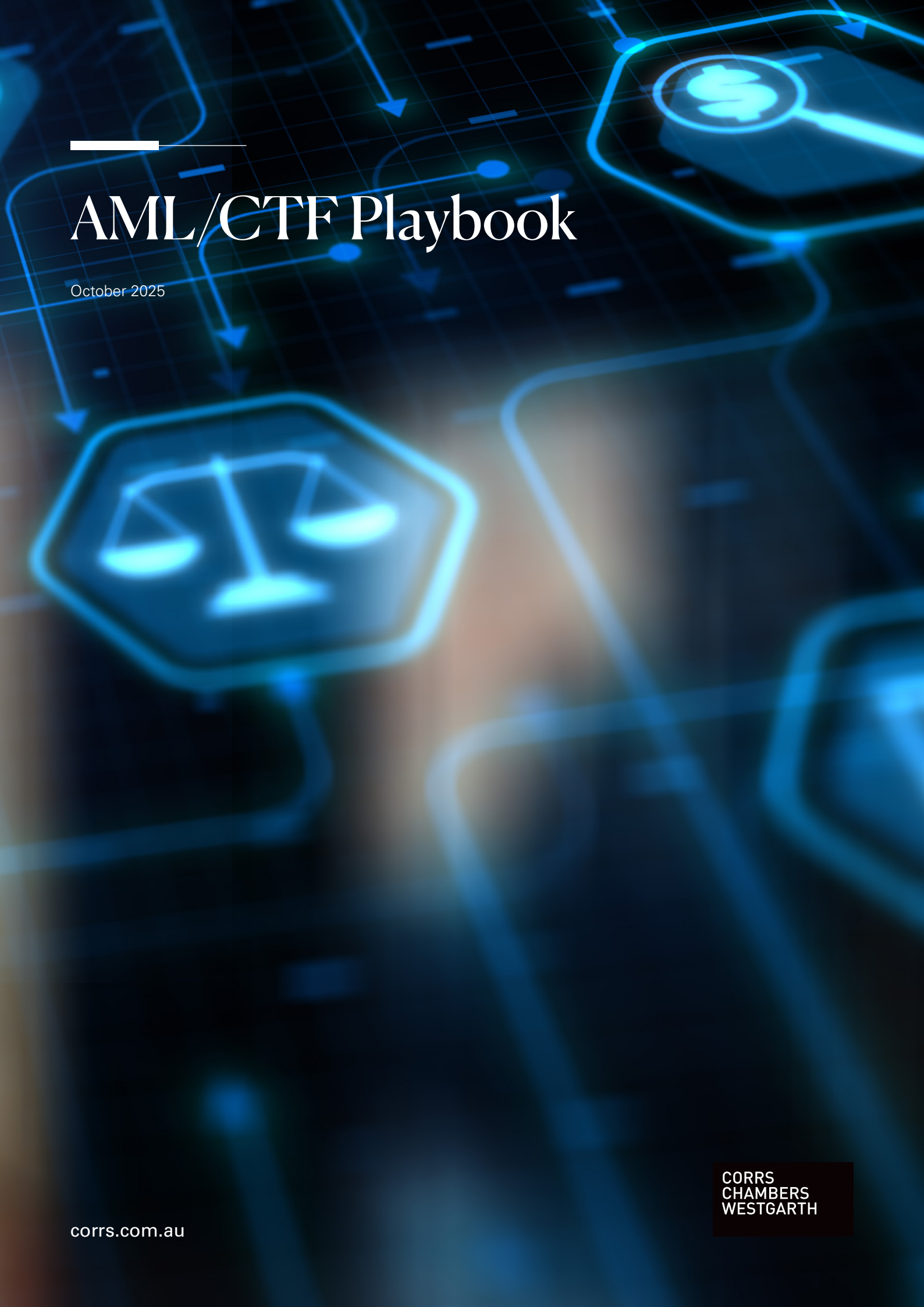


AML/CTF Playbook

October 2025

CORRS
CHAMBERS
WESTGARTH

corrs.com.au

Contents

Introduction

The *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024* (**Amended AML/CTF Act**) introduces the most significant changes to Australia's anti-money laundering (**AML**) and counter-terrorism financing (**CTF**) framework since the original Act was introduced in 2006 (*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act 2006**)). These reforms aim to simplify, modernise, and expand the regulatory framework to cover real estate professionals and developers, professional services providers (such as lawyers, accountants, insolvency and restructuring practitioners, consultants), and dealers in precious metals and stones (**Tranche 2 Entities**).

The Amended AML/CTF Act has also strengthened AUSTRAC's powers to monitor, investigate, and enforce compliance with the AML/CTF regime. Enhancements to AUSTRAC's information and examination powers came into effect on 7 January 2025.

For existing reporting entities, most changes will take effect on 31 March 2026, while changes for Tranche 2 entities will be implemented on 1 July 2026. These amendments aim to align Australia's AML/CTF framework with international standards, particularly those set by the Financial Action Task Force (**FATF**).

The reforms are supported by an updated set of AML/CTF rules: The *Anti-Money Laundering and Counter Terrorism Financing Rules 2025* (**AML/CTF Rules 2025**) which were published on 29 August 2025 and provide further details on the new requirements.

This Playbook is designed to support reporting entities in understanding the key changes required for compliance and in navigating the upcoming reforms effectively. It outlines both immediate and long-term considerations to help ensure a smooth transition. Each chapter highlights the key changes, compares the current and future regimes, and offers actionable steps to guide your organisation towards compliance by March 2026. While not a comprehensive step-by-step guide, this Playbook serves as a practical tool to assess the potential impact on your organisation and help you stay ahead of the new requirements as they come into effect.

All references to the Amended AML/CTF Act are based on the latest *Future Law Compilation of the Anti-Money Laundering and Counter Terrorism Financing Act 2006*, which incorporates the amendments introduced by the Amended AML/CTF Act, as published by AUSTRAC.[1]

1 Future Law Compilation of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), available here.

Cheat Sheet – Key changes under the Australian AML/CTF reforms

01 ML/TF/PF Risk Assessments

The Amended AML/CTF Act introduces an explicit requirement to undertake a money-laundering, terrorism financing and proliferation financing (ML/TF/PF) risk assessment, and reporting entities will need to identify the level of money laundering, terrorism financing and proliferation financing risk faced by the business, taking into account:

- the nature, size and complexity of their business; and
- any relevant risks identified and communicated by AUSTRAC.

This will mean that reporting entities will need to create and adopt a new procedure to conduct tailored risk assessments. For current reporting entities, these provisions will come into effect on 31 March 2026.

02 AML/CTF programs

The Amended AML/CTF Act revises the structure of AML/CTF programs and requires programs to consist of two main components:

- the reporting entity's ML/TF/PF risk assessment; and
- its AML/CTF policies (including the AML/CTF program).

This will mean that reporting entities will need to create and adopt a new AML/CTF program that contains most of its underlying AML/CTF procedures.

At a high level, AML/CTF programs must be:

- in place prior to the provision of any designated service;
- documented in writing and approved by a senior manager;
- tailored to the nature, size and complexity of the reporting entity's business; and
- reviewed and updated regularly, including in response to adverse findings or material changes in risk.

The AML/CTF policies must address how the reporting entity identifies, assesses, manages and mitigates ML/TF/PF risks, and ensure compliance with all legislative obligations. They must also include key governance, due diligence, training, record-keeping and independent evaluation arrangements, including how the governing body remains informed of relevant risks.

For existing reporting entities, these provisions will come into effect on 31 March 2026.

03 Board oversight

The Amended AML/CTF Act removes the requirement for the Board to approve the AML/CTF program. However, the Board will still need to ensure that it:

- exercises appropriate ongoing oversight of the ML/TF/PF risk assessment and the entity's compliance with AML/CTF legislation; and
- has taken reasonable steps to ensure that the entity is appropriately identifying, assessing and managing its ML/TF/PF risks and complying with its AML/CTF policies.

These provisions will come into effect on 31 March 2026.

04 Appointment of a 'Senior Manager'

The Amended AML/CTF Act introduces a requirement to appoint a 'senior manager' who will be responsible for approving any changes to the ML/TF/PF risk assessment and the AML/CTF policies.

For existing reporting entities, a senior manager needs to be appointed by 31 March 2026.

05 AML/CTF Compliance Officer

The Amended AML/CTF Act contains additional requirements that the AML/CTF Compliance Officer must be resident in Australia if the reporting entity is providing the services through a permanent establishment in Australia, and:

- employed or otherwise engaged by the reporting entity at management level; and
- a 'fit and proper' person with sufficient authority, independence and access to information and resources.

Reporting entities will need to document how the AML/CTF Compliance Officer meets these requirements. These provisions will come into effect for existing reporting entities on 31 March 2026.

06 Customer due diligence

The Amended AML/CTF Act introduces reforms to customer due diligence requirements, and requires reporting entities to risk rate their customers before undertaking customer due diligence. The risk rating will then determine the level of due diligence required for the customer.

The Amended AML/CTF Act also introduces a requirement to screen customers against sanctions lists at the outset of the customer relationship.

These provisions will come into effect for existing reporting entities on 31 March 2026.

07 Tipping off provisions

The Amended AML/CTF Act makes amendments to the existing 'tipping off' offence to allow for greater information sharing with third parties, except where the disclosure of SMR material would or could reasonably be expected to prejudice a law enforcement investigation.

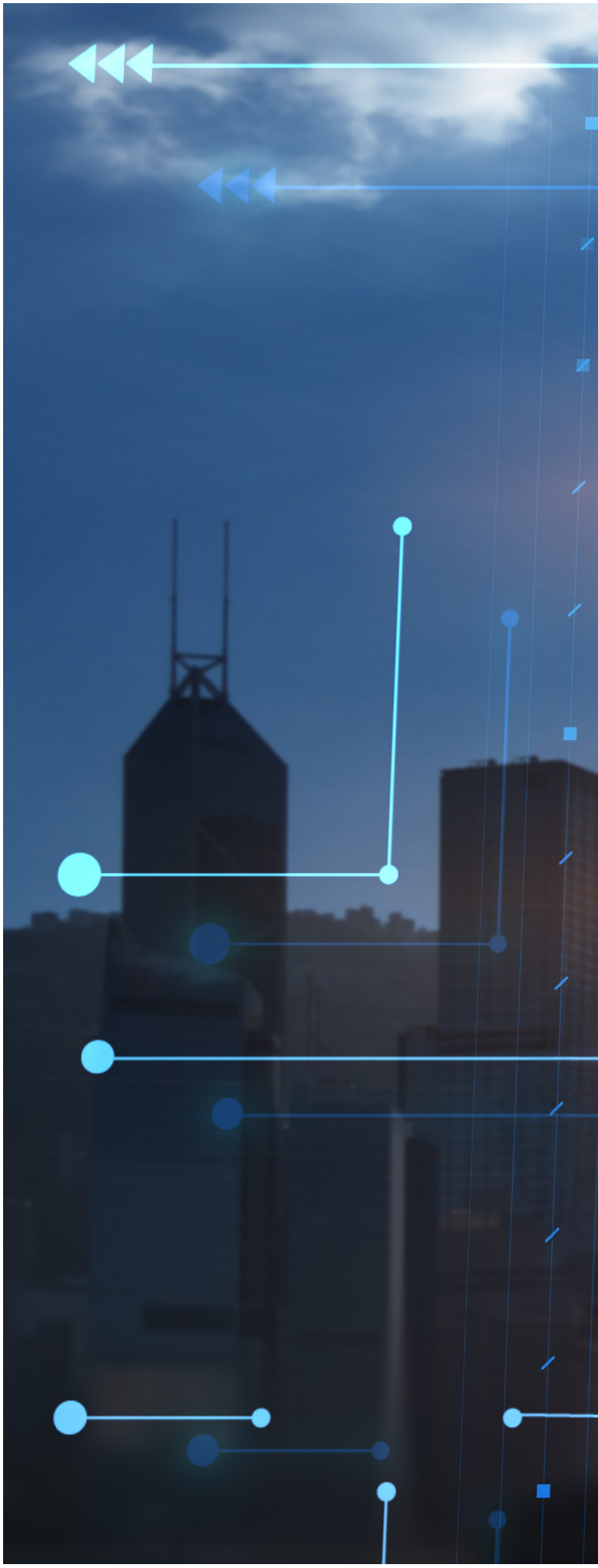
These provisions are effective as of 31 March 2025.

