.4.3 To establish the SoW and SoF, developers should document and make a reasonable assessment of the purchaser's representations by doing the following, in addition to obtaining the information from the purchaser's declarations:

a. corroborate the information on SoW and SoF against documentary evidence or public information sources such as commercial databases, audited accounts, salary details, bank statements. Where independent documents or sources are not readily available, developers should assess whether residual risk of

uncorroborated wealth is acceptable or additional risk mitigation measures would be necessary; and

b. exercise reasonable judgment in determining which documents and information are critical for SoW corroboration, focusing on more material or higher risk SoW (such as SoW from higher risk countries or higher risk industries). Documents from many years ago may no longer be easily available and may not be of high relevance to the purchaser's SoW. Additional triangulation checks against multiple sources may be conducted where required, based on the developer's risk assessment of the purchaser.

7.4.4 Developers should take appropriate and reasonable means to independently corroborate information obtained from the purchasers against documentary evidence or public information sources. Developers should ensure that their SoW and SoF checks are risk-proportionate and take into account the unique circumstances and profile of each purchaser. Developers are advised not to adopt a one-size-fits-all approach and to instead consider the following risk principles of relevance, materiality and prudence:

a. obtain relevant and pertinent information (e.g. income tax statement, audited accounts) without the need to obtain unnecessary information such as long-dated financial or employment records;

b. avoid excessive measures and requesting for irrelevant information to establish purchasers' SoW/SoF that are disproportionate to the requirements and international standards. For example, if SoW originates from low-risk countries or is backed by reliable sources of information such as audited accounts of companies, bank statements, salary slips from established companies, it would be deemed less risky compared to if it originates from higher risk countries/ shell companies or comprises gifts from unrelated parties;

c. where information obtained is already from reliable and public information sources, there is no need for triangulation checks against different information sources;

d. there is no need to attempt to corroborate every single piece of SoW information gathered. It may not be possible or practicable to corroborate some SoW from many years ago for which the information may no longer be easily available. In such cases, developers should focus on corroborating the more material and higher risk SoW and assess whether the residual risk of the uncorroborated wealth is acceptable and whether additional risk mitigating measures are needed in absence of the corroboration; and/or

e. for transactions involving a single property purchase at price points reflecting market norms, less checks would be expected. This is in line with the risk-proportionate approach.

7.4.5 The following are examples of information that developers can use to corroborate individuals' SoW/SoF:

a. salaries and savings: Salary slips, tax returns, bank statements showing credited salary;

b. gift/inheritance/windfall: Bank statements/documents showing the payouts/transfers, will (for inheritance). Developers should establish the relationship between the asset contributor and the purchaser by reasonable means – such as obtaining birth certificate (if available) or address proof.

Developers should also pay attention on the legitimacy and reasonableness of the gift, especially if it is from unrelated parties. This could be done through obtaining independent information to verify a gifting transaction, and assessing the plausibility of the asset contributor's financial ability to provide as well as reasons for providing the gift;

c. business profits over the years: Audited financial statements showing the profits and dividend payments and the individual's ownership of the company. Information from company registers (e.g. ACRA's database) to corroborate the individual's ownership in the company, or changes in ownership. Unaudited management accounts should only be considered as an alternative. If used, developers should conduct additional triangulation checks against independent sources to assess their reliability; and/or

d. investment gains over the years: Independent documents evidencing the ownership of the shares, sale of shares, and dividend income.

8 Simplified Customer Due Diligence ("SCDD")

8.1 When to Perform SCDD

8.1.1 Developers may, instead of performing the standard CDD measures in Section 6, perform SCDD measures if it is deemed that SCDD measures are adequate to effectively ascertain the identity of the purchaser or beneficial owner of the purchaser, or any person who is acting on behalf of the purchaser, in any particular transaction.

8.2 Requirements of SCDD

8.2.1 SCDD measures can only be performed if all the following conditions are met:

a. developers have assessed the risk of ML, PF and TF in relation to the purchaser to be low;

b. the SCDD measures are commensurate with the level of the risk of the purchaser engaging in ML, PF and TF, as identified by the developers; and

c. none of the circumstances mentioned in Section 7 requiring ECDD measures exists.

8.3 How to Perform SCDD

8.3.1 Developers must record the details of the risk assessment that forms the basis for the decision and the SCDD measures carried out.

9 Customer Due Diligence (CDD) on Existing Purchasers

9.1 For existing purchasers with whom developers have entered into a transaction before the implementation of the prevention of ML/PF/TF requirements, developers must perform CDD, ECDD or SCDD measures in relation to any existing purchaser, taking into account:

a. when CDD, ECDD or SCDD measures (if any) were last applied to that purchaser; and

b. the adequacy of information already obtained by the developer in relation to that purchaser.

9.2 Developers may use information previously obtained from CDD, ECDD or SCDD measures performed in relation to the same purchaser unless developers have doubts about the veracity or adequacy of the information, or whether the information is up-to-date. For existing purchasers, developers should conduct CDD, ECDD or SCDD before issuing the notice of payment for temporary occupation permit (TOP) or completion of sale, whichever is applicable.

9.3 If the existing purchasers originated from[9] or are residents of high-risk countries or jurisdictions subject to a call for action by FATF ("FATF black list"), developers should perform enhanced ongoing monitoring of the transaction which could include more frequent checks on the source of wealth and funds, payment patterns etc.

10 Performance of CDD Measures by Third Parties

10.1 Developers may rely on a third party to perform the CDD measures which developers are required to perform, if the following requirements are met:

a. developers are satisfied that the third party it intends to rely on:

[9] Refers to the relevant person's current citizenship.

i. is subject to and supervised for compliance with requirements for the prevention of ML, PF and TF consistent with standards set by the FATF;

ii. has adequate measures in place to comply with the FATF requirements; and

iii. is willing and able to provide, without delay, on the developer's request, any document acquired by the third party as a result of the CDD, ECDD or SCDD measures performed for the developer.

b. the third party is not precluded from acting as such by the Controller; and

c. developers take appropriate steps to identify, assess and understand the risks of ML, PF and TF in the foreign countries that the third party also conducts its business in, if applicable.

10.2 Where a developer decides to rely on a third party to carry out CDD, ECDD or SCDD measures which will be based on the third party's own prevention of ML/PF/TF rules and processes, the developer must:

a. document the basis for the developer's opinion in paragraph 10.1a;

b. obtain from the third party without delay all documents acquired as a result of the CDD, ECDD or SCDD measures performed by the third party; and

c. be ultimately responsible for compliance with the obligations to perform CDD, ECDD or SCDD measures and keep records as required under the Acts and Rules.

10.3 Developers are not allowed to rely on a third party to conduct ongoing monitoring (see Section 11), as the CDD measures are conducted based on the third party's own prevention of ML/PF/TF rules and processes and developers would not be able to have adequate control, timely information and ability to mitigate the risks arising from unusual/suspicious transactions during the ongoing monitoring process.

