GHL Resources

CEA Licence No: L3011042J

AML / CPF / CFT COMPLIANCE FRAMEWORK

Internal Policies, Procedures and Controls (IPPC) for the Prevention of Money Laundering, Proliferation Financing and Terrorism Financing

Issued pursuant to the Estate Agents Act 2010 (Part 4A) and the Estate Agents (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Regulations 2021

Document control	
Version	1.0
Effective date	1 January 2026 (full compliance with revised PMLPFTF requirements is mandatory for all transactions from 1 January 2026)
Document owner	Compliance Officer, Adrian Goh, Key Executive Officer
Approved by	Key Executive Officer (KEO), Adrian Goh
Review cycle	At least annually, and upon any change to legislation, CEA guidance, or the Agency's business
Applies to	All Real Estate Salespersons (RESs), the KEO, directors, and all administrative and support staff of the Agency

Contents

Part 1 — Purpose, Scope and Regulatory Basis

1.1 This Framework sets out the Agency's internal policies, procedures and controls (IPPC) to detect, prevent, mitigate and report money laundering (ML), proliferation financing (PF) and terrorism financing (TF) risks arising from estate agency work. It gives effect to the three key roles CEA prescribes for estate agents (EAs) and real estate salespersons (RESs): conducting due diligence on customers and unrepresented counterparties, reporting suspicious transactions, and establishing risk assessment, internal controls and compliance procedures.

1.2 This Framework is binding on every RES registered under the Agency and on all staff. Non-compliance with this Framework may amount to a breach of law and will be dealt with under Part 14 (Breach Management).

1.3 Scope of transactions. This Framework applies to ALL sale, purchase and rental transactions of any property type (HDB resale, private residential, commercial, industrial, land), with no minimum transaction value. The only exemption from CDD and UCPDD measures is a rental of an HDB property that is wholly for residential use (whole-flat or room rental). Even for exempted HDB residential rentals, the obligation to file a Suspicious Transaction Report (STR) still applies where suspicion arises.

1.4 Regulatory basis. This Framework implements the requirements of: (a) the Estate Agents Act 2010 (EAA), in particular Part 4A and section 44C; (b) the Estate Agents (Prevention of Money Laundering, Proliferation Financing and Terrorism Financing) Regulations 2021 (PMLPFTF Regulations); (c) the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA), sections 45, 47 and 57; (d) the Terrorism (Suppression of Financing) Act 2002 (TSOFA); (e) the United Nations Act 2001 and regulations made under it; (f) the Personal Data Protection Act 2012 (PDPA); and (g) CEA's Guide on the PMLPFTF Regulations (version 30 June 2025), the prescribed template forms, CEA's FAQs (29 December 2025), and CEA's industry briefing of 3 September 2025.

1.5 Where this Framework is silent or ambiguous, the PMLPFTF Regulations and the EAA prevail, and the matter must be escalated to the Compliance Officer.

> **Key deadline already in force**
> CEA's transition period ended on 31 December 2025. Every transaction from 1 January 2026 must FULLY comply with the revised PMLPFTF requirements, including UCPDD, PF screening, submission of all due diligence documents to the Agency, and use of the 30 June 2025 forms. Forms from the superseded PMLFT Guide must no longer be used.

Part 2 — Governance, Roles and Accountability

2.1 Compliance Officer

2.1.1 The Agency has appointed a Compliance Officer at management level. The Compliance Officer must be a designated officer of the Agency (CEO, KEO, director, partner, member of a management committee/manager, or an officer duly authorised by the Agency). For a sole proprietorship, the sole proprietor/KEO is the Compliance Officer. The appointment is documented by a letter of appointment retained in the Agency's records, and the identity of the Compliance Officer is communicated to all RESs through this Framework and onboarding materials.

2.1.2 The Compliance Officer is responsible for: (a) being trained in and familiar with Part 4A of the EAA, the PMLPFTF Regulations and all relevant CEA and government guidance; (b) ensuring the Agency and every RES fully comply with those obligations; (c) ensuring timely and effective remedial action whenever non-compliance is found; (d) conducting or arranging regular internal checks and independent audits; (e) approving or rejecting higher-risk relationships as designated officer under Regulation 6(3)(a); (f) filing STRs via SONAR using the Agency's CorpPass; and (g) maintaining this Framework and the Agency's entity risk assessment.