08 IFTIs regime

The Amended AML/CTF Act replaces the regimes relating to the international funds transfer instructions (IFTI) and designated remittance arrangements with the concept of 'transfers of value' and 'international value transfer services' (IVTS). It also amends the reporting requirements, and requires more information to be reported through the value transfer chain.

These provisions will come into effect on 31 March 2026, but transitional arrangements will be agreed post-2026 for IVTS reporting requirements.

The changes to that regime are largely contained in the AML/CTF Rules 2025. The reporting requirements will be set out in transitional rules to be drafted post-2026, which will be subject to consultation.



01

AML/CTF Programs – Risk assessment and policies

Snapshot of the reforms

- Under the current AML/CTF regime, reporting entities must maintain an AML/CTF program, divided into Part A and Part B, outlining measures employed by the reporting entity to ensure compliance with the AML/CTF legislation. The Amended AML/CTF Act significantly recasts reporting entities' obligations in respect of AML/CTF programs and establishes a new concept of 'AML/CTF policies'. This will contain a broader set of the reporting entity's AML/CTF procedures and its ML/TF/PF risk assessment.
- When conducting their risk assessment, in addition to ML/TF risks, reporting entities will need to assess any proliferation financing risks that they may reasonably face in the provision of a designated service.
- Reporting entities are free to maintain the current division of programs into Part A and Part B and are permitted to organise the documentation of their AML/CTF program as they see fit, provided that the policies comply with the obligations set out in the Amended AML/CTF Act.
- The reforms maintain the civil penalty provisions for non-compliance with the AML/CTF Program. However, under the Amended AML/CTF Act, non-compliance with any of the reporting entity's AML/CTF policies will constitute a civil penalty offence, being the broader set of AML/CTF procedures. As such, it is important that businesses carefully consider the content and scope of their AML/CTF policies.

Summary of the key changes

Format of AML/CTF programs	
Current regime	**Change**
Under the current regime, AML/CTF programs must be set out in writing and demonstrate how a reporting entity identifies, mitigates and manages the ML/TF risks that it may reasonably face.[2] AML/CTF programs are generally comprised of two parts:[3] • Part A must set out any processes or procedures adopted by the reporting entity to identify, mitigate and manage ML/TF risks that it may reasonably face.[4] • Part B sets out the procedures for identifying customers and beneficial owners and verifying their identity.[5]	Under the reforms, AML/CTF programs will no longer need to be split into Parts A and B. Reporting entities will be given greater flexibility in how they prepare their policy documents to identify and address ML/TF/PF risks. However, the contents of the AML/CTF policies will need to be more detailed and include 'the policies, procedures, systems and controls of the reporting entity to manage and mitigate ML/TF risk (see below).[6] Reporting entities will be required to document both the ML/TF/PF risk assessment and AML/CTF policies prior to first providing a designated service and must document any updates within 14 days of their occurrence.[7]

2 AML/CTF Act 2006 ss 84(1)-(2).
3 Ibid s 84(1)(b).
4 Ibid s 84(2).
5 Ibid s 84(3).
6 Amended AML/CTF Act s 5, definition of 'AML/CTF policies'.
7 AML/CTF Rules 2025 ss 5-15(1)-(2).

Risk assessments	
Current regime	**Change**
The AML/CTF Act does not explicitly require reporting entities to conduct a risk assessment before providing a designated service. Reporting entities are expected to infer this requirement from the legislation. AUSTRAC has also made this expectation clear in recent civil penalty proceedings.[8] While Part 7 of the AML/CTF Act and the accompanying *Anti Money Laundering and Counter Terrorism Financing Rules Instrument 2007 (No. 1)* (**Old AML/CTF Rules**) mandate a risk-based approach to guide the development of an appropriate AML/CTF program, the Act does not specify the methodology for conducting the ML/TF risk assessment.	The Amended AML/CTF Act requires reporting entities to identify and assess the ML/TF/PF risks that they may reasonably expect to face in providing designated services to customers. This risk assessment must be conducted prior to providing such services and should inform the development of policies, procedures, systems, and controls within the entity's AML/CTF program to mitigate those risks.[9] The Amended AML/CTF Act requires a reporting entity's ML/TF/PF risk assessment to: • consider the nature, size and complexity of its business in determining the level of risk;[10] and • incorporate relevant risks identified by AUSTRAC.[11] In conducting their risk assessments, reporting entities must evaluate factors such as the types of customers, designated services offered, delivery channels, and operating jurisdictions, as well as any information communicated by AUSTRAC that identifies risks faced by the entity.[12] Reporting entities will need to review and update their ML/TF/PF risk assessments when there is a significant change to their business' risk profile, when AUSTRAC communicates a specific risk, or at least once every 3 years.[13]

Proliferation financing	
Current regime	**Change**
There is currently no explicit requirement to consider risks of proliferation financing.	As part of the risk assessment, reporting entities must consider the risk of facilitating proliferation financing through their operations when providing designated services.[14] Reporting entities are not required to develop or maintain policies and systems for proliferation financing if they reasonably assess that the associated risk is low and adequately managed.[15]

8 AUSTRAC initiated civil penalty proceedings against Crown Melbourne and Crown Perth for alleged breaches of the AML/CTF Act, which alleged that Crown did not include a risk assessment methodology.

9 Amended AML/CTF Act s 26D.

10 Ibid s 26C(2).

11 Ibid s 26D(1)(a)(ii).

12 Ibid s 26C(3).

13 Ibid s 26D(1).

14 Proliferation financing refers to the act of providing funds for the manufacture, acquisition, or use of nuclear, chemical or biological weapons. Under the Amended AML/CTF Act, it is defined to include relevant offences set out in the *Charter of the United Nations Act 1945*, the *Autonomous Sanctions Act 2011* (Cth), Commonwealth, state, and territory statutes, and any foreign laws relating to sanctions offence, and proliferation financing: Amended AML/CTF Act s 5.

15 Amended AML/CTF Act s 26F(11).

Policy contents/ Risk mitigation measures	
Current regime	**Change**
Reporting entities must develop and maintain an AML/CTF program containing systems and controls that are designed to mitigate and manage risks that it has identified.[16]	The Amended AML/CTF Act requires reporting entities to develop, implement and maintain policies, procedures, systems and controls that are adapted to the size, nature and type of the business and appropriately and effectively manage and mitigate the ML/TF/PF risks the entity may face (**AML/CTF policies**).[17] This is intended to replace the current 'check-box' approach to compliance. Whilst the Amended AML/CTF Act does not prescribe any specific measures to mitigate risks, it does set out a non-exhaustive list of the matters that must be covered by the AML/CTF policies, which is supplemented by matters required by the AML/CTF Rules 2025. AML/CTF policies must (among other things): • appropriately manage and mitigate the risks of money laundering, financing of terrorism and proliferation financing that the reporting entity may reasonably face;[18] • ensure that the reporting entity complies with AML/CTF legislation;[19] • be appropriate to the nature, size and complexity of the reporting entity's business;[20] • identify significant changes to the kinds of designated services provided, the reporting entity's customers and delivery channels, and the countries with which the reporting entity deals or will deal, and information communicated by AUSTRAC;[21] • outline customer due diligence processes;[22] • outline the procedure to review and update the policy where new risks arise;[23] • deal with ensuring no assets are made available to sanctioned individuals;[24] • outline when senior manager approval is required in accordance with the AML/CTF Rules 2025;[25] • set out procedures to review the AML/CTF policies at least every 3 years;[26] • deal with establishing safeguards to prevent tipping off;[27] • deal with the provision of information to the governing body[28] and reporting from the AML/CTF compliance officer to the governing body;[29] • require the reporting entity to assess specified matters in relation to personnel due diligence;[30] • deal with ensuring AUSTRAC reporting is correct and accurate;[31] • deal with the timely review and reporting of SMRs;[32] • deal with personnel training;[33]

16 AML/CTF Act 2006 s 80.
17 Amended AML/CTF Act s 26F.
18 Ibid s 26F(1)(a).
19 Ibid s 26F(1)(b).
20 Ibid s 26F(1)(c).
21 Ibid s 26F(3)(a).
22 Ibid s 26F(3)(b).
23 Ibid s 26F(3)(c).
24 AML/CTF Rules 2025 s 5-3.
25 Ibid s 5-5.
26 Amended AML/CTF Act s 26F(3)(d).
27 AML/CTF Rules 2025 s 5-13.
28 Ibid s 5-6.
29 Ibid s 5-7.
30 Ibid s 5-8.
31 Ibid s 5-11.
32 Ibid s 5-12.
33 Ibid s 5-9.

Policy contents/ Risk mitigation measures (continued)	
Current regime	**Change**
	• require the reporting entity to conduct an independent evaluation of, among other things, its risk assessment, the design of its AML/CTF policies, and general compliance[34] and update its AML/CTF policies in response to any adverse findings;[35] • address key governance and operational requirements, including:[36] – ensuring the governing body is sufficiently informed of the entity's ML/TF/PF risks; – designating an AML/CTF compliance officer and senior manager responsible for approving AML/CTF policies and risk assessments; – conducting employee due diligence and providing targeted training to employees engaged in AML/CTF functions; and – scheduling independent evaluations of the AML/CTF program, at intervals appropriate to the entity's nature, size and complexity, but no less than once every 3 years. For 'lead entities' of 'reporting groups', AML/CTF policies must also:[37] • facilitate appropriate and confidential sharing of information between group members to enable effective customer due diligence and risk management; • clearly allocate responsibility for discharging AML/CTF obligations among group members, including maintaining access to records evidencing compliance; • ensure compliance with relevant legislative requirements and the 'lead entity's' AML/CTF policies across the group; and • ensure confidentiality and appropriate use of any information shared and preventing 'tipping off' risks. 'Lead entities' (see Chapter '*Reformed Governance Requirements*') will also need to consider and establish procedures within their AML/CTF policies to share risk management information between members of the 'reporting group'.[38]

Independent review of AML/CTF Program	
Current regime	**Change**
Reporting entities must regularly monitor the effectiveness of their controls in managing ML/TF risks and present the findings to the Board.[39]	Reporting entities must independently review their AML/CTF policies at least every 3 years.[40] The AML/CTF policies of a reporting entity must incorporate procedures for conducting independent evaluations that cover risk assessment, policy design, and operational compliance, and require written reports to be provided to the governing body and relevant senior managers.[41] They must also specify how the reporting entity will respond to findings in an independent evaluation report,[42] and provide for the review of the ML/TF risk assessment if an independent evaluation report contains adverse findings, with the review to occur as soon as practicable after receipt of the report by the governing body.[43]

34 Ibid s 5-10.
35 Ibid s 5-4.
36 Amended AML/CTF Act s 26F(4)(f).
37 Ibid ss 26F(5)-(6).
38 Ibid s 26F(5)(a).
39 Old AML/CTF Rules Parts 8.6 and 9.6.
40 Amended AML/CTF Act s 26F(3)(d).
41 AML/CTF Rules 2025 s 5-10(1)-(2).
42 Ibid s 5-10(3).
43 Ibid ss 5-1(1)-(2).