11 Ongoing Monitoring of Transactions

11.1 Developers must, before issuing the notice of payment for TOP and for completion of sale, review the adequacy of the information and documents obtained as a result of the CDD, ECDD or SCDD measures. This is to ascertain whether the transactions carried out by the purchasers are consistent with the developers' knowledge of the purchaser, the purchaser's income and risk profile and the purchaser's source(s) of funds, particularly in cases where there is a higher risk of ML, PF or TF.

11.2 Subject to 11.1, if the completion of sale occurs within 1 year from the last review of information and documents conducted prior to the issuance of the notice of payment

for TOP, ongoing monitoring of transactions need not be repeated, provided there are no changes to the developer's knowledge or risk profile of the purchaser.

12 Reporting of Suspicious Transactions

12.1 Submitting a Suspicious Transaction Report

12.1.1 If there are suspicions that ML/PF/TF activities are committed, developers are required to file a Suspicious Transaction Report with the STRO of the Singapore Police Force as soon as is reasonably practicable after it comes to the developers' attention. at http://www.police.gov.sg/sonar.

12.1.2 The filing of an STR should be done as soon as possible, which should be within 5 business days after suspicion was first established[10], and within 15 business days of the case being referred by the developer's staff to the management, unless the circumstances are exceptional or extraordinary. In cases where the relevant person or person acting on behalf of the purchaser is listed in the Sanctions Lists, developers should file the STRs immediately, no later than 1 business day after suspicion was first established[10].

12.1.3 The STR must be filed electronically via SONAR. Developers may refer to the instructions on the SONAR website at https://www.police.gov.sg/sonar on how to file a STR.

13 Record Keeping

13.1 Developers are required to keep the following documents and information (including any analysis performed) relating to a person whom CDD, ECDD or SCDD measures have been performed, for 5 years after the expiry or cancellation of the OTP, or the termination or annulment of the S&PA, or the legal completion of the sale and purchase of the property, whichever is applicable:

a. OTP;
b. S&PA;
c. Form 3;
d. Prescribed form to notify purchasers of the information/documents required for CDD checks; and
e. Records of CDD, ECDD or SCDD conducted.

14 Identifying Risks from New Technologies

14.1 Developers must identify and assess the ML/PF/TF risks that may arise in relation to:

[10] This refers to the instance after the developer had considered the information and circumstances available and concluded that the filing of an STR was necessary.

a. the development of any new service or new business practice (including any new delivery mechanism for any new or existing service); and

b. the use of any new or developing technology for any new or existing service.

15 Managing and Mitigating Risks from New Technologies

15.1 Before offering any new service, starting any new business practice, using any new or developing technology, developers must assess the ML/PF/TF risks that may arise in relation to the offering of that service, the starting of that business practice or the use of that technology. Subsequently, developers must take appropriate measures to manage and mitigate such risks.

ANNEXURE 1

RISK ANALYSIS TEMPLATE

This template serves to guide developers to perform risk analysis to identify, assess and understand their money laundering, proliferation financing and terrorism financing 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, proliferation financing 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 e.g. directors, CEO. As part of the oversight and governance on prevention of ML/PF/TF, 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 any project launch

S/N	Risk factor to consider	Indicate whether risk factor is met, i.e. Yes or No. If yes, provide details.
(I) Countries and jurisdictions in which the developers have operations in *(Note: If Risk Factor 1 is met, developer should rate itself as "high-risk".)*		
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		
3	Sole/heavy reliance on online platforms for marketing, without physical face-to-face interactions with purchasers	
(III) Profile of developers' higher-risk purchasers *(Note: The following risk factors should be considered after project is launched and units sold.)*		

4	⩾20% of purchaser are non-Singapore Citizens (e.g. PRs, foreigners, entities and legal arrangements)	
5	Purchasers buying ⩾2 properties within 1 year	
6	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	
7	Purchasers originating from or are residents of: a) high-risk countries or jurisdictions subject to a call for action ("FATF black list"); or 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, PEP purchasers		
8	*(Developers to list down relevant risk factors)*	
V) Overall risk rating		
9	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 be commensurate with the risk level and size of the developer's business.

Risk mitigating measures *(Note: these are examples that developers may consider)*	
Implement a system of performing CDD and ECDD checks	
Training of staff	*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 assessed to be high, the developer should consider more rigorous training and increase the frequency.*

Review of risk analysis	*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.*
Independent auditor to audit CDD and ECDD process, in addition to audit checks on IPPC	*Where risk level is assessed to be high, developers should consider increasing the frequency of audit*
Review of transactions	*Where risk level is assessed to be high, developers should consider conducting more frequent review of transactions*

Section D: Developer's acknowledgement of risk analysis report

Project Details:	
Name of project	
Name of licensed developer	
Housing Developer Licence No.	
Completed by:	
Name	
Designation	
Date	
Approved by:	
Name	
Designation *(Note: The Risk Analysis must be approved by the Senior Management e.g. director or CEO)*	
Date	
Date of next review:	
Target date of developer's next risk analysis *(Note: 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.)*	

ANNEXURE 2

CHECKLIST FOR CONDUCTING CUSTOMER DUE DILIGENCE (CDD)

IMPORTANT POINTS TO NOTE:

1. This checklist guides developers in the conduct of customer due diligence (CDD) to comply with the Housing Developers (Prevention of Money Laundering, Proliferation Financing & Terrorism Financing) Rules and Sale of Commercial Properties (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Rules ("the Rules"). Developers are advised to read this checklist in conjunction with the Rules.

2. Developers are required to perform CDD in any of the following circumstances:

   a. before granting to a purchaser an option to purchase a unit, or before accepting any sum of money (including any booking fee) from a purchaser in relation to the intended purchase, whichever is earlier;

   b. when a purchaser intends to assign or has assigned to an assignee purchaser all the purchaser's rights, title and interest, under the Sale and Purchase Agreement (S&PA) made between the purchaser and the developer, and the developer receives written notice from the assignee purchaser requiring the developer to enter into a new S&PA with the assignee purchaser;

   c. when the developer has reason to suspect that a purchaser is engaging in money laundering (ML), proliferation financing (PF) or terrorism financing (TF);

   d. when the developer has reason to doubt the veracity or adequacy of information obtained from earlier CDD measures about the same purchaser.

3. Developers must complete the checklist and the relevant forms for each property transaction. Developers may use their own checklist to conduct the CDD but have to ensure that the requirements under the Rules are complied with.