2.1.3 Where one individual serves as compliance officer for more than one estate agency in a group, that individual must meet the definition of designated officer for each entity, be formally appointed by each, and have adequate capacity to discharge the role across all entities.

2.2 Key Executive Officer (KEO)

2.2.1 The KEO ensures that: (a) this Framework is documented, kept current and readily accessible to all RESs and relevant staff; (b) regular training on the IPPC is conducted; (c) implementation is monitored and the IPPC enhanced where necessary; and (d) updates are made when regulatory requirements or business operations change.

2.3 Real Estate Salespersons (RESs)

2.3.1 Every RES must, for every in-scope transaction: (a) complete CDD (and where applicable UCPDD, ECDD and ongoing due diligence) before the client enters into any agreement to acquire or dispose of property; (b) screen all relevant persons against the mandatory lists; (c) document risk determinations and conclusions on the prescribed forms; (d) promptly submit ALL forms, information and supporting documents obtained to the Agency — both the Agency and the RES are jointly responsible for proper record-keeping; (e) escalate suspicions to the Compliance Officer without delay and take the necessary steps to file an STR; and (f) never tip off any person about screening results, risk assessments or STR filings.

2.3.2 RESs must NEVER backdate, fabricate or alter due diligence documentation to conceal non-compliance. Doing so is treated as gross misconduct and will be reported to CEA where required.

2.4 Three lines of defence

2.4.1 First line: RESs and their team leaders performing due diligence in the transaction workflow. Second line: the Compliance Officer, who advises, approves higher-risk relationships, monitors implementation and files STRs. Third line: the independent audit function under Part 12, which tests compliance on a sampling basis and is never performed by a person auditing their own transactions.

Part 3 — Agency-Level Risk Assessment

3.1 The Compliance Officer conducts and documents an entity-level ML/PF/TF risk assessment using CEA's suggested template (Annex E of the PMLPFTF Guide), analysing the Agency's transactions over the past three years across: transaction types (sales and leases), client profiles (local/foreign, individual/corporate), property types (residential/commercial/industrial), transaction patterns and values, payment methods, geographic factors, non-face-to-face dealings and complex ownership structures.

3.2 Suggested higher-risk indicators adopted by the Agency, in line with CEA's template: physical cash transactions (e.g. above S$20,000); sale and purchase transactions at S$3 million or higher; three or more properties transacted by one customer in a year; monthly rental of S$10,000 or higher; foreign buyer/seller/tenant/landlord involvement (including PRs for analysis purposes); complex corporate structures; and any red flags in Annex B of this Framework.

3.3 The risk assessment is reviewed and updated at least annually, kept up to date in between where CEA notifies the Agency of risks, and informs the intensity of due diligence, monitoring frequency, training focus and audit sampling. RESs and the Agency must also take reference from the national Money Laundering, Terrorism Financing and Proliferation Financing National Risk Assessments published on the MAS website.

3.4 Before launching any new service, business practice or technology (e.g. non-face-to-face onboarding tools, new client-instruction systems, acceptance of new payment methods such as virtual assets), the Agency must first assess the ML/PF/TF risks and implement mitigating measures. No new service or technology may be launched without the Compliance Officer's sign-off.

Part 4 — Customer Due Diligence (CDD)

4.1 When CDD must be performed

4.1.1 CDD must be COMPLETED before the client enters into any agreement to acquire or dispose of property — i.e. before the Option to Purchase (OTP) is issued/exercised or the Tenancy Agreement (TA) is signed. CDD completed after the OTP is signed is CEA's most commonly cited breach and is treated by the Agency as non-compliance. CDD must also be refreshed whenever there is doubt about the accuracy or adequacy of previously obtained identification data, and in any other circumstances prescribed by CEA.

4.1.2 An estate agency agreement setting out the terms of the business relationship must be entered into with the client before conducting any estate agency work. Use the prescribed estate agency agreements and have them signed upfront.

4.1.3 Due diligence is not required merely to arrange viewings or introduce properties. It becomes due once the sale/lease is likely to proceed (e.g. an offer has been made and the client indicates willingness to accept), and must be completed before any binding agreement is entered into. CDD and UCPDD may be performed concurrently while preparing transaction paperwork.