Penalties	
Current regime	**Change**
Under the current regime, a failure to have an AML/CTF program, and non-compliance with an AML/CTF program constitute contraventions of a civil penalty provision.[44]	Under the Amended AML/CTF Act, the following actions constitute a breach of a civil penalty provision: • the provision of a designated service without having undertaken a risk assessment (in respect of each designated service that the reporting entity provides to a customer) and reviewing the risk assessment at least once every three years;[45] • a failure to develop and maintain AML/CTF policies (in respect of each designated service that the reporting entity provides to a customer);[46] and • a failure to comply with a reporting entity's own AML/CTF policies.[47] The maximum civil penalty is 100,000 penalty units for a corporation[48] and 20,000 penalty units for individuals.[49]

Matters for reporting entities to consider

Immediate priorities

- Undertake a careful review of the new ML/TF/PF risk assessment and AML/CTF Program requirements and identify what might need to change to comply with the Amended AML/CTF Act.
- Consider what needs to be included in the AML/CTF policies and understand the extent of AML/CTF policy documentation.

By 31 March 2026

- Update the ML/TF/PF risk assessment and include it within your AML/CTF policies.
- Update your AML/CTF Policies to require an independent evaluation of them every three years.
- Based on the above assessments and reviews (see "Immediate Priorities"), develop, amend or update the entity's AML/CTF program, including its AML/CTF policies and its ML/TF risk assessment, as necessary to comply with the new requirements set out above.

44 AML/CTF Act 2006 ss 81(2) and 82(2).
45 Amended AML/CTF Act s 26E.
46 Ibid s 26F(8)(g).
47 Ibid s 26G.
48 Ibid s 175(4).
49 Ibid s 175(5).

02

Reformed governance requirements

Snapshot of the reforms

- The Amended AML/CTF Act replaces the concept of 'designated business group' with a new 'reporting group' framework, which both reporting and non-reporting entities can be part of. Reporting entities will be required to designate a 'lead entity' to exercise ongoing AML/CTF oversight across the 'reporting group', taking reasonable steps to ensure the 'reporting group' is adequately identifying ML/TF/PF risks and complying with AML/CTF obligations.
- Under the new framework, 'lead entities' will have greater responsibility and therefore greater exposure, particularly in terms of group-wide oversight and risk management.
- As with the current position, a reporting entity's board or equivalent senior management will be required to:
  - exercise ongoing oversight of the ML/TF risk assessment and compliance with the reporting entity's AML/CTF policies and AML/CTF laws; and
  - take reasonable steps to ensure that a reporting entity is appropriately identifying relevant ML/TF/PF risks and complying with the AML/CTF policies and laws.

However, a reporting entity's board will no longer be required to approve the AML/CTF policies.

- Reporting entities must appoint a 'senior manager' responsible for approving the ML/TF risk assessment and AML/CTF policies, as well as for notifying the Board of any updates to the risk assessment.
- As is currently required, an AML/CTF compliance officer must be appointed.
- The AML/CTF compliance officer must be employed or otherwise engaged at management level and have sufficient authority, independence and access to resources and information. The officer must now also be a 'fit and proper' person and resident in Australia (if the reporting entity provides designated services through a permanent establishment in Australia).

Summary of the key changes

Approval of the ML/TF risk assessment and AML/CTF policies	
Current regime	**Change**
Under the current regime, the Board and senior management is responsible for approving Part A of the reporting entity's AML/CTF program.[50] The board and senior management must also provide ongoing oversight over Part A of the AML/CTF program.[51]	The Board or equivalent governing body will no longer be required to approve the AML/CTF policies. Instead, a senior manager of the reporting entity must approve the ML/TF/PF risk assessment and the AML/CTF policies, and any subsequent updates or amendments.[52] A 'senior manager' is defined as an individual who makes or participates in making decisions about the whole or substantial parts of a reporting entity's business.[53] At least in larger entities, this role is distinct from the governing body responsible for strategic decisions.[54] The Amended AML/CTF Act requires that copies of the reporting entity's ML/TF risk assessment be provided to the reporting entity's governing body, and that any changes to it be notified to the Board.[55]

Board oversight	
Current regime	**Change**
The Board is responsible for the effective implementation and ongoing oversight of the operation of the AML/CTF program.[56] The Board must ensure that the program undergoes periodic independent reviews and that it remains informed of key ML/TF risks and issues as they arise.[57] Boards must also be comfortable that the level of AML/CTF reporting and escalation is adequate, so that they can discharge their ongoing oversight obligation.	The Board or equivalent governing body will need to ensure that it: • exercises appropriate ongoing oversight of the ML/TF risk assessment and the entity's compliance with AML/CTF legislation;[58] and • has taken reasonable steps to ensure that the entity is appropriately identifying, assessing and managing its ML/TF risks and complying with its AML/CTF policies.[59] AUSTRAC has issued guidance on board and senior management responsibilities, emphasising the importance of good governance and adequate oversight of AML/CTF matters.[60] AUSTRAC expects boards and senior management to have consistent access to coordinated, structured and quality information on a consistent basis, not limited to specific events or incidents. This is likely to continue to apply.

50 Old AML/CTF Rules Part 8.4.1 and Part 9.4.1.
51 Ibid Parts 8.4.1 and 9.4.1.
52 Amended AML/CTF Act s 26P(1).
53 Ibid s 5.
54 *Explanatory Memorandum for the Anti-Money Laundering and Counter-Terrorism Financing Amendment Bill 2024*, para 37; see also para 131 which indicates that the distinction between governing body, senior manager and AML/CTF compliance officer may be redundant for small businesses or sole traders.
55 Amended AML/CTF Act s 26P(2).
56 Old AML/CTF Rules Parts 8.4.1 and 9.4.
57 Ibid Parts 8.6 and 9.6.
58 Amended AML/CTF Act s 26H(1)(a).
59 Ibid s 26H(1)(b).
60 AUSTRAC Regulatory Quick Guide, 'Governance: board and senior management oversight', available here.

AML/CTF Officer	
Current regime	**Change**
Reporting entities must designate an AML/CTF compliance officer at management level.[61] The reporting entity must notify AUSTRAC of the details of the AML/CTF compliance officer[62] upon enrolment of the reporting entity and within 14 days of any change.[63]	The requirement to designate an AML/CTF compliance officer and notify AUSTRAC remain in place.[64] Additionally, the AML/CTF compliance officer must be a fit and proper person, employed or otherwise engaged by the reporting entity at management level,[65] with adequate resources, authority and independence to perform their functions effectively.[66] Factors influencing whether a person is fit and proper include assessment of their character, their qualifications, conflicts of interest, and relevant regulatory or criminal history.[67] The AML/CTF compliance officer is responsible for overseeing and coordinating the operational implementation of the AML/CTF program.[68] If the designated services are provided through a permanent establishment in Australia, the AML/CTF compliance officer must be resident in Australia.[69] A reporting entity must notify AUSTRAC of the details of the AML/CTF compliance officer within 14 days after the person is designated as the AML/CTF compliance officer.[70]

Designated Business Groups	
Current regime	**Change**
A Designated Business Group (DBG) is a group of two or more reporting entities who join together to share the administration of some or all of their AML/CTF obligations.[71] A member of the DBG must meet certain criteria (such as being a related body corporate), be a reporting entity and have nominated to form a DBG.[72] The AML/CTF program may be approved and overseen by the main holding company of the group where each member of the DBG is related to the other members.[73]	The current concept of a DBG will be replaced by a new concept of a 'reporting group', comprising a 'lead entity' and the 'reporting group' members.[74] A 'lead entity' does not need to provide designated services,[75] but a 'reporting group' is required to have a 'lead entity'.[76] 'Reporting groups' may be formed by default[77] (eg for business groups) or by election[78] (eg for entities meeting certain criteria). It is the 'lead entity's' governing body that will be required to maintain oversight across the 'reporting group' and have AML/CTF Policies to ensure appropriate sharing of information between members of the 'reporting group' to adequately identify, assess, manage and mitigate their ML/TF/PF risks and otherwise comply with their AML/CTF obligations.[79] It is permissible for non-reporting entities in a 'reporting group' to discharge AML/CTF Act obligations, but that entity must meet training and due diligence standards aligned with the group's AML/CTF policies.[80]

61 Old AML/CTF Rules Parts 8.5.1 and 9.5.1.
62 Ibid Chapter 63 Part A 23.
63 AML/CTF Act 2006 s 51F.
64 Amended AML/CTF Act ss 26J(1) and 26M(1).
65 Ibid s 26J(2)(a).
66 bid s 26J(2)(b).
67 AML/CTF Rules 2025 ss 5-14(1)(a)-(g).
68 Amended AML/CTF Act s 26L(a).
69 Ibid s 26J(3)(a).
70 Ibid s 26M(1).
71 AML/CTF Act 2006 s 5.
72 Old AML/CTF Rules Part 2.1.2(4).
73 Ibid Part 9.4.2.
74 Amended AML/CTF Act s 10A.
75 Ibid s 236B(2).
76 AML/CTF Rules 2025 s 2-3.
77 Amended AML/CTF Act s 10A(1)(a).
78 Ibid s 10A(2).
79 Ibid s 26F(5)-(6).
80 AML/CTF Rules 2025 s 2-4.

Designated Business Groups (continued)	
Current regime	**Change**
	Designated services provided by a reporting entity member of a 'reporting group' are taken to have been provided by the 'lead entity'.[81] If a reporting entity member of a group fails to comply with an obligation under the AML/CTF Act, both the contravening member and the 'lead entity' will be liable for the contravention. For 'reporting groups', group-level compliance management is required, with provisions for the sharing of ML/TF risk-related and AML/CTF compliance-related information, subject to appropriate safeguards to protect the information. These matters must be covered in the reporting group's AML/CTF policies.[82] The AML/CTF Rules 2025 specify how the 'lead entity' of a 'reporting group' is identified.[83] Compared to the previous regime, the amended AML/CTF regime gives greater flexibility for members of a 'reporting group' to agree in writing[84] which entity should be the 'lead entity', provided that, among other things, the proposed 'lead entity' is not controlled by another member of the group that provides designated services.[85]

Penalties	
Current regime	**Change**
Many of the governance-related requirements are outlined in the Old AML/CTF Rules and are not civil penalty provisions.	Most of the governance-related provisions have been incorporated into the Amended AML/CTF Act and are now civil penalty provisions.