DETAILED STEPS AND ACTIVITIES	**Tick (√) accordingly**	**Remarks**
1. **Obtain Purchaser's Particulars & Verify his/her Identity**		
a. Before granting an Option to Purchase (OTP) or before accepting any sum of money (including booking fee) from an intending purchaser or when written notice is received from an assignee purchaser to enter into a new S&PA with the assignee purchaser for sub-sales, have you:	☐ Yes ☐ No	

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
i. notified the intending purchaser on the documents and information that the developer must obtain to perform the CDD measures and obtained the intending purchaser's or assignee purchaser's written acknowledgement on the receipt of the notice. Refer to https://go.gov.sg/ura-amltf for the documents and information. ii. asked the intending purchaser or assignee purchaser to fill in the **Purchaser's Particulars Form (Form A1 for individuals, Form A2 for entities and Form A3 for legal arrangements)**? iii. verified the identity of the intending purchaser or assignee purchaser? *[Pointer:* Developers should verify purchaser's identity by requesting to see and record details of documents such as his NRIC or passport. If the purchaser is unable to produce an original document, developers 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.*]*		
b. If a person purports to act on behalf of the purchaser, have you: i. asked the person to fill in their particulars in **Form B on "Details of Person(s) Acting on Behalf of Purchaser"?** ii. verified the identity of this person and requested for supporting documents such as letter of authorisation, power of attorney? If the supporting documents are not provided, do not deal with the person and assess if a Suspicious Transaction Report (STR) should be filed at https://www.police.gov.sg/sonar.	☐ Yes ☐ No ☐ Not applicable	
c. If the purchaser is acting on behalf of any other person (known as P), have you:	☐ Yes ☐ No	

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
i. asked the purchaser to fill in **Form D** "**Details of natural person/entity/legal arrangement on whose behalf the purchaser is acting"**; ii. obtain appropriate documentary evidence (such as an authorisation letter or power of attorney) to verify that the purchaser is authorised to act on behalf of P. If the supporting documents are not provided, do not deal with the person and assess if a Suspicious Transaction Report (STR) should be filed at https://www.police.gov.sg/sonar	☐ Not applicable	
c. Is the purchaser: i. an entity listed on the Singapore Exchange and subject to disclosure requirements by the Singapore Exchange; or ii. a financial institution that is listed in Appendix 1 of the direction known as MAS Notice 626 issued by the Monetary Authority of Singapore; or iii. a financial institution incorporated or established outside Singapore that is subject to and supervised for compliance with requirements for the prevention of money laundering, proliferation financing and terrorism financing, consistent with the standards set by the Financial Action Task Force (FATF)? If yes, you must record the basis for determining that the purchaser falls into one of the categories in (i), (ii) & (iii) above. You are not required to proceed with other Sections of this checklist. You may proceed to sign off this checklist and keep all relevant records of the purchaser. If no, please continue with this checklist.	☐ Yes ☐ No ☐ Not applicable	
2. **CONDUCT OF CUSTOMER DUE DILIGENCE (CDD) MEASURES** *[Note: In situations where developer have reason to suspect that the transaction relates to ML, PF or TF and believes that performing this measure will tip off the purchaser or any other person, developers may choose not to perform or complete performing this measure. In such*		

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
situations, developers must not grant the OTP to the purchaser or accept any sum of money (including booking fee) in relation to the purchase or enter into a S&PA with the purchaser or assignee purchaser. The developer must determine whether to file a STR and record the basis of the determination for filing the STR.]		
2.1. <u>Identification and verification of Beneficial Owner (BO)*[Pointer: In relation to an entity or a legal arrangement, a BO refers to an individual who ultimately owns or controls the entity or legal arrangement, or who exercises ultimate effective control over the entity or legal arrangement, or on whose behalf the transaction is being conducted. Ultimate effective control depends on the ownership structure of the entity or legal arrangement, and may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).]*		
a. For a purchaser that is an entity or legal arrangement, have you: i. determined whether the purchaser has any BO; and ii. ascertained the identity and obtained the identifying information of each BO of the purchaser (Refer to **Form C "Details of BO"**); and iii. understood the nature of the purchaser's business, the ownership and control structure of the purchaser, by obtaining the necessary information? *[Pointers: The identification of the BO for a purchaser who is an <u>entity</u> would include:* *(i) identify each individual (if any) who ultimately has a controlling ownership interest in the purchaser,* according to the law and instrument under which the purchaser is constituted*;* *(ii) if it is doubtful whether all or any of the individuals who ultimately have a controlling interest in the purchaser are its BOs, or where no individual exerts control through ownership interests, to ascertain the identity and obtain the identifying information of each individual (if any) exercising control of the purchaser through other means; and* *(iii) where no individual is identified through (i) and (ii), to ascertain the identity and obtain the identifying information of every individual holding a senior*	☐ Yes ☐ No ☐ Not applicable	

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
management office in the purchaser (e.g. the Director in a company). *The identification of the BO for a purchaser who is a <u>legal arrangement</u> would include:* *(i) for trusts – ascertain the identity and obtain the identifying information of the settlor, each trustee(s), the protector (if any), each beneficiary, and any other individual exercising ultimate effective control over the trust;* *(ii) for a legal arrangement which is not a trust – ascertain the identity and obtain the identifying information of each person holding a position equivalent or similar to the settlor, trustee, protector, beneficiary or other individual exercising ultimate effective control over the trust.* *To understand the nature of the business and the ownership and control structure of the purchaser, you may rely on any of the following information but not limited to:* *(i) information provided by the purchaser (e.g. organisation chart);* *(ii) information available from the purchaser's website or published annual reports;* *(iii) information available on the purchaser from public sources (e.g. annual returns and filing with the Accounting and Corporate Regulatory Authority (ACRA), ACRA's business profile);* *(iv) information obtained from other reliable sources (e.g. research reports, third party service providers) or other research.]*		
2.2. <u>Politically Exposed Person (PEP)</u> a. Have you checked if any of the relevant person is a PEP, a family member of a PEP or a close associate of a PEP: *"relevant person" means a purchaser, a beneficial owner of a purchaser, a person (P) on whose behalf a purchaser is acting or a beneficial owner of P.* *"politically exposed person" means a domestic politically exposed person, a foreign politically exposed*	☐ Yes ☐ No ☐ Not applicable	

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
person or an international organisation politically exposed person. *"domestic politically exposed person" means an individual who is or has been entrusted with any prominent public function in Singapore";* *"foreign politically exposed person" means an individual who is or has been entrusted with a prominent public function in a foreign country;* *"international organisation politically exposed person" means an individual who is or has been a member of the senior management of an international organisation (including a director, deputy director or member of a board of the international organisation, or an equivalent appointment in the international organisation);* *"prominent public function" includes the role held by —* *(a) a head of state;* *(b) a head of government;* *(c) a government minister;* *(d) a senior politician;* *(e) a senior civil or public servant;* *(f) a senior government, judicial or military official;* *(g) a senior executive of a state-owned corporation;* *(h) a senior political party official; or* *(i) a member of the legislature;*		
b. If any of the relevant person is a PEP, or a family member or a close associate of a PEP, have you asked the relevant person to fill in **Form E on "Details of PEP"**?	☐ Yes ☐ No ☐ Not applicable	
2.3. <u>Screening for ML, PF and TF risks</u> a. Have you screened all the relevant persons and persons acting on behalf of the purchaser for ML, PF and TF risks, and completed **Form F on "Screening of Purchasers for Money Laundering, Proliferation Financing and Terrorism Financing Risks"**?	☐ Yes ☐ No	

