Comparison of Changes

Guidelines for Developers on Prevention of Money Laundering, Proliferation Financing and Terrorism Financing

Version 1.3 (30 June 2025) → Version 1.4 (7 July 2026)

Prepared for internal reference — detailed section-by-section comparison

Executive Summary

Version 1.4 of the Guidelines for Developers, released 7 July 2026, is primarily a clarification and consolidation update rather than a fundamental overhaul of the ML/PF/TF prevention framework. The key changes are summarised below, with full section-by-section detail provided in the tables that follow.

- Consolidation: Targeted financial sanctions requirements (formerly standalone Section 14) have been merged into the CDD screening section (new Section 6.4), streamlining the sanctions-screening and CDD workflow into one place.
- More flexibility for developers: New allowances permit reliance on third-party regulated entities for CDD (6.2.2) and ECDD (7.3.3) at point of sale; a risk-based option to still transact with higher-risk (non-sanctioned) purchasers after ECDD (6.4.5); a 1-year exemption from repeating ongoing monitoring between TOP and completion (11.2); and no need to re-request unchanged information during enhanced ongoing monitoring (7.3.1d).
- Clarified compliance officer role: The compliance officer must now hold genuine authority and a managerial role (e.g. conducting/arranging audits, taking timely remedial action), not just a nominal title (5.1.3a).
- Risk-proportionality emphasised for SoW/SoF checks: Substantial new guidance (7.4.4) discourages a one-size-fits-all approach, excessive documentation demands, and unnecessary triangulation, especially for lower-risk or straightforward transactions.
- New definitions and clarifications: A new "International Organisation" definition was added; several sections now clarify that "resident of/originates from" refers to the relevant person's current citizenship.
- New practical tools: Annexure 3 (flow chart for CDD/ECDD checks) was added, and the red-flag indicator list reference was updated with a reminder that the list is not exhaustive.
- Notable removals: The MHA Inter-Ministry Committee on Terrorist Designation (IMC-TD) website was dropped from the screening list sources (6.4.1); the adverse-news/nationality guidance (former 6.3.8) was removed; and the "political office holder (PEP)" example was removed from the SoW/SoF corroboration examples.
- Terminology: "Sanctioned party" has been replaced with "listed in the Sanctions Lists" for consistency with the new consolidated Section 6.4.

1. Structural / Organisational Changes

The overall document structure was reorganised as follows:

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
Section numbering	Section 14 = "Additional Measures Relating to Targeted Financial Sanctions" (standalone). Sections 15–16 = New Technologies.	Old Section 14 content consolidated into new Section 6.4 "Screening and Targeted Financial Sanctions Obligations." New Technologies sections renumbered to 14–15.
Section 3.3.3	Implications of ML/PF/TF for Singapore included as unnumbered final paragraph under Section 3.3 (Terrorism Financing).	Promoted to its own subsection: 3.4 "Implications of ML, PF and TF for Singapore."
Section 6.4 / 6.5	6.4 = "Failure to Satisfactorily Perform or Complete CDD Measures."	New 6.4 = "Screening and Targeted Financial Sanctions Obligations" (absorbs old Section 14 content). Old 6.4 renumbered to 6.5.
Annexures	Annexure 1 (Risk Analysis Template), Annexure 2 (CDD Checklist).	Annexure 1 updated; Annexure 2 retained; new Annexure 3 added: "Flow Chart for CDD/ECDD Checks Prior to Property Transactions."
CDD Form titles	Form A1: "Purchaser's Particulars Form for Individuals." Form C: "Details of Beneficial Owner(s)." Form D: "Details of natural person/entity/legal arrangement on whose behalf purchaser is acting."	Form A1 retitled "...for Natural Persons." Form C retitled "...of an Entity or Legal Arrangement Purchaser." Form D title expanded/clarified: "...on whose behalf the Purchaser (who is a Natural Person) is Acting."