Matters for reporting entities to consider

Immediate priorities

- Review how AML/CTF issues or concerns are reported to the Board or senior management, as well as existing reporting lines, and internal information channels at entity level and, where applicable, also at group level. Identify the AML/CTF reporting lines that the reporting entity will need to update and adapt.
- Assess who would be best placed to be appointed as the 'senior manager' and what approval requirements need to be documented of the senior manager's approval of the reporting entity's ML/TF risk assessment and the AML/CTF policies.
- Consider whether the entity's AML/CTF Compliance Officer meets the new fit and proper criteria and has adequate resources, authority and independence to carry out their functions appropriately. Document that assessment accordingly.
- If the entity is part of a group, carefully consider which entity within the group might act as the 'lead entity' for the 'reporting group', and which entities should be part of the 'reporting group'.

By 31 March 2026

- Designate an individual as a 'senior manager' to carry out the new ML/TF risk assessment and AML/CTF policy approval requirements in the future.
- If not already done, conduct a documented 'fit and proper' person test for your AML/CTF compliance officer and ensure that they have adequate resources and are independent from the business lines and units. If necessary, establish a dedicated AML/CTF unit to support the AML/CTF Compliance Officer. Reporting entities providing designated services in Australia should ensure that their AML/CTF compliance officer is resident in Australia.
- Appoint a 'lead entity' for the 'reporting group'.
- Within 'reporting groups', develop an effective group-wide information sharing system and agree it with the group members. While the tipping off restrictions have been relaxed, reporting entities within a group should continue to exercise care when sharing information subject to the tipping off offence and only share where required and with appropriate safeguards in place.

81 Amended AML/CTF Act ss 236B(1)-(2).
82 Ibid ss 26F(5)-(6).
83 AML/CTF Rules 2025 ss 2-1 and 2-2.
84 Ibid s 2-1(1).
85 Ibid ss 2-1(2)(b) and 2-2(3)(a).

03

Reformed customer due diligence requirements

Snapshot of the reforms

The Amended AML/CTF Act revises the current due diligence requirements (**CDD**) clarifying when due diligence measures may be simplified or must be enhanced based on the ML/TF risk of the customer. Reporting entities shall:

- undertake identification and verification for customers;[86]
- assess the ML/TF/PF and proliferation financing risks linked to providing designated services to their customers;[87] and
- implement appropriate procedures and measures to regularly assess, mitigate and manage these risks.[88]

The new AML/CTF Rules have resulted in a rewrite of the approach to what minimum information must be collected and verified for different customer types. Although earlier drafts of the AML/CTF Rules envisaged the removal of prescriptive minimum information requirements, the final AML/CTF Rules prescribe what information must be collected for different customer types. The AML/CTF Rules however do not prescribe what KYC information must be verified for each customer type or provide any 'safe harbours' for sources that are reliable and independent.

It is critical to note that reporting entities must establish the customer's initial risk rating in addition to various identification matters relating to the customer, its beneficial owners, the nature and purpose of the business relationship and additional matters specified in the AML/CTF Rules 2025. This must occur before providing designated services unless it would interrupt the ordinary course of business.

It is also important to note that the ML/TF/PF risk of a customer is not static and reporting entities must assess it over the course of the relationship with the customer, reflecting the reporting entity's continuing monitoring obligations including through ongoing CDD (**OCDD**) and transaction monitoring.

The Amended AML/CTF Act provides for additional OCDD and enhanced CDD (**ECDD**) requirements, and also introduces sanctions screening requirements into CDD.

Summary of the key changes

CDD	
Current regime	**Change**
Under the current regime, reporting entities are required to undertake identification and verification procedures before providing a designated service to customers.[89] The identification and verification procedures are carried out through an applicable customer identification procedure (ACIP), which is set out in Part B of the reporting entities' AML/CTF program.[90] The requirements for ACIP are prescribed by the Old AML/CTF Rules.[91]	The Amended AML/CTF Act repeals Divisions 1 to 5 of Part 2 (Identification Procedures), and substitutes them with new provisions related to initial and ongoing CDD.[92]

86 AML/CTF Act 2006 ss 28(3)(b) and (d).
87 Ibid s 26C(1).
88 Ibid s 26F(1).
89 AML/CTF Act 2006 s 32(1).
90 Ibid s 84(3)(a).
91 Old AML/CTF Rules Parts 4.2 – 4.8.
92 Amended AML/CTF Act ss 28 and 30.

Identification procedures	
Current regime	**Change**
A reporting entity must not commence the provision of a designated service to a customer until it has carried out the ACIP, unless one of the exceptions apply.[93] There is no explicit requirement for reporting entities to assess the ML/TF risk in respect of their customers. In certain circumstances, reporting entities may complete ACIP after providing designated services to the customer.[94]	A reporting entity must complete initial CDD before providing a designated service to a customer unless it would interrupt the ordinary course of business. Matters that must be established on reasonable grounds as part of initial CDD are:[95] • the identity of the customer. The specific KYC information that must be collected to establish the customer's identity is specified in the AML/CTF Rules 2025 and depends on whether the customer is a sole trader, body corporate, trust, or government body; • the identity of any person on whose behalf the customer is receiving the designated service; • the identity of any person acting on behalf of the customer and their authority to act; • the identity of any beneficial owners of the customer; • whether the customer, any beneficial owner of the customer, any person on whose behalf the customer is receiving the designated service, or any person acting on behalf of the customer is: (i) a politically exposed person; or (ii) a person designated for targeted financial sanctions; and • the nature and purpose of the business relationship or occasional transaction (the information that must be collected to establish this is at least KYC information about the nature of the customer's business or operations[96]). To establish the customer's identity on reasonable grounds, the reporting entity must:[97] • take reasonable steps to establish the customer is the person they claim to be; • identify the ML/TF/PF risk of the customer, based on KYC information reasonably available; • collect KYC information about the customer, appropriate to their ML/TF/PF risk; and • verify, using reliable and independent information, the KYC information. The exemption allowing designated services to be provided before completing CDD remains[98] where it is 'essential to avoid interrupting the ordinary course of business', along with other conditions, such as complying with policies and ensuring the customer's risk rating is low.[99] Failure to comply with initial CDD requirements is a civil penalty contravention.[100]

Minimum information to collect and verify	
Current regime	**Change**
The Old AML/CTF Rules prescribed what information needed to be collected and verified for certain customer types.[101]	The AML/CTF Rules 2025 also prescribe minimum information that must be collected for different customer types as part of initial customer due diligence.[102] However, they do not specify what KYC information must be verified for each customer type.

93 AML/CTF Act 2006 ss 32(1)-(2).
94 Ibid s 33.
95 Amended AML/CTF Act s 28(2).
96 AML/CTF Rules 2025 ss 6-1(3), 6-2(4), 6-3(6) and 6-4(3).
97 Amended AML/CTF Act s 28(3).
98 Ibid s 29.
99 Ibid ss 29(a)–(f).
100 Ibid ss 28(9)-(10).
101 Old AML/CTF Rules Chapter 4.
102 AML/CTF Rules 2025 ss 6-1–6-4.

Deemed compliance	
Current regime	**Change**
The AML/CTF Act does not provide for deemed compliance with initial and ongoing CDD requirements.	The Amended AML/CTF Act provides for the AML/CTF Rules 2025 to set out circumstances of deemed compliance with initial and ongoing CDD requirements.[103] The AML/CTF Rules 2025 establish deemed compliance on reasonable grounds in the following circumstances: • where the reporting entity has, before 31 March 2026, carried out the applicable customer identification procedure in respect of that customer or the trustee in line with the AML/CTF Act 2006;[104] • where the proposed designated services will be provided at or through a permanent establishment of the reporting entity in a foreign country and the reporting entity has, before 31 March 2026, complied with the laws of that country giving effect to the FATF Recommendations relating to CDD and record-keeping for that customer;[105] • where the customer has become a customer of the reporting entity as a result of a business transfer, acquisition or sale and the records or transaction and KYC records are accessible to the reporting entity.[106] • where the customer is an individual and has been unable to prove all matters to be established for CDD due to circumstances beyond their control, but the reporting entity has taken reasonable steps to establish the customer's identity and identify and respond to their level of ML/TF/PF risk, and the reporting entity has policies to mitigate and manage any additional risk;[107] • where the reporting entity or a member of its 'reporting group' has previously provided a service to the customer in a foreign country that gives effect to the FATF Recommendations relating to CDD, and the reporting entity holds appropriate KYC records for that customer;[108] • if seeking to establish the identity of any person on whose behalf the customer is receiving the designated service: – where the customer is not a trust or an equivalent foreign legal arrangement, the proposed designated service does not relate to a life policy or sinking fund policy as specified in the AML/CTF Act 2006, and the reporting entity has established on reasonable grounds the identity of the customer;[109] – where the customer is a trust or an equivalent foreign legal arrangement, the proposed designated services will be provided at or through a permanent establishment of the reporting entity in a foreign country, and the reporting entity establishes on reasonable grounds the identity of the beneficiaries of the trust, or, where identification is not possible, a description of each class of beneficiary;[110]

103 Amended AML/CTF Act s 28(6)(b).
104 AML/CTF Rules 2025 s 6-42.
105 Ibid s 6-43.
106 Ibid s 6-27.
107 Ibid s 6-10.
108 Ibid s 6-11.
109 Ibid s 6-6(1).
110 Ibid s 6-6(2).