4.2 Core CDD measures

4.2.1 For every in-scope transaction the RES must: (a) identify the client and verify identity from reliable, independent sources; (b) where the client is an entity or legal arrangement, identify and take reasonable measures to verify its beneficial owners (BOs); (c) determine whether the client is acting on behalf of another person and, if so, obtain evidence of authority (POA, letter of authorisation, board resolution or equivalent) and perform full CDD on that other person; (d) determine and document the ML/PF/TF risk of the client and any person the client acts for; and (e) screen all such persons under Part 5.

4.2.2 Acceptable verification documents (preferring those hardest to counterfeit): NRIC, passport or other government-issued photo ID; Singpass App verification; MyInfo reports; independent company registry records (e.g. ACRA BizFile); published or audited annual reports. Documents must be current, clear and legible; the verifying RES signs and dates copies sighted; certified true copies (notary public, lawyer, public/professional accountant) may be accepted where originals cannot be produced. Rigour must match the client's risk profile, especially for non-face-to-face onboarding.

4.3 Entities, trusts and legal arrangements

4.3.1 For a legal person, obtain and verify: name; legal form; proof of existence (e.g. ACRA BizFile); place of incorporation; constitutional documents (constitution/M&A, partnership deed, trust deed, society rules, or equivalent); UEN or foreign registration number; identities of senior management; and registered office / principal place of business.

4.3.2 The client is the company itself, not the representative you liaise with (HR manager, CFO, director). Verify the representative's identity AND authority (letter of authorisation, board/director's resolution, or company policy documents — a verbal assurance is not sufficient, even from an ACRA-named director), then conduct CDD on the company and its BOs.

4.3.3 Beneficial owners are the natural persons who ultimately own or control the entity or exercise ultimate effective control. As working guidance: any individual holding or controlling at least 25% of the shares, voting rights or assets. If no such individual exists or there is doubt, identify individuals exercising control by other means; failing which, identify senior management. Directors on ACRA are not automatically BOs. For layered or offshore structures (e.g. BVI), trace on a best-effort basis to the ultimate individuals using share registers, shareholder lists or BO declarations; if the structure cannot be penetrated after reasonable efforts, treat it as a potential red flag, apply ECDD, obtain Compliance Officer approval, and consider an STR.

4.3.4 Publicly listed entities on SGX or a foreign exchange with adequate BO transparency requirements: individual BO identification is not required. Instead obtain and verify the PLE's identifying information, understand its structure from public filings, and screen the PLE.

4.3.5 Trusts: identify and take reasonable measures to verify the settlor, all trustees, any protector, each beneficiary or class of beneficiaries, and any other individual exercising ultimate effective control. Estates of deceased persons are legal arrangements: the executor completes Form A1 and Form A4 is prepared for the beneficiaries, with Form B screening for each. Other legal arrangements: identify persons in equivalent positions.

4.3.6 Power of Attorney: the POA holder instructing the RES is the client (Form A1); the actual owners are the persons the client acts for (Form A3); conduct Form B screening on both. Sole proprietors and general partnerships use individual forms (Form A1); LLPs and companies use entity forms (Form A2).

4.3.7 Singapore Government entities (Ministries, Organs of State, statutory boards): confirm the entity's government status and the representative's authority; the Regulation 5(6) relaxation applies. It does NOT extend to foreign embassies or diplomatic missions — full CDD applies to them, including MFA verification, foreign-PEP determination and adverse news checks.

4.4 Rental transactions

4.4.1 HDB rentals wholly for residential use (whole flat or room, including the living quarters of an HDB shophouse rented on their own) are exempt from CDD/UCPDD: no forms or screening are required, but the STR obligation remains, and where doubts arise the RES should nonetheless conduct checks and file an STR if warranted. A tenancy covering the commercial space of an HDB shophouse (alone or together with living quarters) is NOT exempt.

4.4.2 For all other rentals, CDD applies. Where BOTH the client/UCP and the transaction are assessed low risk under Regulations 7/12E, BO identification for corporate parties may be omitted (omit Section 3 of Form A2/U2; one Form B/U5 for the entity). Risk may never be defaulted to "low" to avoid work — every assessment must be a genuine, documented judgement on the facts. Occupiers who are not parties to the TA do not require CDD, but their identification must still be collected and verified under the Women's Charter/Immigration Act practice guidelines.