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
b. In the screening of all the relevant persons and persons acting on behalf of the purchaser, are any of the parties: i. a terrorist or terrorist entity under the Terrorism (Suppression of Financing) Act 2002; or ii. a designated person as defined in any regulations made under the United Nations Act 2001; or iii. a person suspected of, or at risk of, facilitating ML, PF or TF who is specified by the Controller in any written notice issued by the Controller? Note: If yes, the developer must not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from or on behalf of the purchaser, or enter into a S&PA with the purchaser or assignee purchaser, and **file a STR.** You are not required to proceed with the other Sections in this checklist.	☐ Yes ☐ No	
c. In the screening of all the relevant person and persons acting on behalf of the purchaser, do you suspect that any of the parties is involved in ML, PF or TF? **Note: File a STR if there are suspicions of ML, PF or TF and seek approval from a person holding senior managerial or executive position in the developer to proceed with the transaction.**	☐ Yes ☐ No	
2.4. Enhanced Customer Due Diligence Measures a. Where the any of the relevant person is: i. a foreign PEP, a family member or a close associate of a foreign PEP; ii. a resident of or originates from a relevant country which is a foreign country subject to a call made by the FATF for countermeasures		

DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
or enhanced customer due diligence measures. Please visit: https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html for the list of countries; iii. a person that the Controller or other relevant authorities have notified the developer to be of a higher ML/PF/TF risk; or iv. a person (including a domestic or international organisation PEP, a family member or a close associate of a domestic or international organisation PEP), who presents a higher ML/PF/TF risk, as assessed by the developer in Form F. have you conducted enhanced CDD measures by: I. seeking approval from the senior managerial or executive position in the developer to continue with the transaction; II. asking for additional information, e.g. income level, source of funds and source of wealth of the relevant person, and corroborating the information; III. ascertaining the identity of a person P on whose behalf the purchaser is acting and obtaining P's identifying information, where the developer suspects that the purchaser is trying to conceal the identity of P; IV. conducting enhanced ongoing monitoring of the transactions entered into with the purchaser to identify suspicious transactions, including transactions that are inconsistent with the purchaser's profile; and V. taking all reasonable measures as are appropriate to the risks of ML, PF or TF in relation to the relevant person.	☐ Yes ☐ No ☐ Not applicable ☐ Yes	

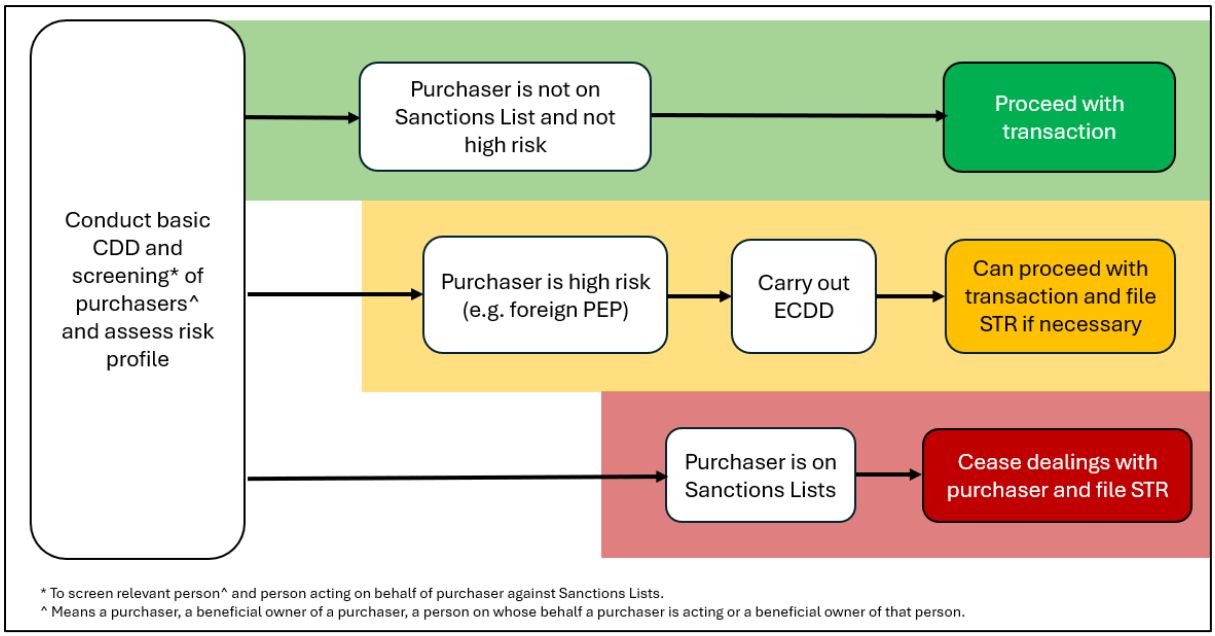
DETAILED STEPS AND ACTIVITIES	Tick (√) accordingly	Remarks
b. Have you implemented appropriate policies, controls and procedures to determine if any of the circumstances mentioned in Qn 2.4a exist?	☐ No ☐ Not applicable	

Name and designation of developer's representative who completed the checklist: _____ Signature: _____ Date: _____	
The following section is applicable only if the checklist is completed by a Third Party	
Name of person who completed the checklist	
Signature	
Occupation of Third party	☐ Salesperson ☐ Legal professional ☐ Others (please specify) _____
Company's name	

ANNEXURE 3

Refer to the following flow chart, common scenarios and corresponding actions table to guide the performance of customer due diligence checks (CDD).

Flow chart for CDD/ECDD checks prior to property transaction



CDD/ ECDD scenarios and corresponding actions

Examples of Scenarios	Actions taken	Follow-up action
(1a) Purchaser is a Singaporean couple who are HDB upgraders. (1b) Purchaser is a domestic PEP.	Obtain verifying information and screen the purchasers to confirm there are no matches with Sanctions List and adverse news.	If no matches with Sanctions Lists and adverse news, developer may proceed with transaction. If there are matches with Sanctions Lists, developer should cease dealings and file STR. If there are adverse news, developer should conduct a risk assessment on whether they should proceed.
(2a) Purchaser is a national from a relevant country, who is higher risk.	• Obtain verifying information and screen the purchaser to confirm no matches with Sanctions Lists and adverse news.	If no matches with Sanctions Lists and adverse news, developer may proceed with transaction. If there are matches with Sanctions Lists, developer

(2b) Purchaser is a foreign PEP.	• Carry out ECDD, including checks on SoW/SoF (e.g. obtaining income records and proof of employment). • SoW/SoF checks should be risk-proportionate, as guided under 7.3.3 of the Guidelines.	should cease dealings and file STR. If there are adverse news, developer should conduct a risk assessment on whether they should proceed. File STR if there is suspicion of illicit activity.
(3) Purchaser's name matches an individual in the Sanctions Lists.	Obtain verifying information and screen the purchaser to confirm if it is a true match (e.g. name and ID match).	If there are matches with Sanctions Lists, developer should cease dealings and file STR

FORM A1

PURCHASER'S PARTICULARS FORM FOR <u>NATURAL PERSONS</u>

Note: All the information listed in this form must be obtained for all purchasers named in the Option to Purchase or Sale and Purchase Agreement (use additional forms if necessary). The information declared must be true and correct. Documents to verify the information will be requested.