Deemed compliance (continued)	
Current regime	Change
	– where the designated service is issuing, or undertaking liability as the insurer under, a life policy or sinking fund policy, or accepting a premium in relation to a life policy or sinking fund policy, in the capacity of insurer for the policy, and the reporting entity has collected the full name of any person who may be entitled to receive a payment under the policy or, where that is not possible, collected information describing each class of persons that may be entitled to a payment under the policy;[111] and – where the customer is low risk so that ECDD obligations do not apply to the customer, the reporting entity has identified the ML/TF/PF risk of the customer based on collected KYC information of an appropriate level about the customer that is reasonably available to the reporting entity, and, if the customer is an individual, the reporting entity has taken reasonable steps to establish that the customer is the person the customer claims to be;[112] • if seeking to establish the identity of any beneficial owners of the customer: – where the reporting entity establishes on reasonable grounds that the customer is a listed public company subject to public disclosure requirements that ensure transparency regarding beneficial owners;[113] – where the reporting entity is unable to establish the identity of any beneficial owners, and the customer is a body corporate, partnership or unincorporated association, the reporting entity takes and records all reasonable steps to establish the identity of any beneficial owners, collects information about the CEO or equivalent of the customer, and verifies collected information using reliable and independent data appropriate to the ML/TF risk of the customer;[114] – where the customer is low risk, so that ECDD obligations do not apply to the customer, and the customer is a government body, an entity subject to oversight by a prudential, insurance or investor protection regulator, a corporation or association of homeowners in a strata title or community title scheme or a listed public company;[115] and – where the customer is low risk so that ECDD obligations do not apply to the customer, the reporting entity has identified the ML/TF risk of the customer based on collected KYC information of an appropriate level about the customer that is reasonably available to the reporting entity, and if the customer is an individual, the reporting entity has taken reasonable steps to establish that the customer is the person the customer claims to be and there are no reasonable grounds for the reporting entity to doubt the adequacy or veracity of that KYC information;[116]

111 Ibid s 6-34.
112 Ibid s 6-17.
113 Ibid s 6-7.
114 Ibid s 6-8(1).
115 Ibid s 6-18.
116 Ibid s 6-17.

Deemed compliance (continued)	
Current regime	**Change**
	• if seeking to establish the identity of a person acting on behalf of the customer and their authority to do so: – where the customer is not an individual; and the reporting entity has established on reasonable grounds the authority of the person to act on behalf of the customer and that any additional risk of ML/TF/PF, terrorism financing or proliferation financing associated with the person acting on behalf of the customer is low, the reporting entity has collected KYC information about the customer, relating to the person acting on behalf of the customer, that is appropriate to the ML/TF/PF risk of the customer, and there are no reasonable grounds for the reporting entity to doubt the adequacy or veracity of that KYC information.[117]

OCDD	
Current regime	**Change**
A reporting entity must monitor its customers in relation to the provision of designated services at or through its permanent establishment, aiming to identify, mitigate, and manage its ML/TF risk.[118] This requirement does not apply if the reporting entity provides a designated service as the holder of an Australian financial services licence (AFSL) under item 54 of table 1 in s 6 of the AML/CTF Act.[119] If the reporting entity is part of a DBG, the obligation may be fulfilled by any other group member.[120] If the reporting entity is a registered remittance affiliate of a registered remittance network provider, the obligation may be fulfilled by the remittance network provider.[121]	The OCDD obligation remains. However, the scope of matters a reporting entity must monitor as part of OCDD has expanded.[122] A reporting entity must monitor its customers in relation to designated services to identify, assess, manage, and mitigate the ML/TF/PF risks it may face.[123] This includes:[124] • monitoring for unusual transactions or behaviours which would give rise to SMR obligations; • if there is a significant change to the customer's risk assessment; • reverifying KYC information if the reporting entity has doubts about the adequacy or veracity of the KYC information relating to the customer; • for pre-commencement customers, monitor for significant changes in the nature or purpose of the relationship that may increase the ML/TF risk to medium or high; and • review and, where appropriate, update and reverify KYC information if, during the course of the customer relationship, a customer becomes: (a) a foreign PEP; or (b) a domestic PEP or international organisation PEP, and the ML/TF risk of the customer is high.[125] The AML/CTF Rules 2025 list the possible offences that the reporting entity must monitor its customers for in order to be taken to have complied with these monitoring obligations.[126] Listed offences include money laundering, terrorism and terrorism financing, proliferation financing, human trafficking, sexual exploitation, corruption and bribery.

117 Ibid s 6-19.
118 AML/CTF Act 2006 s 36(1).
119 Ibid s 36(3).
120 Ibid s 36(4).
121 Ibid s 36(5).
122 Amended AML/CTF Act s 30(2).
123 Ibid s 30(1).
124 Ibid s 30(2).
125 AML/CTF Rules 2025 s 6-24.
126 Amended AML/CTF Act s 30(2); AML/CTF Rules 2025 s 6-35. The requirement applies irrespective of whether the customer is in a business relationship with the reporting entity, or they are just undertaking an occasional transaction.

OCDD (continued)	
Current regime	**Change**
	The Amended AML/CTF Act provides a non-exhaustive list of examples of unusual transactions and behaviours:[127] • unusually large or complex transactions; • transactions and behaviours that are part of an unusual pattern of transactions; • transactions and behaviours that have no apparent economic or lawful purpose; and • transactions and behaviours that are inconsistent with what the reporting entity reasonably knows about the customer; the nature and purpose of the business relationship; the ML/TF risk of the customer; or the customer's source of funds or source of wealth. Failure to undertake OCDD constitutes a civil penalty contravention.[128] The Amended AML/CTF Act retains exemptions for reporting entities where they are providing services: • in the capacity as a registered remittance affiliate where the obligation is discharged by the registered remittance network provider;[129] and • under an item 54, table 1 designated service.[130]

Sanctions screening	
Current regime	**Change**
Sanctions Screening is not currently required under the AML/CTF Act 2006. Instead, requirements to comply with sanctions laws have been imposed under the *Charter of the United Nations Act 1945* and the *Autonomous Sanctions Act 2011* (and subordinate legislation), which impose criminal rather than civil penalties for breaches.	The Amended AML/CTF Act requires that reporting entities must establish during initial CDD whether a customer, or any beneficial owner or person acting on the customer's behalf is designated for targeted financial sanctions.[131] The AML/CTF Rules 2025 also provide that a reporting entity's AML/CTF policies must deal with ensuring that when providing designated services, the reporting entity:[132] • does not make any assets available to, or available for the benefit of, a sanctioned person; and • does not use or deal with, or allow or facilitate the use of or dealing with, any assets owned or controlled (directly or indirectly) by a sanctioned person.

127 Amended AML/CTF Act s 30(5).
128 Ibid ss 30(7)-(8).
129 Ibid s 30(9).
130 Ibid s 30(10).
131 Ibid s 28(2)(e)(ii).
132 AML/CTF Rules 2025 s 5-3.

Screening of politically exposed persons (PEPs)	
Current regime	**Change**
The Old AML/CTF Rules require that reporting entities have appropriate risk management systems in place to identify PEPs, determine if they are of a high ML/TF risk, and if so, obtain senior management approval for providing services to them, establish their source of wealth and funds, and undertake OCDD.[133] They also require a reporting entity to collect source of wealth and source of funds for foreign PEPs and high risk domestic or international organisation PEPs.[134]	The Amended AML/CTF Act requires that, as part of initial CDD, a designated service must not be provided unless the reporting entity has established a customer's PEP status.[135] As is presently the case, if the customer is a foreign PEP or a high risk domestic or international organisation PEP, the AML/CTF Rules 2025 require that the person's source of wealth and source of funds must be established prior to providing the designated service.[136]

CDD in respect of trust arrangements	
Current regime	**Change**
The AML/CTF Act 2006 does not set out any specific requirements relating to CDD in respect of trust arrangements. However, the Old AML/CTF Rules specify the customer identification procedures that must be applied for trustees of a trust, and what information needs to be collected and verified in relation to a trustee of a trust. [137] In particular a reporting entity's AML/CTF Program must have controls in place to collect, and information that confirms, that the trust exists, and the name of each trustee and beneficiary, or a description of each class of beneficiary.[138]	The Amended AML/CTF Act requires reporting entities to establish the identity of any person on whose behalf the customer is receiving the designated service, before providing that designated service, and requires more information to be collected about trusts.[139] Instead of the customer being the trustee of a trust, the AML/CTF Rules 2025 characterise the customer as the trust. Where the customer is a trust, or an equivalent foreign legal arrangement, the reporting entity must comply with the requirements set out at AML/CTF Rules 2025.[140]

133 Old AML/CTF Rules Part 4.13.
134 Ibid Part 4.13.3(3).
135 Amended AML/CTF Act s 28(2)(e)(i).
136 AML/CTF Rules 2025 s 6-23.
137 Old AML/CTF Rules Part 4.4.
138 Ibid Part 4.4.2.
139 Amended AML/CTF Act s 28(2)(b).
140 AML/CTF Rules 2025 s 6-3(1).

Identifying the beneficial owner	
Current regime	**Change**
The definition of 'beneficial owner' of a customer is set out in the Old AML/CTF Rules as an individual who ultimately owns or controls (directly or indirectly) the customer.[141] 'Control' is defined to mean control as a result of, or by means of, trusts, agreements, arrangements, understandings and practices, whether or not having legal or equitable force and whether or not based on legal or equitable rights, and includes exercising control through the capacity to determine decisions about financial and operating policies. 'Owns' is defined to mean ownership (either directly or indirectly) of 25% or more of a person.	The Amended AML/CTF Act requires that, where the customer is not an individual, the reporting entity must establish the identity of any 'beneficial owner' of the customer.[142] The definition of 'beneficial owner' is an individual who ultimately owns (either directly or indirectly) 25% or more of the entity or controls (directly or indirectly) the entity.[143] Where there are no beneficial owners that satisfy these criteria, and the customer is a body corporate, partnership or unincorporated association, the AML/CTF Rules 2025 require the reporting entity to establish the identity of the chief executive officer (or equivalent) of the customer.[144]

Senior manager approval	
Current regime	**Change**
The Old AML/CTF Rules state that an AML/CTF program must require senior management approval before establishing or continuing a business relationship with a foreign PEP or high risk domestic or international organisation PEP.[145]	The AML/CTF Rules 2025 require that the AML/CTF policies of a reporting entity ensure that senior manager approval is obtained before the reporting entity commences to provide a designated service to:[146] • a foreign PEP; • a domestic PEP or an international organisation PEP and the ML/TF risk is high; or • the service is being provided as part of a nested services relationship.

141 Old AML/CTF Rules Part 1.2.1.
142 Amended AML/CTF Act s 28(2)(d).
143 Ibid s 5.
144 AML/CTF Rules 2025 ss 6-8(2)-(3).
145 Old AML/CTF Rules Part 4.13.3(2).
146 AML/CTF Rules 2025 s 5-5.

Simplified CDD	
Current regime	**Change**
The AML/CTF Act 2006 does not provide for a simplified CDD regime, but the Old AML/CTF Rules outline when simplified verification procedures are to be applied.[147] A reporting entity may use a simplified verification procedure for: • domestic listed public companies or their majority-owned subsidiaries, or companies licensed and regulated by an Australian authority;[148] and • Australian Securities and Investments Commission (**ASIC**) – regulated managed investment schemes and wholesale managed investment schemes not registered with ASIC, trusts registered and subject to Commonwealth regulatory oversight, or government superannuation funds established by legislation.[149]	The Amended AML/CTF Act introduces simplified CDD regimes directly into the Act. The Act outlines the circumstances under which reporting entities may apply simplified CDD as part of both initial CDD and OCDD.[150] For initial CDD, the Act notes that a reporting entity may apply simplified CDD if:[151] • the ML/TF/PF risk of the customer is low; • ECDD requirements do not apply to the customer; and • the reporting entity complies with the requirements in the AML/CTF Rules 2025. The AML/CTF Rules 2025 clarify that a reporting entity may only conduct simplified CDD if the application of those measures is dealt with in the AML/CTF policies of the reporting entity.[152]

Enhanced CDD	
Current regime	**Change**
An ECDD procedure must be included in Part A of the AML/CTF program and must apply if:[153] • the ML/TF risk of a customer is determined to be high; or • a designated service is provided to a foreign PEP; • an SMR obligation arises; or • a transaction involves a party physically present in, or incorporated in, a prescribed foreign country.	The Amended AML/CTF Act introduces ECDD into the text of the Act, and broadens the ECDD requirements. ECDD must be applied where one or more of the following applies:[154] • the ML/TF/PF risk of the customer is high; • an SMR obligation arises, and the reporting entity proposes to continue providing designated services to the customer; • the customer, any beneficial owner of the customer, or a person acting or receiving services on behalf of the customer are foreign PEPs or physically present in a high-risk jurisdiction; • the customer is a body corporate or legal arrangement formed in a high-risk jurisdiction; • the designated service is provided through a nested services relationship; • the customer seeks designated services which have no apparent economic or legal purpose, or would involve unusually complex or large transactions, or an unusual pattern of transactions.