2. Definitions (Section 2)

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
"International Organisation"	No standalone definition (only "International organisation politically exposed person" was defined).	New definition added, describing International Organisations as entities established by formal political agreements between member States, with examples (UN, IMO, Council of Europe, EU institutions, OSCE, OAS, NATO, WTO, ASEAN, etc.).

3. Section 3 — Money Laundering, Proliferation Financing and Terrorism Financing

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
3.3.1 – What is TF	"...involves providing services, supplies and materials to support terrorist organisations..."	"...involves providing services, supplies, materials and assets to support terrorist organisations..." (broadened to include "assets").
3.3.2 – Funding sources	"...may be financed using legitimate funds (e.g. business or charity funds)..."	"...may be financed using legitimate funds (e.g. business or charitable funds/donations)..." (wording expanded).
3.4 (new) – Implications for Singapore	Content existed as 3.3.3, not separately headed.	Same substantive content, now given its own subsection heading 3.4.

4. Section 4 — Risk Analysis

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
4.2.4a – "resident of or originates from"	No clarifying footnote on what "originates from" means.	New footnote 3 added: "Refers to the relevant person's current citizenship." (Also carried through to Sections 7.2.1 and 9.3.)

5. Section 5 — Programmes and Measures / Governance

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
5.1.3a – Compliance officer	Required "appropriate compliance management arrangements, including the appointment of a compliance officer at the management level e.g. a director, Chief Executive Officer, Chief Financial Officer." No detail on authority/duties.	Expanded significantly: the compliance officer "must have the necessary authority to ensure the developer complies" with ML/PF/TF requirements, e.g. conducting/arranging independent audits on IPPC, taking timely remedial action for non-compliance. Developer must ensure the officer "plays a managerial role and is duly authorised to perform the necessary duties."
5.1.3 footnote – "Senior Management"	Footnote 4 only notes that IPPC must be approved by Senior Management (may also seek Board approval).	New, more detailed footnote 5 defines "Senior Management" as persons responsible for management/conduct of the business, with strategic decision-making authority and the highest level of executive responsibility (e.g. Director, CEO, CFO).

6. Section 6 — Customer Due Diligence (CDD)

This section saw the most extensive changes, including consolidation of the former Section 14 into new Section 6.4.

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
6.2 – New sub-clause 6.2.2	No provision allowing third-party reliance specifically at point of sale (general third-party rules only in Section 10).	New paragraph 6.2.2: developers may engage and rely on a third-party regulated entity to fulfil the CDD requirement at point of sale (6.2.1(a)–(b)), provided Section 10 requirements are met. Developers remain responsible for CDD/ECDD compliance.
6.3.1(e) – PEP determination	"...take reasonable measures to determine whether the purchaser or a natural person on whose behalf the purchaser is acting, is a politically exposed person..." (no examples given).	Same requirement, now with concrete examples of "reasonable measures": e.g. screening relevant person(s) against public sources of information such as UN website lists provided by relevant authorities or third-party commercial screening databases.
6.3.6 / 6.2.2 (v1.3) – Red-flag indicator list	Link to police.gov.sg red-flag indicators list provided, without further comment.	Link updated (new URL path) and new sentence added: "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."
6.3.6 (v1.3) – Screening sources list	Four sources: (a) MHA's Inter-Ministry Committee on Terrorist Designation (IMC-TD) website; (b) First Schedule of TSOFA; (c) UN Act Regulations (MAS website); (d) lists from Controller/other authorities.	Moved to new 6.4.1, now three sources: (a) First Schedule of TSOFA; (b) UN Act Regulations (MAS website); (c) lists from Controller/other authorities. The MHA IMC-TD website reference has been removed.
6.3.8 (v1.3) – Adverse news/nationality	Required developers to consider a relevant person's current and previous nationality/identity when assessing adverse news alerts, and not dismiss alerts based solely on current nationality; recommended adverse media searches in native languages.	This paragraph has been removed entirely; no equivalent provision appears in v1.4.
6.4 (new) – Targeted financial	Sanctions screening obligations were split between old 6.3.6–6.3.9 (screening + STR filing on positive	Consolidated into new Section 6.4: 6.4.1 (screening lists, now called "Sanctions Lists"), 6.4.2 (MAS