Part 5 — Screening and PEP Determination

5.1 For every client, BO, person the client acts for, and UCP (and their principals/BOs), the RES must screen against ALL of: (a) the First Schedule of the TSOFA; (b) the UN Security Council Consolidated List and lists under regulations made under the UN Act 2001; (c) FATF's high-risk and other monitored jurisdictions ("black and grey" lists); and (d) any lists provided by CEA or other authorities. The Agency subscribes to MAS's targeted financial sanctions alerts and the MHA IMC-TD mailing list, and circulates updates to all RESs.

5.2 Evidence of screening is mandatory: manual screeners must capture date/time-stamped screenshots of results; users of the Agency's commercial screening solution must retain the screening report. All evidence is recorded on Form B/U5 and submitted to the Agency.

5.3 Positive sanctions hit (TSOFA/UN): unless an Exemption Order has been obtained, the RES must NOT carry out the transaction, must terminate any transaction already entered into, must immediately inform the Compliance Officer, and an STR must be filed. Continuing to facilitate the transaction may itself be an offence under the TSOFA or UN Act. Do not disclose the hit or the STR to the client, the UCP or any other party; simply inform your client that the transaction cannot proceed.

5.4 PEP determination: take reasonable measures (internet/media searches, commercial databases) to determine whether any relevant person is a politically exposed person — a person entrusted with prominent public functions in Singapore or abroad (head of state/government, minister, senior civil servant, senior judicial/military official, senior executive of a state-owned corporation, senior political party official, legislator) or a prominent function in an international organisation — or a family member or close associate of one. Any FOREIGN PEP, or family member or close associate of a foreign PEP, automatically triggers ECDD under Part 6.

Part 6 — Enhanced Customer Due Diligence (ECDD)

6.1 ECDD (Form C for clients; Form U6 for UCPs) is mandatory, in addition to CDD, in any of these higher-risk situations: (a) the transaction presents higher ML/PF/TF risk — including complex or unusually large transactions, or unusual patterns with no apparent economic or lawful purpose; (b) any transacting party, principal or BO is from or in a FATF-identified high-risk or monitored jurisdiction; (c) any such person is a foreign PEP or a family member or close associate of one; or (d) the RES has reason to suspect any such person is engaged in ML/PF/TF. Record the reasons for conducting ECDD and every additional step taken.

6.2 ECDD measures: (a) take reasonable measures to establish the income level, source of wealth (SOW — the origin of the person's entire body of wealth) and source of funds (SOF — the origin and generating activity of the specific funds for this transaction) of the client/UCP and, where an entity, of its BOs; (b) obtain the PRIOR approval of the Compliance Officer (as designated officer) before establishing or continuing the business relationship; and (c) where the relationship continues, apply risk-appropriate measures including closer monitoring of transactions against the person's profile.

6.3 SOW/SOF must be corroborated with reliable, independent documents — e.g. OTP/completion documents for a prior property sale; IRAS Notices of Assessment, payslips or tax statements for employment income; ACRA records, audited financial statements, bank statements or tax returns for business income (with overseas equivalents); and probate/estate documents or bank statements plus evidence of relationship for gifts and inheritance. A landlord's SOW/SOF check should verify how the property was acquired; a tenant's should cover deposits, advance payments and rent.

6.4 Never tell a client or UCP that SOW/SOF is being sought because they are considered high-risk or suspected of ML/PF/TF — explain only that the law requires the information. If the person refuses or gives unsatisfactory explanations, do not proceed, document the attempts and responses, escalate to the Compliance Officer and consider an STR. Whether an explanation is adequate is a holistic judgement: corroborated explanations (e.g. documented windfall) can resolve red flags; vague, uncorroborated claims (e.g. unnamed offshore companies funding a purchase) do not.

Part 7 — Unrepresented Counterparty Due Diligence (UCPDD)

7.1 Where the other party to the transaction (not the Agency's client) has no EA/RES representing them (a "DIY" party), the RES must conduct UCPDD on that unrepresented counterparty before the client enters into any agreement for the acquisition or disposition of the property. This applies to all sale, purchase and rental transactions except HDB residential rentals. In a co-broke transaction where each party has their own RES, no UCPDD is needed and CDD documents are NOT exchanged between co-broking RESs.