147 Old AML/CTF Rules Parts 4.3.8 and 4.4.8.
148 Old AML/CTF Rules Part 4.3.8.
149 Ibid Part 4.4.8.
150 Amended AML/CTF Act s 31.
151 Ibid.
152 AML/CTF Rules 2025 s 6-16.
153 Old AML/CTF Rules Part 15.9.
154 Amended AML/CTF Act s 32; AML/CTF Rules 2025 s 6-20.

Enhanced CDD (continued)	
Current regime	**Change**
	ECDD can apply to both initial and OCDD and include processes that enable the collection and verification of additional KYC information to manage the identified higher risk.[155] OCDD must be adjusted to reflect ML/TF risk and meet the requirements in the AML/CTF Rules 2025. ECDD must now also include the collection of source of wealth and source of funds in certain circumstances.[156]

Record keeping	
Current regime	**Change**
Record-keeping obligations are imposed on the reporting entity regarding documents produced during the ACIP process.[157] The reporting entity must maintain a record of the procedures and information obtained during ACIP, retaining these records for 7 years.[158] These obligations can be fulfilled by another member of the designated business group to which the reporting entity belongs.[159]	The Amended AML/CTF Act repeals and expands the existing record-keeping obligations under the AML/CTF Act. Section 111 requires reporting entities to retain specific records when complying with ss 28 (initial CDD) or 30 (OCDD). These records must be kept for 7 years after the business relationship ends or an occasional transaction is completed.[160] The records must contain sufficient and accurate information demonstrating the reporting entity's compliance with Part 2 of the Amended AML/CTF Act. This includes records that reflect the type and content of data collected, as well as any analysis, identification, or assessment of ML/TF risks, or decision-making related to the customer.[161] All records must be in English, or in a form that is readily accessible and translatable into English.

Matters for reporting entities to consider

Immediate priorities

With the significant overhaul of the current CDD regime and the introduction of civil penalty offences for non-compliance, the amendments require reporting entities to:

- due diligence their customers and risk rate them before conducting CDD; and
- update or develop new processes and technology systems as needed to ensure compliance with the amended CDD obligations, including sanctions screening requirements.

By 31 March 2026

Reporting entities must ensure that:

- they have updated their CDD and ECDD procedures to meet the new requirements in the Amended AML/CTF Act, and AML/CTF Rules 2025, including updates of systems and policies to include sanctions screening; and
- they do not provide designated services to customers before conducting initial CDD, unless applicable exemptions apply.

155 Amended AML/CTF Act s 32.
156 AML/CTF Rules 2025 s 6-21.
157 AML/CTF Act 2006 ss 111-114B.
158 Ibid s 114A(1).
159 AML/CTF Act 2006 s 114B(4).
160 Amended AML/CTF Act ss 111(1)-(2).
161 Amended AML/CTF Act s 111(3).

04

Transfers of value

Snapshot of the reforms

- The reforms to the AML/CTF Act replace the existing requirements relating to electronic funds transfer instructions (**EFTIs**) and international funds transfer instructions (**IFTIs**) with the concept of 'transfer of value' that will apply to all reporting entities. These replace the current obligations in relation to EFTIs, IFTIs, and IFTIs under a designated remittance arrangement (**IFTI-DRA**).
- The Amended AML/CTF Act adopts a technology-neutral approach to transfers, eliminating the existing distinction between designated services based on the nature of the person receiving instructions and the person ultimately making money available to the beneficiary. It does so by introducing the concept of 'transfers of value', which, consistent with other changes, will apply beyond the traditional scope of electronic payments. This will include virtual assets, consistent with changes to the FATF Recommendations.
- In addition, the so-called Travel Rule will be applied across the 'transfer of value' chain, including to ordering institutions, intermediary institutions, and beneficiary institutions. The Travel Rule relates to the information about the payers and beneficiaries that must be included in any transfer of value between financial institutions and virtual asset service providers. The core requirement to pass on information will remain, and the AML/CTF Rules 2025 set out what information is to be transmitted.
- In connection with the Travel Rule, ordering institutions, intermediary institutions, and beneficiary institutions will have new obligations relating to collecting, verifying and passing on information, which reflect their role in the 'transfer of value':
  - the 'ordering institution' must collect and verify Travel Rule information (as defined below), and pass it to the next institution in the value transfer chain before passing on a value transfer message; and
  - the 'beneficiary institution' and 'intermediary institution' must both take reasonable steps to monitor whether it has received Travel Rule information from the preceding entity(ies), and whether the information received is accurate. They also must not pass on the value transfer message (or take other action, as appropriate) if they do not receive all the Travel Rule information.
- For reporting purposes, the Amended AML/CTF Act introduces a new concept of 'international value transfer services' (**IVTS**). The Government has announced that transitional rules will be made to provide for a later commencement of the new IVTS obligations post-2026. These transitional rules will preserve the existing IFTI reporting requirements so that these provisions are still in force.[162] The new obligations for value transfer and the travel rule will commence on 31 March 2026.

162 Department of Home Affairs, 'Changes to value transfer obligations', available here.

Summary of the key changes

Designated services	
Current regime	**Change**
The relevant 'designated services' draw distinctions based on the persons involved in the transfer of money or property. There are two 'designated services' in respect of financial institutions transferring money by way of EFTIs: • **item 29:** accepting an EFTI from a 'payer'; and • **item 30:** making money available to a 'payee' as a result of an EFTI. There are two 'designated services' in respect of transferring money or property under a 'designated remittance arrangement': • **item 31**: accepting instructions to transfer money or property under a 'designated remittance arrangement'; and • **item 32:** making money or property available as a result of a 'designated remittance arrangement'.	Three amended designated services (each, a **Value Transfer Designated Service**) have been introduced in relation to transfers of value, which remove the references to EFTIs and refer to the new institution categories that have been introduced:[163] • **new item 29:** an 'ordering institution' accepting an instruction for a 'transfer of value' from a 'payer'; • **new item 30:** a 'beneficiary institution' making transferred value available to a 'payee'; and • **new item 31:** an 'intermediary institution' passing on a 'transfer message' for a 'transfer of value'.

Transfers of value	
Current regime	**Change**
EFTIs involve financial institutions, where:[164] • an 'ordering institution' receives the EFTI from a 'payer'; and • a 'beneficiary institution' makes money available to a 'payee'. There are different types of EFTIs depending on whether: • the 'ordering institution' is the same as the 'beneficiary institution', and • the 'payer' is the same as the 'payee'. 'Designated remittance arrangements' involve 'non-financiers'.	A streamlined concept of a 'transfer of value' will be introduced which will apply beyond the traditional scope of electronic payments. 'Transfer of value' includes (inter alia) money, virtual assets or property but excludes physical currency or other tangible property.[165] The 'value transfer chain' includes:[166] • an 'ordering institution'; • a 'beneficiary institution'; and • any 'intermediary institution', with simplified definitions of each based on their role in the value transfer chain. An ordering institution is a person that accepts an instruction for a 'transfer of value' on behalf of a payer in the course of carrying on a business.[167] A beneficiary institution is a person who, in relation to a 'transfer of value', makes the value transferred available to a payee in the course of carrying on a business.[168] There is no separate concept of a 'remittance arrangement' for 'designated services' purposes.

163 Amended AML/CTF Act s 6.
164 AML/CTF Act 2006 s 8.
165 Amended AML/CTF Act s 5.
166 Ibid s 63A.
167 AML/CTF Rules 2025 s 8-1(2).
168 Ibid s 8-2(2).

Travel rule	
Current regime	**Change**
Financial institutions which provide item 29 and item 30 designated services above must collect, transmit and maintain records of certain information about a 'payer' (**Travel Rule Obligation**).	The Travel Rule Obligation applies to all entities in a 'value transfer chain' described above and covers information both about a 'payer' and a 'payee'.[169] The AML/CTF Rules 2025 set out details of the information subject to the Travel Rule Obligation.[170] Before an ordering institution passes on a value transfer message, it must have collected and verified the Travel Rule information, and must pass on that information to the next institution in the value transfer chain.[171] The Travel Rule information that must be collected, verified and passed on depends on the circumstances; the AML/CTF Rules 2025 list relevant circumstances that may apply.[172] A 'beneficiary institution' will be required to take reasonable steps to monitor whether it has received the Travel Rule information from the preceding entity(ies), and whether the information received about the payee is accurate.[173] Additionally, a 'beneficiary institution' will be prohibited from passing on the value transfer message (or take other action as appropriate) if it does not receive all the Travel Rule information or the information it does receive is inaccurate.[174] The AML/CTF Rules 2025 specify the circumstances that determine what information the beneficiary institution must monitor for.[175] An 'intermediary institution' will also be required to take reasonable steps to monitor whether they have received the Travel Rule information from the preceding entity(ies) and whether it is accurate.[176] Additionally, an 'intermediary institution' will be prohibited from passing on the value transfer message (or take other action as appropriate) if it does not receive all the Travel Rule information. The AML/CTF Rules 2025 specify the circumstances that determine what information the intermediary institution must monitor for and pass on.[177]

IFTI reporting	
Current regime	**Change**
An IFTI is: • an instruction accepted in Australia to make money or property available in another country; or • an instruction accepted in another country to make money or property available in Australia, being either an EFTI or an instruction under a 'designated remittance arrangement'.	An IVTS is a Value Transfer Designated Service involving value transferred between Australia and another country.[178] It is envisaged that the obligation to provide an IVTS report will shift to the entity that sits closest to the Australian customer. A reporting entity which provides an IVTS through a 'permanent establishment' of the reporting entity in Australia must submit a report of the IVTS to AUSTRAC within 10 business days.[179]

169 Ibid ss 8-3 – 8-5.
170 Amended AML/CTF Act s 64(6), 65(4), 66(6); AML/CTF Rules 2025 ss 8-3 – 8-5.
171 Ibid s 64(2).
172 AML/CTF Rules 2025 s 8-3.
173 Amended AML/CTF Act s 65(2).
174 Ibid s 65(3).
175 AML/CTF Rules 2025 s 8-4.
176 Amended AML/CTF Act s 66(2).
177 AML/CTF Rules 2025 s 8-5.
178 Amended AML/CTF Act s 45(1).
179 Ibid ss 46(1)(a)-(b), (2) and (4).

IFTI reporting (continued)	
Current regime	**Change**
A person who sends an IFTI out of Australia or receives an IFTI transmitted into Australia must submit a report of the IFTI to AUSTRAC within 10 business days, including such information as set out in the Old AML/CTF Rules.	The AML/CTF Rules 2025 relating to reporting of IVTS have not yet been published; transitional arrangements will be put in place for 2026, which will be subject to consultation. We anticipate that these rules may prescribe: • circumstances in which an 'intermediary institution' in the value transfer chain must report an IVTS instead of a 'reporting entity';[180] • exemptions to the requirement to report an IVTS;[181] and • other conditions that must be satisfied before a reporting entity must report an IVTS.[182]

Policy requirements relating to the travel rule	
Current regime	**Change**
	Changes to the 'transfer of value' rules mean that reporting entities will be required to take additional steps to collect and verify Travel Rule information. They will also keep existing obligations in relation to passing on the Travel Rule information. The AML/CTF Rules 2025 also require that reporting entities have in place AML/CTF policies in relation to their obligations as ordering institutions,[183] intermediary institutions[184] and beneficiary institutions[185] relating to 'transfers of value'.