(A) PURCHASER'S PARTICULARS		
1. Full name of purchaser, including any alias used		
2. Identification number		
3. Type of identification (document must be issued by a government)	☐ NRIC ☐ Passport ☐ Others (Please specify) _____	
4. Expiry date of identification document, if applicable		
5. Date of birth		
6. Place of birth		
7. Address of usual place of residence		
8. Nationality	Current Nationality: _____ Previous Nationality (if applicable): _____	
9. Occupation		
10. Contact number(s)		
11. Purpose of purchase	☐ Owner-Occupation ☐ Investment/Rental ☐ Others (Please specify) _____	
12. Are you acting on behalf of another person?	☐ Yes Please complete **Form D "Details of natural person/entity/legal arrangement on whose behalf the purchaser is acting"**	☐ No
13. Are you a current or former Politically Exposed Person (PEP)?	☐ Yes	☐ No

("PEP" means an individual who is or has been entrusted with a prominent public function in Singapore, a foreign country or an international organisation; *"prominent public function" includes the role held by:* *(a) a head of state;* *(b) a head of government;* *(c) a government minister;* *(d) a senior politician;* *(e) a senior civil or public servant;* *(f) a senior government, judicial or military official;* *(g) a senior executive of a state-owned corporation;* *(h) a senior political party official;* *(i) a member of the legislature; or* *(j) a member of the senior management of an international organisation (including a director, deputy director or member of a board of the international organisation, or an equivalent appointment in the international organisation)*		
14. Are you a family member of a current or former PEP? *"family member" means a spouse, a child, an adopted child or a stepchild, a sibling, an adopted sibling or a stepsibling or a parent or step-parent, of the PEP.*	☐ Yes	☐ No
15. Are you a close associate of a current or former PEP? *"close associate", means —* *(a) a partner of the PEP;* *(b) a person accustomed or under an obligation, whether formal or informal, to act in accordance with the directions, instructions or wishes of the PEP;* (c) *a person whose directions, instructions or wishes the PEP is*	☐ Yes	☐ No

accustomed or under an obligation, whether formal or informal, to act in accordance with; or (d) *a person with whom the PEP has an agreement or arrangement, whether oral or in writing and whether express or implied, to act together.*		
16. If any of the responses to Qn 13 to 15 is "Yes", please complete **Form E "Details of PEP"**		
(B) PURCHASER'S ACKNOWLEDGEMENT		
Name of purchaser:		
Signature:		
Date:		

FORM A2

PURCHASER'S PARTICULARS FORM FOR <u>ENTITIES</u>
(e.g. company, limited liability partnership, society)

Note: All the information listed in this form must be obtained for all purchasers named in the Option to Purchase or Sale and Purchase Agreement (use additional forms if necessary). The information declared must be true and correct. Documents to verify the information will be requested.

(A) PARTICULARS OF ENTITY	
1. Full name of entity	
2. Identification or registration number	
3. Type of identification (e.g. Business Profile from the Accounting and Corporate Regulatory Authority, any other document issued by any government certifying the incorporation, registration or existence)	
4. Expiry date of identification document (if applicable)	
5. Place of incorporation/ registration	
6. Address of registered office (to indicate as "shared" if it is a shared address)	
7. Address of principal place of business (to be completed if the registered office is not the principal place of business)	
8. Nature of business (e.g. principal activities as stated in ACRA's Business Profile)	
9. Ownership and control structure of entity *[Pointer: Information that may be provided:* *(i) memorandum and articles of association;* (ii) *information available on the entity's website or published annual reports;* (iii) *information available on the entity from public sources (e.g. annual returns and filing with the Accounting and Corporate Regulatory Authority (ACRA), ACRA's business profile)]*	*[To describe]*

10. Details of all individuals holding a senior management position (e.g. senior managing directors in a company)	<u>Individual 1</u> • Name, including any alias: • Date of birth: • Place of birth: • Identification no.: • Identification document: • Nationality: • Address of place of residence: • Contact no.: • Position held: <u>Individual 2</u> • Name, including any alias: • Date of birth: • Place of birth: • Identification no.: • Identification document: • Nationality: • Address of place of residence: • Contact no.: • Position held:
11. Contact number(s)	
12. Purpose of purchase	☐ Owner-Occupation ☐ Investment/Rental ☐ Others (Please specify) _____
(B) PARTICULARS OF BENEFICIAL OWNER(S) (BO)	
13. Does the entity have any BO? *BO refers to an individual:* *a) who ultimately owns or controls the entity or legal arrangement;* *b) who exercises ultimate effective control over the entity or legal arrangement; or* *c) on whose behalf the entity or legal arrangement conducts any transaction with a developer.* *Ultimate effective control depends on the ownership structure of the entity or legal arrangement. It may be based on a threshold, e.g. any person owning more than*	☐ Yes ☐ No If "yes", please complete **Form C "Details of BO".**

a certain percentage of the company (e.g. 25% based on FATF recommendations).	
(C) PURCHASER'S ACKNOWLEDGEMENT	
Name of person acting on behalf of the entity	
Position in the entity	
Signature	
Date	

FORM A3

PURCHASER'S PARTICULARS FORM FOR <u>LEGAL ARRANGEMENTS</u>
(e.g. trust)

Note: All the information listed in this form must be obtained for all purchasers named in the Option to Purchase or Sale and Purchase Agreement (use additional forms if necessary). The information declared must be true and correct. Documents to verify the information will be requested.

(A) PARTICULARS OF LEGAL ARRANGEMENT	
1. Full name of legal arrangement	
2. Type of legal arrangement	☐ Trust ☐ Others (Please specify) _____
3. Country in which the legal arrangement is constituted	
4. Nature of business	
5. Proof of the legal arrangement's existence	
6. Instrument under which the legal arrangement is constituted e.g. deed of trust	
APPLICABLE WHERE THE LEGAL ARRANGEMENT IS A TRUST	
7. Full name of **<u>settlor</u>**	
8. Identification number	
9. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
10. Expiry date of identification document (if applicable)	
11. Date of birth	
12. Place of birth	
13. Address of usual place of residence	
14. Nationality	
15. Occupation	
16. Contact number(s)	
17. Full name of **<u>trustee(s)</u>**	
18. Identification number	

19. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
20. Expiry date of identification document, if applicable	
21. Date of birth	
22. Place of birth	
23. Address of usual place of residence	
24. Nationality	
25. Occupation	
26. Contact number(s)	
27. Full name of **protector**	
28. Identification number	
29. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
30. Expiry date of identification document (if applicable)	
31. Date of birth	
32. Place of birth	
33. Address of usual place of residence	
34. Nationality	
35. Occupation	
36. Contact number(s)	
37. Full name/class of **beneficiary(ies)**	
38. Identification number	
39. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
40. Expiry date of identification document (if applicable)	
41. Date of birth	
42. Place of birth	
43. Address of usual place of residence	
44. Nationality	
45. Occupation	
46. Contact number(s)	