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
sanctions obligations	hits) and old Section 14 (pre-OTP/S&PA sanctions assessment).	subscription), 6.4.3 (pre-OTP/S&PA sanctions assessment, merged from old Section 14.1), 6.4.4 (actions on positive hit, merged from old 6.3.9/14.2).
6.4.5 (new) – Risk-based approach for higher-risk, non-sanctioned purchasers	No equivalent; higher-risk purchasers were addressed only through ECDD obligations (Section 7) with no explicit statement that developers could still choose to transact after ECDD.	New paragraph: except for persons on the Sanctions Lists (with whom transacting is prohibited), developers may take a risk-based approach and decide whether to transact with a higher ML/PF/TF-risk purchaser after performing ECDD checks; an STR should be filed if there is suspicion of illicit activity or funds.
6.5 (was 6.4) – Failure to complete CDD	6.4.1(a)–(b): "suspect... and believe..." (conjunctive "and"). 6.4.2(a)-(b): general inability to obtain/verify "any information required."	6.5.1(a)–(b): changed to "and/or." 6.5.2(a) narrowed to focus specifically on the purchaser's identity information; 6.5.2(b) adds an example: "e.g. explanations provided is inconsistent or not reasonable."
6.5.4 (new)	No equivalent cross-reference.	New paragraph directing developers to the new Annexure 3 flow chart and an accompanying table of example scenarios and required follow-up actions.

6a. Former Section 14 — Now Merged into Section 6.4

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
Old Section 14 – Additional Measures Relating to Targeted Financial Sanctions	Standalone Section 14 (14.1–14.2): pre-OTP/S&PA assessment of whether relevant person is a terrorist/designated person/notified risk person; if suspected, must not grant OTP/accept money/enter S&PA and must file an STR.	Removed as a standalone section; its substance is merged into new Section 6.4 ("Screening and Targeted Financial Sanctions Obligations"), specifically sub-paragraphs 6.4.3 and 6.4.4.

7. Section 7 — Enhanced Customer Due Diligence (ECDD)

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
7.2.1 – When to perform ECDD	Split into two paragraphs: (a) relevant person is foreign PEP/family/close associate, resident of relevant country, or notified higher-risk person; (b) developers separately assess (under 4.2) that the relevant person, including domestic/international-organisation PEPs, may present higher risk.	Restructured into a single unified list (i)–(iv), folding the former separate paragraph (b) into item (iv): "assessed to present a higher risk of ML, PF or TF under paragraph 4.2.4."
7.2.2 (new)	No equivalent clarifying statement.	New paragraph explicitly clarifying that for the vast majority of purchasers, including domestic PEPs not assessed as higher risk, developers need only conduct standard CDD checks (6.3), not ECDD.
7.3.1(d) – Enhanced ongoing monitoring	Required enhanced ongoing monitoring of transactions to identify suspicious transactions/patterns inconsistent with the purchaser's profile.	Same requirement, plus new sentence: "Where information has been previously provided and remains unchanged, developers are not required to request for the same information again."
7.3.2 (new)	No equivalent.	New paragraph cross-referencing 6.5.1–6.5.3: if a developer cannot complete ECDD or believes it would tip off the purchaser, it should follow those requirements/restrictions.
7.3.3 (new) – Third-party reliance for ECDD	No provision permitting third-party reliance specifically for pre-OTP ECDD checks.	New paragraph allowing developers to engage and rely on a third-party regulated entity for required ECDD checks before issuing an OTP or accepting money, subject to Section 10 requirements; developer remains responsible for compliance.
7.3.2(c) (v1.3) / 7.4.3–7.4.4 (v1.4) – SoW/SoF corroboration approach	Required corroboration against documentary evidence/public sources; additional triangulation checks against a few sources for robustness (with a detailed Middle East senior-banker example); exercise reasonable judgment on which documents are critical.	Retains corroboration and reasonable-judgment requirements (7.4.3) but removes the detailed Middle East example. Adds an entirely new paragraph 7.4.4 setting out risk-proportionate principles (relevance, materiality, prudence): obtain only relevant/pertinent information; avoid excessive or disproportionate requests; no need for triangulation if source is already reliable/public; no need to