Matters for reporting entities to consider

Immediate priorities

- Consider whether any services provided are in relation to a 'transfer of value' between one or more persons, and the role played in bringing about the transfer of value (i.e. whether you are an ordering, beneficiary or intermediary institution).
- This determination will involve detailed consideration of the role(s) played in 'transfers of value', for example, whether the transferred value is made available to the payee directly, or to a person acting on behalf of the payee;[186] whether the value held is to be transferred in an account provided to the payer or on deposit from the payer,[187] whether payment is arranged to be made under an offsetting arrangement;[188] and whether the transferred value is made available to the payee, under an arrangement with the payee, by depositing the value with a third-party deposit-taker or credit provider.[189]
- If providing transfer of value services, assess your current processes are sufficient to ensure that Travel Rule Obligations are met, including the monitoring of transactions, and reporting suspicious matters to AUSTRAC.
- Consider whether existing systems are sufficient to (where applicable), collect, verify and pass on Travel Rule information.

By 31 March 2026

- Uplift AML/CTF policies to include procedures relating to collecting, verifying and passing on information in a transfer of value chain.
- For ordering institutions, update 'transfer of value' systems to reflect value transfer obligations, including Travel Rule information.
- Ensure that systems are capable of detecting and reporting incomplete Travel Rule information. Determine the steps to be taken where incomplete Travel Rule information is provided by an earlier value transfer chain participant.

180 Ibid ss 46(5)-(6).
181 Ibid ss 46(3) and (8)-(9).
182 Ibid s 46(1)(b).
183 AML/CTF Rules 2025 s 5-17.
184 Ibid s 5-18.
185 Ibid s 5-19.
186 Ibid ss 8-1(3)(a) and 8-2(3)(a).
187 Ibid ss 8-1(3)(b) and 8-2(3)(b).
188 Ibid s 8-1(3)(d) and 8-2(3)(d).
189 Ibid s 8-1(3)(c) and 8-2(3)(c).

05

Offshore activities

Snapshot of the reforms

- The wide territorial reach of the AML/CTF Act will be retained. The Amended AML/CTF Act captures:
  - services provided at or through a permanent establishment in Australia;
  - activities undertaken by residents in Australia at or through permanent establishments in foreign countries; and
  - subsidiaries of companies resident in Australia providing services at or through permanent establishments in foreign countries.
- Under the reforms, CDD requirements, including both initial CDD and OCDD, will also apply to reporting entities that provide services at or through offshore branches or subsidiaries. These obligations will apply with less prescriptive requirements than for reporting entities providing designated services through a permanent establishment in Australia, to minimise potential conflicts with local laws in the host country.
- The updated ML/TF/PF risk assessment requirements and AML/CTF policy obligations (for details see chapter '*AML/CTF Programs – Risk Assessments and policies*') will apply to all reporting entities, including those engaging in offshore activities. The Amended AML/CTF Act establishes less specific obligations, as it does not prescribe the factors to be considered in the risk assessment or the specific AML/CTF policies that must be included in the AML/CTF programs.
- Foreign branches or subsidiaries providing designated services must have or be able to produce records of compliance with their obligations under the AML/CTF Act, which must be in English or readily convertible into English and readily accessible.

Summary of the key changes

CDD requirements	
Current regime	**Change**
Currently, Part 2 of the AML/CTF Act, including both initial and ongoing CDD requirements, does not apply to reporting entities providing designated services through offshore branches or subsidiaries.	Under the Amended AML/CTF Act, initial and ongoing CDD requirements apply to all reporting entities, though the requirements for those providing designated services through offshore activities are less prescriptive.[190] The AML/CTF Rules 2025 provide that offshore companies may delay initial CDD where the service will be provided in a foreign country that gives effect to the FATF Recommendations, provided that other safeguards are in place.[191] They also provide that an offshore entity is taken to have established certain CDD matters where these have been established in another jurisdiction that gives effect to FATF recommendations.[192]

190 Amended AML/CTF Act ss 28(1)-(3) which addresses reporting entities without distinguishing between foreign and domestic entities.
191 Ibid s 29; AML/CTF Rules 2025 s 6-15.
192 AML/CTF Rules 2025 s 6-11.

ML/TF Risk Assessment and AML/CTF Policies requirements	
Current regime	**Change**
The AML/CTF Act does not contain explicit or specific requirements related to offshore branches or subsidiaries. For the general requirements applying to all reporting entities, see chapter '*AML/CTF programs – risk assessments and policies*'.	Entities providing designated services through offshore activities must: • undertake and keep an up-to-date ML/TF/PF risk assessment;[193] and • develop and maintain AML/CTF policies.[194]

Record keeping	
Current regime	**Change**
There are no explicit requirements with regard to the language to be used and the availability of records.	There will be a general obligation on all reporting entities to maintain records of compliance with their obligations under their AML/CTF program.[195]

New AUSTRAC conflict of laws notification requirement	
Current regime	**Change**
	A foreign branch or subsidiary of a reporting entity must notify AUSTRAC before the contravening conduct occurs if a conflict of laws prevents the implementation of Australian AML/CTF Act obligations in the host country. The entity must also demonstrate that it is taking reasonable steps to identify, assess, mitigate and manage the ML/TF risks arising from its inability to comply.[196] A reporting entity that adheres to these reporting and risk management requirements will not be liable for failure to comply with AML/CTF obligations due to the host country's regime.[197] The foreign branch or subsidiary must provide evidence of the conflicting laws to rely on this defence in civil penalty proceedings.[198]

Matters for reporting entities to consider

Immediate priorities

- Assess the AML/CTF compliance of foreign entities or branches by reviewing existing policies, procedures, and systems to identify any gaps or areas impacted by the new regime.
- Review the organisation's current documentation practices, focusing on information storage methods and the use of foreign languages.
- Analyse whether host country laws prevent the entity from implementing any of the forthcoming changes to Australia's AML/CTF framework.

By 31 March 2026

- Based on the assessment of the entity's policies, procedures and systems, prepare an action plan to address any identified gaps and ensure compliance with the future regime. Where not already in place:
  - implement effective CDD procedures in foreign branches or subsidiaries;
  - ensure compliance with ML/TF risk assessment and AML/CTF policies requirements; and
  - establish adequate record keeping procedures that ensure that documentation is comprehensive and accessible.
- Notify AUSTRAC of any conflicts of laws in the relevant host country that prevent the entity from complying with Australia's new AML/CTF regime. Additionally, develop alternative procedures and mechanisms to actively manage the associated ML/TF risks.

193 Amended AML/CTF Act ss 26C(1) and 26D.
194 Ibid s 26F(1).
195 Ibid s 107(1).
196 Ibid s 236A(1)(c).
197 Ibid s 236A(1).
198 Ibid s 236A(2).

06

‘Tipping off’ offence – more flexibility for information sharing

Snapshot of the reforms

- The Amended AML/CTF Act reforms the ‘tipping off’ offence by:
  - removing the ‘inferential limb’ and narrowing the offence to disclosures that would or could reasonably prejudice an investigation; and
  - adding exceptions such as disclosures between reporting entities (if regulations are passed) and those made for crime prevention purposes.
- These changes, effective 31 March 2025, aim to facilitate greater information sharing to better manage financial crime risks.
- AUSTRAC’s guidance on ‘tipping off’ outlines when disclosures could reasonably prejudice an investigation, specifies expectations for best practices to mitigate tipping off, and provides examples of disclosures unlikely to breach the offence.
- Starting 31 March 2026, reporting entities will be required to adopt and maintain AML/CTF policies within their AML/CTF program to prevent tipping off.

Summary of the key changes

Offence of tipping off	
Former regime	**Regime as of 31 March 2026**
Under the former AML/CTF regime, reporting entities were, subject to certain exceptions, prohibited from disclosing to anyone other than AUSTRAC entrusted persons:[199] • the fact that a reporting entity has or is required to issue a suspicious matter report (**SMR**), or provide information or produce a document under s 49(1) of the AML/CTF Act 2006; or • any information from which the above could reasonably be inferred.	The Amended AML/CTF Act reframes the ‘tipping off’ offence to prohibit disclosures to persons other than AUSTRAC entrusted persons: • that a reporting entity has or is required to submit an SMR;[200] • of SMRs (including copies) or documents purporting to set out information contained in SMRs;[201] • that persons are or have been required by s49(1) and s49B(2) notices to give information or produce documents, or that they have done so;[202] and • of information relating to the suspicions of cash dealers covered by the *Financial Transaction Reports Act 1988*,[203] which *would* or *could* reasonably be expected to prejudice an investigation of an offence against a law of the Commonwealth or a State or Territory, or under proceeds of crime legislation.[204] The offence applies regardless of whether an investigation has commenced.[205]

199 AML/CTF Act 2006 ss 123(1) and (2).
200 Amended AML/CTF Act s 123(1)(b), (2)(a).
201 Ibid ss 123(2)(b)-(d).
202 Ibid ss 123(2)(e)-(h).
203 Ibid s 123(2)(i). See *Financial Transaction Reports Act 1988* (Cth) ss 16(5A)(a), (b) or (c) or (5AA)(a) or (b), as in force immediately before its repeal.
204 Ibid s 123(1)(d).
205 Ibid s 123(3).

Offence of tipping off (continued)	
Former regime	Regime as of 31 March 2026
	AUSTRAC guidance sets out examples when an investigation could be prejudiced as follows:[206] • informing a customer or their associate that an SMR or additional information has been or needs to be reported to AUSTRAC; • making a customer aware of suspicions of criminal conduct, implying a need to report to AUSTRAC; • accidental public disclosure, such as via a website; and • sharing information with individuals who may further disseminate it, such as journalists, regarding activities in SMRs or suspicious transaction reports. Disclosures unlikely to prejudice an investigation include those:[207] • to Australian law enforcement, intelligence or regulatory agencies;[208] • to comply with a requirement under a law of the Commonwealth, a State or Territory; • within a 'reporting group', or to third-party service providers (subject to appropriate safeguards), for ML/TF/PF risk management purposes; • in the context of a merger or acquisition, and • to consultants engaged to support AML/CTF remediation and uplift.

AML/CTF policies	
Former regime	Regime as of 31 March 2026
Under the former AML/CTF regime, reporting entities were not required to set out measures to prevent 'tipping off' in their AML/CTF program.	Under the Amended AML/CTF Act, reporting entities will be required establish safeguards to prevent 'tipping off' in their AML/CTF policies.[209] AUSTRAC recommends implementing robust information controls, including restricting access, de-identifying data, ensuring confidentiality through undertakings, and maintaining secure storage and destruction practices. Third-party disclosures should comply with legal obligations and prevent 'tipping off'.[210]

Who is liable?	
Former regime	Regime as of 31 March 2026
The offence formerly applied only to the reporting entities.	The Amended AML/CTF Act extends liability beyond reporting entities to include *individuals* who are, or have been: • an officer, employee or agent of a reporting entity;[211] • required by a notice under s 49(1) to give information or produce documents;[212] or • required by a notice under s 49B(2) to give information or produce documents.[213] This extension creates a continued obligation for individuals not to disclose relevant information, even after the termination of their employment or association with the 'reporting entity'.