7.2 UCPDD mirrors CDD: identity verification, entity/legal-arrangement measures, BO identification, authority checks where the UCP acts for another, sanctions and PEP screening, risk determination, enhanced due diligence in higher-risk situations, and record-keeping — using Forms U1–U6. Timing follows clause 4.1.3: perform UCPDD when it becomes clear the deal is likely to proceed, before the OTP/TA.

7.3 If the UCP refuses to provide information after the legal requirement is explained, the transaction must not proceed (Regulation 12H); document the attempts and consider an STR. If sanctions screening on the UCP is positive, follow clause 5.3 — cease dealing, inform the Compliance Officer, file an STR, and do not tell the client or the UCP why.

7.4 In developer sales where the RES conducts due diligence on unrepresented buyers on the developer's behalf, the information gathered may concurrently satisfy the RES's own UCPDD obligations; inform the UCP that the documents will also be retained by the Agency, and retain copies (a developer's equivalent particulars form with the buyer's acknowledgement may stand in for Form U1).

Duty	Client	Unrepresented counterparty
Establish client-agent relationship (estate agency agreement)	Yes	No
Obtain identifying information and verify identity	Yes	Yes
Establish whether the party is an entity/legal arrangement; identify BOs	Yes	Yes
Screen against UN lists, TSOFA First Schedule and lists from authorities; PEP determination	Yes	Yes
Enhanced due diligence where required	Yes	Yes
Keep records / submit to Agency	Yes	Yes
Ongoing monitoring (continuing business relationship)	Yes	No
File STR on suspicion of ML/PF/TF	Yes	Yes

Part 8 — Ongoing Due Diligence

8.1 Ongoing due diligence applies to clients with a continuing business relationship — e.g. a client for whom the RES handles multiple transactions over time, a landlord whose property the RES has managed since a prior tenancy, developers or REIT property managers. A one-off engagement every few years generally lacks the continuity of an ongoing relationship.

8.2 For such clients the RES must: (a) periodically review transactions for consistency with the client's known profile, income and source of funds, querying the client where inconsistent; (b) check that identification documents remain valid and current, refreshing them where outdated; and (c) apply more frequent reviews (e.g. six-monthly) to higher-risk clients such as foreign PEPs. Reviews are recorded on Form D and submitted to the Agency; fresh CDD is performed periodically and whenever doubts or significant changes arise. Ongoing due diligence can NEVER be delegated to a third party.

Part 9 — Suspicious Transaction Reporting (STR)

9.1 Under sections 45(1)–(2) CDSA, any person who in the course of their trade or business knows or has reasonable grounds to suspect that any property may be connected to drug dealing or criminal conduct must file an STR as soon as reasonably practicable — whether or not the transaction completes. Failure to file is an offence: for individuals, a fine up to S$250,000 and/or imprisonment up to 3 years; for entities, a fine up to S$500,000.

9.2 Agency procedure. An RES who suspects ML/PF/TF must (a) immediately (and in any case within 24 hours of forming the suspicion) report the facts to the Compliance Officer, and (b) take the necessary steps to file the STR through the Agency via SONAR (www.police.gov.sg/sonar), accessed with the Agency's CorpPass. The RES remains primarily responsible for ensuring the STR is filed; if the RES does not file, the Agency MUST file. Where required (e.g. positive sanctions hit, inability to complete due diligence with suspicion), the suspicious transaction must be reported BEFORE proceeding with any property transaction. RESs report suspicion and file — they are not expected to investigate.

9.3 STR filers are protected: good-faith disclosure to STRO is not a breach of any law, contract or professional rule; the filer's identity is protected under section 47 CDSA and STR contents are not admissible as evidence in civil or criminal proceedings.

9.4 Tipping off is a crime. Under section 57 CDSA it is an offence (fine up to S$250,000 and/or 3 years' imprisonment) to disclose anything that might prejudice an investigation — including telling anyone (the client, the UCP, a co-broking RES, colleagues without a need to know) that an STR has been or will be filed, that screening was positive, or that the person is considered suspicious. Risk assessments and Form B/U5 conclusions are internal documents and are never shown or read out to clients or UCPs.