47. Full name of any other person(s) **exercising ultimate ownership/control over the trust**	
48. Identification number	
49. Type of identification document	☐ NRIC ☐ Passport ☐ Others: (Please specify) _____
50. Expiry date of identification document (if applicable)	
51. Date of birth	
52. Place of birth	
53. Address of usual place of residence	
54. Nationality	
55. Occupation	
56. Contact number(s)	
APPLICABLE WHERE THE LEGAL ARRANGEMENT IS NOT A TRUST	
57. Full name of person holding a position equivalent or similar to a settlor, trustee, protector, beneficiary and any other person exercising ultimate effective control over the trust	
58. Identification number	
59. Type of identification document	☐ NRIC ☐ Passport ☐ Others: (Please specify) _____
60. Expiry date of identification document (if applicable)	
61. Date of birth	
62. Place of birth	
63. Address of usual place of residence	
64. Nationality	
65. Occupation	
66. Contact number(s)	
(B) PARTICULARS OF BENEFICIAL OWNER(S) (BO)	
67. Does the legal arrangement have any BO? *BO refers to an individual:* *a) who ultimately owns or controls the entity or legal arrangement;*	☐ Yes ☐ No If yes, please complete **Form C "Details of BO".**

b) who exercises ultimate effective control over the entity or legal arrangement; or *c) on whose behalf the entity or legal arrangement conducts any transaction with a developer.* *Ultimate effective control depends on the ownership structure of the entity or legal arrangement. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).*	
(C) PURCHASER'S ACKNOWLEDGEMENT	
Name of person acting on behalf of the legal arrangement	
Position in legal arrangement	
Signature	
Date	

FORM B

DETAILS OF PERSON(S) ACTING ON BEHALF OF PURCHASER
(*Use additional forms, if necessary]*

(A) PARTICULARS OF NATURAL PERSON WHO IS ACTING ON BEHALF OF PURCHASER	
1. Full name, including any alias used	
2. Identification number	
3. Type of identification (document must be issued by a government)	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
4. Expiry date of identification document (if applicable)	
5. Date of birth	
6. Place of birth	
7. Address of usual place of residence	
8. Nationality	
9. Occupation	
10. Contact number (s)	
11. Authorisation document, showing that purchaser has authorised the individual to act on the purchaser's behalf (e.g. authorisation letter or Power of Attorney)	

(B) PARTICULARS OF ENTITY WHO IS ACTING ON BEHALF OF PURCHASER	
1. Full Name, including any alias used	
2. Identification or registration number	
3. Type of identification [e.g. Business Profile from the Accounting and Corporate Regulatory Authority (ACRA)]	
4. Expiry date of identification document (if applicable)	
5. Place of incorporation/ registration	
6. Address of registered office (to indicate as "shared" if it is a shared address)	
7. Address of principal place of business (to be completed if the registered office is not the principal place of business)	
8. Nature of business (e.g. principal activities as stated in ACRA's Business Profile)	
9. Ownership and control structure of entity *[pointer: Information that may be provided:* (i) memorandum and articles of association; (ii) *information available on the entity's website or published annual reports;* (iii) *information available on the entity from public sources (e.g. annual returns and filing with ACRA); or* (iv) *information obtained from other reliable sources (e.g. research reports, third-party service providers) or other research.]*	*[To describe.]*
10. Names of all individuals holding a senior management position (e.g. directors of a company, partner and manager of a limited liability partnership, president, treasurer and secretary of a society)	
11. Contact number(s)	
(C) ACKNOWLEDGEMENT	
Name of person(s) purporting to act on behalf of purchaser:	
Signature	
Date:	

FORM C

DETAILS OF BENEFICIAL OWNER(S) (BO) OF AN ENTITY OR LEGAL ARRANGEMENT PURCHASER

(A) PARTICULARS OF BO	
1. Full name, including any alias used	
2. Identification number	
3. Type of identification (document must be issued by a government)	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
4. Expiry date of identification document (if applicable)	
5. Date of birth	
6. Place of birth	
7. Address of usual place of residence	
8. Nationality	
9. Occupation	
10. Contact number(s)	
11. State reason for being a BO (e.g. own xx% of shares of the company)	
12. Is the BO a current or former PEP?	☐ Yes ☐ No
13. Is the BO a family member of a current or former PEP?	☐ Yes ☐ No
14. Is the BO a close associate of a current or former PEP?	☐ Yes ☐ No
15. If any of the responses to Qn 12 to 14 is "Yes", please complete **Form E "Details of PEP(s)".**	
(B) BO'S ACKNOWLEDGEMENT	
Name(s) of BO(s):	
Signature:	
Date:	

FORM D

DETAILS OF NATURAL PERSON(S)/ENTITY/LEGAL ARRANGEMENT ON WHOSE BEHALF THE PURCHASER (WHO IS A NATURAL PERSON) IS ACTING

Note: Form D must be completed for each and every person, or beneficial owner(s) (BO) of each entity or legal arrangement. Use additional forms if necessary.

In relation to an entity or a legal arrangement, a BO refers to an individual who ultimately owns or controls the entity or legal arrangement, or who exercises ultimate effective control over the entity or legal arrangement, or on whose behalf the transaction is being conducted.

Ultimate effective control depends on the ownership structure of the entity or legal arrangement. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).

(I) WHERE THE PERSON(S) ON WHOSE BEHALF THE PURCHASER IS ACTING, IS A NATURAL PERSON

(A) PARTICULARS OF NATURAL PERSON	
1. Full name, including any alias used	
2. Identification number	
3. Type of identification (document must be issued by a government)	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
4. Expiry date of identification document (if applicable)	
5. Date of birth	
6. Place of birth	
7. Address of usual place of residence	
8. Nationality	
9. Occupation	
10. Contact number(s)	
11. Authorisation document, showing that the natural person has authorised the purchaser to act on his/her behalf (e.g. authorisation letter or Power of Attorney)	
12. State reason for appointing the purchaser to act on person's own behalf	
13. Is the person on whose behalf the purchaser is acting, a current or former PEP?	☐ Yes ☐ No

14. Is the person on whose behalf the purchaser is acting, a family member of a current or former PEP?	☐ Yes ☐ No
15. Is the person on whose behalf the purchaser is acting, a close associate of a current or former PEP?	☐ Yes ☐ No
16. If any of the responses to Qn 13 to 15 is "Yes", please complete **Form E "Details of PEP(s)".**	
(B) ACKNOWLEDGEMENT FROM NATURAL PERSON ON WHOSE BEHALF PURCHASER IS ACTING	
Name(s) of person on whose behalf the purchaser is acting	
Signature:	
Date:	

* Delete whichever is inapplicable

(II) WHERE THE PERSON(S) ON WHOSE BEHALF THE PURCHASER IS ACTING, IS AN ENTITY

(A) PARTICULARS OF ENTITY	
1. Full name of entity	
2. Identification or registration number	
3. Type of identification (e.g. Business Profile from the Accounting and Corporate Regulatory Authority, any other document issued by any government certifying the incorporation, registration or existence)	
4. Expiry date of identification document (if applicable)	
5. Place of incorporation/ registration	
6. Address of registered office (to indicate as "shared" if it is a shared address)	
7. Address of principal place of business (to be completed if the registered office is not the principal place of business)	
8. Nature of business (e.g. principal activities as stated in ACRA's Business Profile)	
9. Ownership and control structure of entity *[Pointer: Information that may be provided:* *(iv) memorandum and articles of association;* (v) *information available on the entity's website or published annual reports;* (vi) *information available on the entity from public sources (e.g. annual returns and filing with the Accounting and Corporate Regulatory Authority (ACRA), ACRA's business profile)]*	*[To describe]*
10. Details of all individuals holding a senior management position (e.g. senior managing directors in a company)	<u>Individual 1</u> • Name, including any alias: • Date of birth: • Place of birth: • Identification no.: • Identification document: • Nationality:

	• Address of place of residence: • Contact no.: • Position held: <u>Individual 2</u> • Name, including any alias: • Date of birth: • Place of birth: • Identification no.: • Identification document: • Nationality: • Address of place of residence: • Contact no.: • Position held:
11. Contact number(s)	
12. Purpose of purchase	☐ Owner-Occupation ☐ Investment/Rental ☐ Others (Please specify) _____
13. Authorisation document, showing that the entity has authorised the purchaser to act on its behalf (e.g. authorisation letter or Power of Attorney)	
(B) PARTICULARS OF BENEFICIAL OWNER(S) (BO)	
14. Does the entity have any BO? *BO refers to an individual:* *d) who ultimately owns or controls the entity or legal arrangement;* *e) who exercises ultimate effective control over the entity or legal arrangement; or* *f) on whose behalf the entity or legal arrangement conducts any transaction with a developer.* *Ultimate effective control depends on the ownership structure of the entity or legal arrangement. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).*	☐ Yes ☐ No If "yes", please complete **Form C "Details of BO".**
(C) ACKNOWLEDGEMENT FROM ENTITY ON WHOSE BEHALF PURCHASER IS ACTING	
Name of person acting on behalf of the entity	

Position in the entity	
Signature	
Date	

(III) WHERE THE PERSON(S) ON WHOSE BEHALF THE PURCHASER IS ACTING, IS A LEGAL ARRANGEMENT

(A) PARTICULARS OF LEGAL ARRANGEMENT	
1. Full name of legal arrangement	
2. Type of legal arrangement	☐ Trust ☐ Others (Please specify) _____
3. Country in which the legal arrangement is constituted	
4. Nature of business	
5. Proof of the legal arrangement's existence	
6. Instrument under which the legal arrangement is constituted e.g. deed of trust	
7. Authorisation document, showing that the legal arrangement has authorised the purchaser to act on its behalf (e.g. authorisation letter or Power of Attorney)	
APPLICABLE WHERE THE LEGAL ARRANGEMENT IS A TRUST	
8. Full name of **settlor**	
9. Identification number	
10. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
11. Expiry date of identification document (if applicable)	
12. Date of birth	
13. Place of birth	
14. Address of usual place of residence	
15. Nationality	

16. Occupation	
17. Contact number(s)	
18. Full name of **trustee(s)**	
19. Identification number	
20. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
21. Expiry date of identification document, if applicable	
22. Date of birth	
23. Place of birth	
24. Address of usual place of residence	
25. Nationality	
26. Occupation	
27. Contact number(s)	
28. Full name of **protector**	
29. Identification number	
30. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
31. Expiry date of identification document (if applicable)	
32. Date of birth	
33. Place of birth	
34. Address of usual place of residence	
35. Nationality	
36. Occupation	
37. Contact number(s)	
38. Full name/class of **beneficiary(ies)**	
39. Identification number	
40. Type of identification document	☐ NRIC ☐ Passport ☐ Others (Please specify) _____
41. Expiry date of identification document (if applicable)	
42. Date of birth	
43. Place of birth	
44. Address of usual place of residence	

45. Nationality	
46. Occupation	
47. Contact number(s)	
48. Full name of any other person(s) **exercising ultimate ownership/control over the trust**	
49. Identification number	
50. Type of identification document	☐ NRIC ☐ Passport ☐ Others: (Please specify) _____
51. Expiry date of identification document (if applicable)	
52. Date of birth	
53. Place of birth	
54. Address of usual place of residence	
55. Nationality	
56. Occupation	
57. Contact number(s)	
APPLICABLE WHERE THE LEGAL ARRANGEMENT IS NOT A TRUST	
58. Full name of person holding a position equivalent or similar to a settlor, trustee, protector, beneficiary and any other person exercising ultimate effective control over the trust	
59. Identification number	
60. Type of identification document	☐ NRIC ☐ Passport ☐ Others: (Please specify) _____
61. Expiry date of identification document (if applicable)	
62. Date of birth	
63. Place of birth	
64. Address of usual place of residence	
65. Nationality	
66. Occupation	
67. Contact number(s)	
(B) PARTICULARS OF BENEFICIAL OWNER(S) (BO)	
68. Does the legal arrangement have any BO?	☐ Yes ☐ No

BO refers to an individual: *d) who ultimately owns or controls the entity or legal arrangement;* *e) who exercises ultimate effective control over the entity or legal arrangement; or* *f) on whose behalf the entity or legal arrangement conducts any transaction with a developer.* *Ultimate effective control depends on the ownership structure of the entity or legal arrangement. It may be based on a threshold, e.g. any person owning more than a certain percentage of the company (e.g. 25% based on FATF recommendations).*	If yes, please complete **Form C "Details of BO".**
(C) ACKNOWLEDGEMENT FROM LEGAL ARRANGEMENT ON WHOSE BEHALF PURCHASER IS ACTING	
Name of person acting on behalf of the legal arrangement	
Position in legal arrangement	
Signature	
Date	

FORM E

DETAILS OF POLITICALLY EXPOSED PERSON(S) ("PEP")
(Use additional forms if necessary)

(A) PARTICULARS OF PEP	
I am a:	Please tick the appropriate box: ☐ Domestic PEP ☐ Foreign PEP ☐ International Organisation PEP *Domestic PEP means an individual who is or has been entrusted with any prominent public function in Singapore;* *Foreign PEP means an individual who is or has been entrusted with a prominent public function in a foreign country;* *International Organisation PEP means an individual who is or has been a member of the senior management of an international organisation (including a director, deputy director or member of a board of the international organisation, or an equivalent appointment in the international organisation).* **Or** Family member of a: ☐ Domestic PEP ☐ Foreign PEP ☐ International Organisation PEP As a: ☐ Parent/ step-parent ☐ Spouse ☐ Child/ adopted child/ step-child ☐ Sibling/ adopted sibling/ step-sibling **Or** Close associate^ of a: ☐ Domestic PEP ☐ Foreign PEP ☐ International Organisation PEP My relationship with the PEP: _____ (please describe) *^ Close associate means —*

	(a) a partner of the PEP; *(b) a person accustomed or under an obligation, whether formal or informal, to act in accordance with the directions, instructions or wishes of the PEP;* (c) *a person whose directions, instructions or wishes the PEP is accustomed or under an obligation, whether formal or informal, to act in accordance with; or* (d) *a person with whom the PEP has an agreement or arrangement, whether oral or in writing and whether express or implied, to act together.*
Name of PEP/family member/close associate of PEP*, including any alias used	
Name (and description of responsibilities if not self-explanatory from the name) of the prominent public function that the PEP is currently or formerly entrusted with	
Country	
Period of service	From _____ To _____

(B) ACKNOWLEDGEMENT	
Name of PEP/family member/close associate of PEP*:	
Signature:	
Date:	

* Delete whichever is inapplicable

FORM F

SCREENING OF PURCHASERS FOR MONEY LAUNDERING (ML), PROLIFERATION FINANCING (PF) AND TERRORISM FINANCING (TF) RISKS

Note: Developers are required to screen <u>ALL:</u>

<u>(a)</u> purchasers named in the Option to Purchase or Sale and Purchase Agreement;
(b) BOs of the purchaser(s), where the purchaser(s) is an entity or legal arrangement;
(c) natural persons/entity/legal arrangement on whose behalf the purchaser(s) is acting;
(d) BOs of the entity/legal arrangement on whose behalf the purchaser(s) is acting;
(e) individuals holding senior management position in the entity which has been identified under (b) to (d).