206 AUSTRAC guidance on tipping off (see here). The AUSTRAC guidance also provides several case studies regarding tipping off risks.
207 EM, para 474.
208 In this context, AUSTRAC identifies the following agencies as examples: Australian Taxation Office, National Anti-Corruption Commission, Australian Border Force, and Australian Criminal Intelligence Commission.
209 AML/CTF Rules 2025 s 5-13.
210 For examples see AUSTRAC guidance on tipping off, see here.
211 Amended AML/CTF Act s 123(1)(a)(ii).
212 Ibid s 123(1)(a)(iii).
213 Ibid s 123(1)(a)(iv).

Exceptions	
Former regime	**Regime as of 31 March 2026**
The 'tipping off' offence does not apply to disclosures by reporting entities to:[214] • legal practitioners for the purpose of obtaining legal advice; • external auditors of the reporting entity's AML/CTF program; • another FATF-compliant reporting entity within the same 'reporting group', for the purpose of informing the other entity about the risks involved in dealing with a relevant person; • foreign members of the same corporate or designated business group, where the reporting entity shares a customer with the foreign members, provided these foreign members are regulated by laws of a foreign country that give effect to some or all of the FATF recommendations; • registered remittance affiliates or registered remittance network providers, where communication is between these businesses; • authorised deposit-taking institutions (**ADIs**); or • comply with a law of the Commonwealth, a State or a Territory.	The Amended AML/CTF Act introduces two broad categories of exceptions to the 'tipping off' offence: • crime prevention;[215] and • information sharing to detect, deter or disrupt ML/TF/PF, proliferation financing, or other serious crimes (if additional regulations are passed).[216] The crime prevention exception applies if the disclosure is made in good faith by a lawyer or qualified accountant for the purpose of dissuading the customer from engaging in criminal conduct.[217] It applies only to disclosures related to SMRs, not those related to providing information or producing documents under notices.[218] The information sharing exception will apply if regulations are passed and where the disclosure is made to another reporting entity for the purposes of detecting, deterring, or disrupting ML/TF/PF, or other serious crimes. Any requirements prescribed by regulations must also be met. This provision is intended to allow for private-to-private anti-crime information sharing, subject to appropriate controls and safeguards.[219] AUSTRAC guidance has however clarified that an investigation will not be prejudiced where a disclosure is made in respect of all of the matters set out in the current exceptions in the AML/CTF Act 2006, including disclosure to lawyers, auditors, external providers and within a corporate group to manage ML/TF risk.[220]

Penalties	
Former regime	**Regime as of 31 March 2026**
Imprisonment for 2 years or 120 penalty units, or both.[221]	There is no change to this penalty under the Amended AML/CTF Act.[222]

214 AML/CTF Act 2006 ss 123(4)-(9).
215 Amended AML/CTF Act s 123(4).
216 Ibid s 123(5).
217 Ibid s 123(4).
218 Ibid s 123(4).
219 EM, para 484.
220 AUSTRAC guidance on tipping off, see here.
221 AML/CTF Act 2006 s 124(1).
222 Amended AML/CTF Act s 123(1).

Disclosure of AUSTRAC information to foreign countries or agencies	
Former regime	**Regime as of 31 March 2026**
The AML/CTF Act 2006 prescribes a list of agencies, authorities, bodies and organisations of the Commonwealth authorised to disclose AUSTRAC information to the government of a foreign country, or to a foreign agency.[223]	This list has been moved into the AML/CTF Rules 2025, to allow for greater flexibility in updating the list.[224]

Matters for reporting entities to consider

Immediate priorities

- Thoroughly review AUSTRAC's 'tipping off' guidance and start determining what controls to implement to prevent 'tipping off'.
- Implement strict access controls, secure storage solutions, password protection, and audit trails to safeguard sensitive information from unauthorised disclosure. Assess whether additional security measures may be required.
- Identify typical scenarios in which disclosing information could prejudice an investigation, taking into account the nature of the information, recipients, timing, and method of disclosure.
- Provide comprehensive training for all relevant personnel on the new 'tipping off' offence, highlighting the associated risks and outlining the correct protocols for handling suspicious activity and customer information.
- Ensure that, where applicable, third-party service providers are bound by appropriate confidentiality agreements and are fully aware of their obligations under the 'tipping off' offence.

223 AML/CTF Act 2006 s 127(3).

224 Amended AML/CTF Act s 127(2)(a); AML/CTF Rules 2025 s 10-1.

07

AUSTRAC powers – examination and information-gathering powers

Snapshot of the reforms

- The Amended AML/CTF Act introduces a new examination power, which enables AUSTRAC to obtain information and documents, including by requiring a person to appear before an examiner. This amendment aligns AUSTRAC's powers with those of other regulators such as ASIC and the Australian Prudential Regulation Authority (**APRA**).
- A new information-gathering power for intelligence purposes enables AUSTRAC to make broad requests for information or documents that assist in its intelligence functions, in line with FATF recommendations.
- The expansion of the current information-gathering power for compliance purposes allows AUSTRAC to request information from anyone possessing relevant documents or information related to compliance or enforcement of offences or civil penalties under the AML/CTF regime.
- The Amended AML/CTF Act introduces significant penalties for non-compliance with AUSTRAC's new coercive powers. For certain provisions, non-compliance is punishable by up to 2 years of imprisonment or 100 penalty units (currently $33,000.00).
- These changes have been in effect since January 2025.

Summary of the key changes

Examination power	
Former regime	**Current regime**
AUSTRAC did not possess an examination power under the former AML/CTF regime.	Under the Amended AML/CTF Act, if the AUSTRAC CEO (or their delegate) has reasonable grounds to believe that a person holds information or documents relevant to compliance with the AML/CTF regime, they may issue a written notice requiring the person to produce documents or appear before an examiner for examination.[225] The notice must specify the nature of the matters the examination will cover.[226] The framework for conducting examinations is as follows: • examinations are held in private;[227] • the examinee's lawyer may intervene to address the examiner or examine the examinee;[228] and • examinations may be recorded.[229]

225 Amended AML/CTF Act s 172A.
226 Ibid s 172A(3).
227 Ibid s 172D.
228 Ibid s 172F.
229 Ibid s 172G.

Examination offences	
Former regime	**Current regime**
There were no provisions relating to examinations.	The Amended AML/CTF Act introduces several new offences, including: • failure to comply with a s 172A notice, carrying a maximum penalty of 2 years imprisonment, 100 penalty units, or both;[230] • refusal or failure of an examinee to comply with affirmation requirements, with a maximum penalty of 3 months imprisonment;[231] • reckless refusal or failure of an examinee to answer questions, with a maximum penalty of 2 years imprisonment;[232] and • use or publication of a copy of an examination recording, except for preparing or conducting a proceeding, which carries a maximum penalty of 30 penalty units.[233]

Information gathering for intelligence purposes	
Former regime	**Current regime**
AUSTRAC was permitted to issue a notice requesting the production of information or documents when a suspicious matter had been reported.[234] However, there were no proactive intelligence-gathering powers to seek information or documents independently of a reported suspicious matter.	Under the new information-gathering power, the AUSTRAC CEO may issue a notice requiring a person to provide information or documents that could assist AUSTRAC in performing its intelligence functions.[235] This power allows AUSTRAC to proactively gather information in circumstances not triggered by the receipt of a SMR or threshold transaction report (**TTR**).[236] Individuals may refuse to comply with AUSTRAC's request for information if their response would be self-incriminating.[237] If a person receives a request for information notice from AUSTRAC, they are prohibited from disclosing to others that they have received the notice or what information has been requested.[238] AUSTRAC may also authorise other entities or regulators to supply it with information or documents, helping those entities navigate privacy and confidentiality issues.[239]

230 Ibid s 172A(4).
231 Ibid s 172C(3).
232 Ibid s 172C(5).
233 Ibid s 172H(2).
234 AML/CTF Act 2006 s 49B.
235 Amended AML/CTF Act s 49B.
236 EM para 796.
237 Ibid para 812.
238 Amended AML/CTF Act s 123(2A).
239 Ibid s 49C.

Information gathering for compliance purposes	
Former regime	**Current regime**
Authorised officers were, by written notice, permitted to require a person who is or was a reporting entity, or who was or is an officer, employee, or agent of a reporting entity, or who was or is on the Remittance Sector Registry, to provide information or documents relevant to the operation of the AML/CTF regime.[240] A person could not refuse to produce documents or information on the grounds that doing so might incriminate them. However, any information or documents provided were not admissible in civil or criminal proceedings, except in proceedings brought under the AML/CTF Act 2006.[241]	The Amended AML/CTF Act revises the previous information-gathering power, allowing AUSTRAC to issue a notice to anyone it reasonably believes possesses information or documents relevant to compliance with or enforcement of an offence and/or civil penalty provisions under the AML/CTF regime, the *Commonwealth Crimes Act 1914*, or the *Commonwealth Criminal Code* (as it relates to the Amended AML/CTF Act).[242] Additionally, the amendment narrows the scope of self-incrimination protections, excluding proceedings related to ML, TF/PF, as defined under the Amended AML/CTF Act.[243]

Matters for reporting entities to consider

Immediate priorities

- Implement robust document management systems to ensure accurate, comprehensive, and easily accessible records, enabling quick responses to information requests.
- Assess whether the AML/CTF Compliance Officer, as AUSTRAC's primary point of contact, has the necessary resources to respond quickly and effectively to any AUSTRAC information requests.
- Develop a standardised protocol for handling information requests and examination notices from AUSTRAC, and provide training for employees involved in managing these notices.
- Enhance board-level oversight of AML/CTF programs to ensure effective governance and compliance.

240 AML/CTF Act 2006 s 167(1).
241 AML/CTF Act 2006 s 169(2).
242 Amended AML/CTF Act s 167(1).
243 Amended AML/CTF Act s 169(2).

Contacts and authors

Caroline Marshall
Partner

+61 2 9210 6376
+61 488 004 331
caroline.marshall@corrs.com.au

Steven Rice
Partner

+61 2 9210 6091
+61 411 040 993
steven.rice@corrs.com.au

Angela Morris
Partner

+61 3 9672 3547
+61 406 862 681
angela.morris@corrs.com.au

Peter Anderson
Special Counsel

Leighton McDonald-Stuart
Senior Associate

Lindsey Cullen
Senior Associate

Molly Tredinnick
Senior Associate

Tegan Harrington
Senior Associate

Thilini Joseph
Associate

Tiana De Silva
Lawyer

Caleb Dunn
Lawyer

Salma Yari
Law Graduate

Oscar Loughnan
Law Graduate

**With a special thank you to Julia Vorlaender and Daniel Lee for their contribution to the playbook.*

CORRS
CHAMBERS
WESTGARTH

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au