9.5 Deciding whether to file is the RES's and Agency's own holistic judgement on the known facts — CEA will not decide for you. A single red flag is not automatically suspicious; multiple unexplained red flags usually are. When in doubt, escalate to the Compliance Officer and err on the side of filing.

Part 10 — Inability to Complete Due Diligence

10.1 If any required CDD/UCPDD/ECDD measure cannot be performed or completed — information cannot be obtained or verified, or enquiries receive no satisfactory response — the RES must NOT carry out the transaction, must terminate any existing business relationship with the client, must escalate to the Compliance Officer, and must consider filing an STR.

10.2 The RES may deliberately refrain from performing or completing CDD where there are reasonable grounds to suspect ML/PF/TF and performing CDD would tip off the client or another person — in which case an STR is filed instead.

10.3 Records of the intended transaction must be kept for at least 5 years: date and amount, property type and address, basis for suspicion, STR determination, all supporting documents, and the name and registration number of the handling RES.

Part 11 — Reliance on Third Parties

11.1 The Agency and its RESs may rely on another licensed EA to perform CDD only where multiple RESs represent the SAME client (not co-broke situations), and only if all CDD documentation (particulars forms, screening results, supporting documents) is obtained immediately and the third party can produce identification data promptly on request. The Agency and RES remain FULLY liable for CDD deficiencies of the third party. Ongoing due diligence cannot be delegated.

Part 12 — Record-Keeping and Data Protection

12.1 The Agency retains originals or copies (electronic permitted) of all PMLPFTF records for at least 5 years after the end of the business relationship or the date of the transaction, whichever is later — and longer where STRO or another competent authority requires (e.g. cases under investigation or subject of an STR). Records include: all estate agency work for which CDD/UCPDD was performed; the Agency's AML/CPF/CFT checklist; the entity risk assessment; IPPC communications to RESs; compliance-check and audit records (dates, samples, findings, rectifications); all particulars forms, screening checklists, ongoing-DD checklists, authority documents (LOA/POA/resolutions), entity ownership/control documents; every supporting document; and training records (who was trained, when, how, and the schedule for those not yet trained).

12.2 RESs must submit everything to the Agency promptly upon completion of due diligence and in any case once the transaction closes. After submission, RESs must delete clients'/UCPs' identification images and documents from personal and mobile devices — the statutory record-keeping obligation sits with the Agency, and retention on personal devices creates PDPA risk.

12.3 All personal data collected for due diligence is handled under the PDPA: collected only for compliance purposes, stored securely with access limited to those who need it, and protected by the Agency's data protection policies. Consumers asking why information is required should be referred to the explanation in CEA's Consumer Guide: due diligence is a legal requirement, and without it the transaction cannot proceed.

Part 13 — Training and Competency

13.1 Every RES receives training on this Framework and on AML/CPF/CFT duties: (a) at onboarding, before handling any transaction; (b) refresher training at least annually; (c) targeted retraining after any audit finding or regulatory change; and (d) through CEA-approved CPD courses on PMLPFTF requirements, which RESs are expected to attend. Delivery may be in-person, online, written materials or hybrid.

13.2 Training covers, at minimum: the CDD/UCPDD/ECDD workflow and forms; screening sources and evidence; red flags and holistic risk judgement; the STR process, timelines and tipping-off prohibition; record-submission duties; and consequences of breach. The Agency keeps records of who has been trained, dates and type of training, and the schedule for RESs not yet trained.

Part 14 — Compliance Monitoring, Independent Audit and Breach Management

14.1 The Compliance Officer arranges compliance checks at least quarterly, sampling transactions to verify: presence and completeness of all forms and supporting ID documents; timeliness (due diligence before OTP/TA; prompt submission to the Agency; documents properly dated); performance of verification, screening, approvals and any required STR; and legibility, signatures and correct filing. Findings are recorded and signed off by the KEO.

14.2 Independent audit: the person checking a transaction must not have facilitated or been involved in it (a team leader never audits their own deals). The audit tests the effectiveness of this Framework, identifies gaps and drives remedial action. Audit frequency, samples, findings, remedial actions and timelines are documented and retained.