(i.e. "persons screened"), whichever is applicable, for ML, PF and TF risks.

Use additional forms if necessary.

1. Do you suspect any of the persons screened is:		
a. a terrorist or terrorist entity under the First Schedule of the Terrorism (Suppression of Financing) Act?; or	☐ Yes	☐ No
b. a designated person as defined in any regulations made under the United Nations Act?; or	☐ Yes	☐ No
c. a person suspected of, or at risk of, facilitating ML, PF or TF who is specified by the Controller in any written notice issued by the Controller?; or	☐ Yes	☐ No
d. involved in ML/PF/TF, based on _____ (specify source of information, e.g. Internet search, third-	☐ Yes Please state: i. Name of purchaser / person on whose behalf	☐ No

party screening database)?	purchaser is acting / BO of purchaser / person acting on behalf / senior management in entity or legal arrangement* of the individual under suspicion: _____ ii. Grounds of suspicion (e.g. full name match and same nationality): _____ *[Pointer: For all ML/PF/TF suspicions, developers must file a STR. For (a) to (c), developers must not grant an option to purchase any unit to the purchaser, accept any money (including booking fee) from the purchaser, or enter into a S&PA for a unit with the purchaser or assignee purchaser.* *For (d), developer must seek approval from a person holding senior managerial or executive position in the developer to proceed with the transaction]*	
2. Do you suspect any of the persons screened is from a foreign country: a. that the FATF identifies as a foreign country subject to counter measures; b. that the FATF identifies as a foreign country subject to increased monitoring; c. known to have inadequate measures to prevent ML, PF or TF as notified to you, the developer, generally by the Controller or other	☐ Yes ☐ Yes ☐ Yes Please state: Name of purchaser / BO of purchaser / person on whose behalf purchaser is acting / person acting on behalf / senior	☐ No ☐ No ☐ No

relevant authorities in Singapore	management in entity* under suspicion: _____ The foreign country which the individual is from: _____	
3. Do you suspect any of the persons screened is a PEP, family member or a close associate of a PEP?	☐ Yes Please complete **Form E "Details of PEP(s)"**	☐ No
4. Do you suspect any of the persons screened is of higher risk, e.g. linked to adverse news relating to ML, PF or TF?	☐ Yes Please specify the following: a) Name of purchaser / BO of purchaser / person on whose behalf purchaser is acting / person acting on behalf/ senior management in entity* under suspicion: _____ b) the basis of the determination and source of information: _____	☐ No
5. Is the transaction with the purchaser complex or unusually large, or is part of an unusual pattern of transactions which have no apparent economic or visible lawful purpose? *[Pointer: Complex transactions include attempts to disguise the BO(s) involved in the transaction, use of unnecessarily complex transaction structures designed to obscure the true nature of the*	☐ Yes Please provide the basis of the determination and details of the transaction.	☐ No

transaction or involving the use of multiple intermediaries for the transaction. Unusually large transactions could include a transaction priced at more than the usual or expected amount for a similar typical transaction. Transactions with no apparent economic or lawful purpose could include using trust and company service providers to set up a number of corporate structures in multiple jurisdictions for the transaction without any apparent purpose]		
OVERALL RISK ASSESSMENT		
6. Risk level:	☐ Higher *(if any of the answers to questions 1 to 5 above is "yes")* *[Pointer: Seek approval from a person holding senior managerial or executive position in the developer to continue with the transaction.]*	☐ Lower
7. To proceed with transaction/ continue with the transaction?	☐ Yes For purchasers assessed to be of higher risk, please attach a copy of the approval document endorsed by the senior management of the company, with the date of approval indicated. The approval document should include the following, in addition to those mentioned in questions 1 to 4 above:	☐ No

	a. information on income level, source of wealth (SoW) and source of funds (SoF) of the relevant person); b. corroboration of the information obtained in (a) above; c. identifying information of the person on whose behalf the purchaser is acting ("Person P"), where the developer suspects that the purchaser trying to conceal the identity of Person P; d. target date / milestones to conduct <u>enhanced</u> ongoing monitoring of the transaction(s) entered into with the purchaser. Please specify the types of checks to be conducted e.g. income level, SoW, SoF etc.	
8. Is a STR filed?	☐ Yes Please state the basis of the determination	☐ No
9. Target date or milestone for <u>ongoing</u> monitoring *(Pointer: the target date for ongoing monitoring should be before the target date of issuing the notice of payment for TOP and legal completion, whichever is applicable)*	Date/ Milestone: _____ Please complete **Form G "Ongoing monitoring of transactions".**	

* Delete whichever is inapplicable

Evaluation and Assessment completed by: Name and signature of developer's representative: _____ Designation: _____ Date: _____	
The following section is applicable only if the screening is completed by a Third Party	
Name of Third Party	
Signature	
Occupation of Third party	☐ Salesperson ☐ Legal professional ☐ Others (Please specify) _____
Company's name	

FORM G

ONGOING MONITORING OF TRANSACTIONS

Note: Ongoing monitoring of transactions are NOT allowed to be conducted by a third party

<table>
<tr><td>1. Are the CDD data, documents and information that were obtained earlier, ascertained to be adequate before issuing the notice of payment for TOP and for completion of sale?</td><td>☐ Yes</td><td>☐ No
Please provide details and complete a new CDD checklist for the purchaser.
_____
_____</td></tr>
<tr><td>2. Are the transactions by the purchaser consistent with the developer's knowledge of:
a. the purchaser; and
b. the purchaser's income and risk profile; and
c. the purchaser's source(s) of funds.</td><td>☐ Yes</td><td rowspan="2">☐ No

Please complete Form F "Screening for money laundering, proliferation financing Risks" again.</td></tr>
<tr><td>3. Risk of money laundering, proliferation financing or terrorism financing remains unchanged</td><td>☐ Yes</td></tr>
<tr><td colspan="3">Evaluation and Assessment completed by:

Name and signature of developer's representative: _____

Designation: _____

Date: _____
(Pointer: The form should be completed by the target date set in Form F "Screening of purchasers for money laundering, proliferation financing and terrorism financing risks)</td></tr>
</table>