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
		corroborate every piece of SoW, especially very old information; lighter checks for straightforward, market-rate single-property purchases.
7.3.3(e) (v1.3) – SoW examples: PEP	Included example (e): "Being a political office holder over the years (e.g. a PEP): Reliable public information showing the individual's political position..."	This example has been removed from the SoW/SoF corroboration examples list (7.4.5 in v1.4 covers (a)–(d) only: salaries/savings, gift/inheritance/windfall, business profits, investment gains).
7.3.4 (v1.3) – Consequence of unverifiable SoW/SoF	Standalone paragraph: where legitimacy of SoW/SoF cannot be reasonably ascertained, developers should not grant OTP/accept money, not enter into new S&PA for sub-sales, and determine whether to lodge an STR.	Removed as a standalone paragraph; equivalent effect is instead achieved through the new 7.3.2 cross-reference to Section 6.5.

8. Section 8 — Simplified Customer Due Diligence (SCDD)

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
Section 8 – SCDD	When to perform, requirements, and how to perform SCDD.	No substantive changes; content and requirements are the same.

9. Section 9 — CDD on Existing Purchasers

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
9.3 – "originated from"	No clarifying footnote.	New footnote added: "Refers to the relevant person's current citizenship."

10. Section 10 — Performance of CDD Measures by Third Parties

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
Section 10 – Third-party CDD performance	Sets out conditions for relying on third parties to perform CDD.	No substantive changes to the conditions themselves; this section is now explicitly cross-referenced by the new 6.2.2 and 7.3.3 provisions permitting third-party reliance at point of sale and for ECDD.

11. Section 11 — Ongoing Monitoring of Transactions

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
11.1 – Ongoing monitoring before TOP/completion	Required review of adequacy of CDD/ECDD/SCDD information before issuing notice of payment for TOP and for completion of sale.	Same requirement retained.
11.2 (new) – 1-year exemption	No equivalent; ongoing monitoring appears required at both TOP and completion stages regardless of timing.	New paragraph: if completion of sale occurs within 1 year of the last review conducted prior to the TOP payment notice, ongoing monitoring need not be repeated, provided there is no change to the developer's knowledge or risk profile of the purchaser.

12. Section 12 — Reporting of Suspicious Transactions

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
12.1.1 – STR filing standard	"If there are suspicions that ML/PF/TF activities are committed, developers are required to file a STR..."	Reworded to add an explicit timeliness standard: "...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."
12.1.2 – Referral / terminology	"...within 15 business days of the case being referred by the developer's staff..." Uses the term "sanctioned party" (defined in footnote 8) for expedited 1-business-day filing.	Clarifies referral is "...referred by the developer's staff to the management..." Replaces "sanctioned party" terminology with "listed in the Sanctions Lists."

13. Section 13 — Record Keeping

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
Section 13 – Record Keeping	5-year retention of OTP, S&PA, Form 3, prescribed CDD notification form, and CDD/ECDD/SCDD records.	No substantive changes.

14. New Technologies (Renumbered Sections 14–15)

Section	Version 1.3 (30 Jun 2025)	Version 1.4 (7 Jul 2026)
New Technologies (old 15–16, now 14–15)	Sections 15 (Identifying Risks) and 16 (Managing and Mitigating Risks) from New Technologies.	Renumbered to Sections 14 and 15 respectively (to accommodate removal of the old standalone Section 14). No substantive wording changes.

Notes

This comparison is based on a paragraph-by-paragraph review of Guidelines for Developers Version 1.3 (30 June 2025) and Version 1.4 (7 July 2026). Where wording is substantively identical but renumbered, this is noted as "no substantive changes." Developers should refer to the full text of Version 1.4 for the complete and authoritative wording of all requirements.