14.3 On discovering non-compliance the Agency will: require immediate rectification of the CDD; obtain and document the RES's explanation; file an STR if the late/absent CDD reveals undetected suspicion; issue warnings, increase supervision, require refresher training or take internal disciplinary action; and update this Framework where a systemic gap is found. The Agency will NEVER instruct or permit backdating or fabrication of documents to conceal non-compliance.

14.4 Regulatory consequences of breach (post-amendment penalty framework, on a per-breach basis): CEA letter of censure with financial penalty up to S$5,000 per breach (EA or RES); Disciplinary Committee financial penalties up to S$200,000 per breach for the Agency and S$100,000 per breach for an RES; CDSA offences for failing to file an STR or tipping off (up to S$250,000 fine and/or 3 years' imprisonment for individuals; up to S$500,000 for entities); potential offences under TSOFA/UN Act for dealing with designated persons; and loss of "fit and proper" status — a conviction for ML, PF or TF offences, in Singapore or elsewhere, disqualifies a person from holding an EA licence or RES registration.

Part 15 — Group-Wide Programme (Branches and Subsidiaries)

15.1 If the Agency has branches or subsidiaries (majority ownership above 50%), in Singapore or overseas, this Framework is implemented group-wide, including: policies and procedures for sharing CDD information, transaction-monitoring data and analyses of unusual activity within the group and with group-level compliance; adequate safeguards for confidentiality, appropriate use of shared information and prevention of tipping off; compliance with data protection laws in each jurisdiction; and centralised oversight with clear compliance reporting lines and standardised risk assessment.

15.2 Overseas branches/subsidiaries apply the STRICTER of Singapore's requirements or host-country AML/CPF/CFT law. Where the stricter standard cannot be implemented locally, the Agency reports this to CEA, applies additional risk management measures and complies with any CEA directions.

Annex A — Forms Map and Transaction Workflow

A.1 Which forms to complete (CEA forms, 30 June 2025 version — the only forms authorised for use)

Situation	Forms
Client is an individual acting for themself	A1 + B
Client (individual) acting for another individual (e.g. POA holder for owners)	A1 + A3 + B for each person
Client (individual) acting for an entity/legal arrangement	A1 + A4 + B for each person
Client is an entity/legal arrangement acting for itself (incl. company represented by staff/director)	A2 + B (entity and each BO; one Form B per person)
Client (entity) acting for an individual	A2 + A3 + B for each person
Client (entity) acting for another entity/legal arrangement	A2 + A4 + B for each person
Estate of a deceased person	A1 (executor) + A4 (beneficiaries) + B for each
Unrepresented counterparty — same logic	U1/U2 (+U3/U4 where acting for another) + U5 per person
Higher-risk situation (any Part 6 trigger)	Add Form C (client) / U6 (UCP) + Compliance Officer approval
Continuing business relationship — periodic review	Form D
HDB residential rental (whole flat / room / living quarters only)	No forms, no screening — STR duty remains

A.2 Form B/U5 mechanics: Section 1 (screening) is completed in full for EVERY person screened (client, each BO, each principal). Sections 2 (red flags) and 3 (risk conclusion) are completed once for the client/UCP; for rental transactions, purchase-specific red-flag questions are answered "No". Screening evidence (timestamped screenshots or commercial reports) is attached. If a client refuses to sign a particulars form after explanation, document the attempts and reasons and attach correspondence; for entities whose verified representative refuses to sign, record a remark to that effect.

A.3 Standard workflow for every in-scope transaction

- Step 1 — Engage: sign the estate agency agreement with the client before starting work.
- Step 2 — Identify: collect particulars and verify identity of client, BOs and any principal; establish authority where a representative acts.
- Step 3 — Screen: run TSOFA / UN / FATF / CEA-list screening and PEP checks; capture evidence.
- Step 4 — Assess: complete the red-flag checklist and record a genuine risk conclusion.
- Step 5 — Escalate if higher risk: perform ECDD (SOW/SOF) and obtain the Compliance Officer's approval before proceeding.
- Step 6 — UCPDD: once the deal is likely to proceed, complete due diligence on any unrepresented counterparty.
- Step 7 — Gate: confirm ALL due diligence is complete BEFORE the OTP is issued or the TA is signed. If it cannot be completed, do not proceed.
- Step 8 — Submit: send every form, screenshot and supporting document to the Agency; delete ID images from personal devices after submission.
- Step 9 — Report: at any point, if suspicion arises — escalate to the Compliance Officer within 24 hours and ensure an STR is filed. Never tip off.

Annex B — Red Flag Indicators (summary of CEA Annex A, 30 June 2025)

A single indicator is not conclusive; multiple unexplained indicators point to suspicion. Assess holistically against everything known about the client and transaction.

B.1 Client background

- Linked to negative news, crime reports or UN Security Council designations.
- Multiple travel documents, or documents from citizenship/residency-by-investment countries or FATF-flagged countries.
- Apparent shell company: no physical presence, nominee director controlled by a foreign shareholder or unaware of the business, refusal to disclose BOs.

B.2 Client behaviour

- Concerned about AML checks; resistant or vague when asked for BO or source-of-funds information.
- Hesitant to put their name on documents; uses different names across OTP, closing documents and deposit receipts; uses different IDs/passports for purchases.
- Buys in the name of nominees (other than spouse/child) or for persons lacking economic capacity; acts as a proxy or structures the deal to hide a BO; unexplained last-minute substitution of the purchasing party.
- Address unknown, false or a mere correspondence address/PO box.
- Debt significantly above property value; indifferent to price, location, condition or ABSD; buys without viewing, marketing materials, professional assistance, or any loan; multiple units bought in quick succession.
- Newly created entity transacting amounts large relative to its assets; business profile inconsistent with the transaction.

B.3 Transaction patterns

- Physical cash above S$20,000 for purchase, down payment or rental (cheques/cashier's orders and electronic payments are not "physical cash", but instruments that hide the true payer are a flag).
- Rent prepaid for more than 3 months without market-consistent explanation.

- Third-party payments without apparent connection (other than spouse/parent); funding from offshore banks in FATF high-risk jurisdictions; a company paying for an individual's purchase.
- Price significantly above or below market value; successive sales of the same property at unusual prices, especially between the same parties; transfers within unusually short periods.
- Unnecessarily complex legal structures with no economic logic (layered unrelated entities, offshore trusts/SPVs, cross-border arrangements).

Annex C — Key Contacts, Sources and Links

Item	Details
Compliance Officer	Adrian Goh, Key Executive Officer · adrian@sqftai.co · Phone: ______________ — first point of escalation for all suspicions, approvals and queries
STR filing	SONAR — https://www.police.gov.sg/sonar (via Agency CorpPass; RESs escalate to the Compliance Officer)
TSOFA First Schedule	https://sso.agc.gov.sg/Act/TSFA2002
UN Consolidated List	https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list
FATF black/grey lists	https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html and the high-risk and other monitored jurisdictions page
MAS sanctions alerts	https://www.mas.gov.sg/regulation/anti-money-laundering/targeted-financial-sanctions/lists-of-designated-individuals-and-entities (subscribe)
MHA IMC-TD listings	https://www.mha.gov.sg/what-we-do/managing-security-threats/countering-the-financing-of-terrorism (subscribe)
CEA PMLPFTF page	https://www.cea.gov.sg/regulatory-matters/preventing-money-laundering-proliferation-financing-and-terrorism-financing/ — Guide (30 June 2025), Forms, FAQs (29 Dec 2025), briefing slides
National Risk Assessments	ML, TF and PF NRAs and the National AML Strategy — MAS publications pages
Legislation	EAA 2010 and PMLPFTF Regulations 2021 — Singapore Statutes Online (sso.agc.gov.sg)

This Framework is based on CEA's Guide on the PMLPFTF Regulations (30 June 2025), CEA's FAQs (29 December 2025) and CEA's industry briefing (3 September 2025). The PMLPFTF Regulations and the EAA are the primary sources of the Agency's legal obligations; nothing in this Framework varies them. Where legislation or CEA guidance changes, the Compliance Officer will update this Framework and notify all RESs.

Issued by

SQFT AI is operated by GHL Resources
CEA Licence No. L3011042J
60 Paya Lebar Road, #06-28, Paya Lebar Square, Singapore 409051
sqftai.co
adrian@sqftai.co