KordaMentha

Key things Tranche 1 organisations need to know to be reform ready

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

March 2025

kordamentha.com

Updates and key things to know for Tranche 1 businesses

In November 2024, reforms to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) were passed by Parliament.

The reforms have been made to strengthen Australia's stance on money laundering and terrorism financing and bring the laws in line with standards recommended by global body, the Financial Action Task Force.

The changes aim to reduce the complexity and regulatory burden for reporting entities, ensure the regime responds to evolving threats, and protect businesses against exploitation by criminals.

These reforms are to be supported by a significant redrafting of the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Rules, and comprehensive guidance from AUSTRAC.

Key proposed areas of change

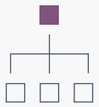
Following are summaries of key proposed areas of change:

AML/CTF programs

There will be flexibility in how businesses organise their AML/CTF Program, provided they meet their AML/CTF obligations.

AML/CTF Programs must comprise both the ML/TF risk assessment and AML/CTF policies, and they must be appropriately tailored to the nature, size and complexity of the business. Approval of the ML/TF risk assessment and AML/CTF policies and their updates are to be made by a designated senior manager, who must be someone who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business of the reporting entity. Updates to the ML/TF risk assessment must be notified in writing to the governing board.

The ML/TF risk assessment is an assessment of the risks of money laundering, financing of terrorism and proliferation financing of a business. The AML/CTF policies must appropriately manage and mitigate those risks, ensuring that the business complies with the AML/CTF Act.



AML/CTF compliance officers

The role and function of an AML/CTF Compliance Officer ('AMLCO') moving to the AML/CTF Act highlights the importance of the role. In summary:

- A business must designate an individual as an AMLCO who is employed or otherwise engaged and be at the management level.
- They must have sufficient authority, independence and access to resources and information to ensure they can perform the functions effectively.
- They must be a resident of Australia (in cases where the business is based in Australia and provides a designated service through a permanent establishment of Australia).
- They must be a fit and proper person.
- They are to fulfil functions that include:
  - overseeing and coordinating the day-to-day compliance with the AML/CTF Act and the effective operation of and compliance with the AML/CTF policies; and
  - communicating with AUSTRAC.

An AMLCO must be designated within 28 days of the business providing a designated service, and AUSTRAC must be notified within 14 days of that designation.

There are civil penalty provisions for failing to meet these requirements

ML/TF/PF risk assessment

Risk assessments are critical in understanding and mitigating an organisation's potential threats relating to ML/TF. Risk assessments undertaken must reflect a business's nature, size and complexity, meaning that the required assessment of larger or more complex businesses will differ to the assessment of smaller businesses.

Risk assessments also need to extend to the risk(s) the business faces from proliferation financing ('PF'). If the assessment of the PF risk is low and it can be appropriately managed by existing AML/CTF policies, businesses will not be required to develop or maintain specific AML/CTF policies to mitigate and manage their PF risk. AUSTRAC's Proliferation Financing in Australia – National Risk Assessment can assist in understanding the PF risks businesses may face.

The matters that need to be considered for a ML/TF risk assessment continue to include: customer types, the types of services provided, how they are delivered, and the countries that a business deals in. The reforms have included an additional matter, being information communicated either directly or indirectly by AUSTRAC that identifies or assesses the risks associated with services provided. The reforms also allow the AUSTRAC CEO to add more matters.

The reforms also mandate reviews of ML/TF risk assessments if there are any significant changes to the above matters. If these triggers do not occur, businesses will be required to undertake a review every three years.

Reviews will be required to be undertaken prior to a significant change that is within the control of the business, for example the introduction of a new designated service, and as soon as practicable for those not in control of the business or involve a communication from AUSTRAC. Updates to the ML/TF risk assessment must be made to address any issues identified, again prior to significant changes for those within control of the business and otherwise as soon as practicable.

There are civil penalty provisions for providing a designated service without undertaking an ML/TF risk assessment, or if businesses have not reviewed and updated it when required.

AML/CTF policies

The reforms bring a requirement for organisations to develop and maintain policies, procedures, systems and controls that achieve both management and mitigation of ML/TF risks, as well as internal compliance management to ensure compliance. These AML/CTF policies must be appropriate to the nature, size and complexity of the business and form part of the AML/CTF Program. There are civil penalty provisions for providing a designated service without meeting these requirements.

The areas of focus will largely include the contents of existing AML/CTF Programs.

Risk management and mitigation policies are to include how businesses:

- identify significant changes that would trigger an ML/TF risk assessment review
- conduct customer due diligence (CDD)
- will review and update AML/CTF policies.

Internal compliance management policies are to include:

- how businesses inform their governing body of their ML/TF risk
- designation of their AML/CTF compliance officer and a senior manager for approving changes to the ML/TF risk assessment and AML/CTF policies
- how businesses undertake employee due diligence and train staff
- how and when they undertake an independent evaluation of their AML/CTF Program.

Businesses are required to comply with their AML/CTF policies. Civil penalty provisions apply for failing to comply with these policies.

AML/CTF responsibilities and governing bodies

A definition of a governing body of a reporting entity has been introduced. If a reporting entity is an individual, the governing body is simply that individual. For all other entities, it is considered to be the individual, or group of individuals, with primary responsibility for the governance and executive decisions of that entity.

Governing bodies will have the responsibility for ongoing oversight of the identification and assessment of risk for the purposes of the ML/TF risk assessment as well as compliance with the AML/CTF policies and AML/CTF Act. They are also tasked with ensuring that the business takes reasonable steps to identify, assess, mitigate and manage ML/TF risks and comply with the AML/CTF policies and the AML/CTF Act. Failing to do so is a civil penalty provision.

Reporting Groups

The current concept of a ‘designated business group’ is to be replaced with a ‘reporting group.’ The composition of a reporting group will be allowed to align with traditional corporate group structures and provide more flexibility by allowing non-reporting entities that fulfil AML/CTF obligations on behalf of other group members to join the group. It is also to extend to non-corporate structures such as groups of partnerships and franchise arrangements.

All reporting groups will require a lead entity. Lead entities of a reporting group must have an AML/CTF Program that is appropriate to the nature, size and complexity of the business of each reporting entity in the reporting group, and those members that are reporting entities must comply with the AML/CTF policies of the lead entity of the reporting group that apply to it.

The lead entity’s AML/CTF policies must include how they will ensure the sharing of information relating to customer due diligence and ML/TF risk, and be subject to information protection safeguards. The AML/CTF policies will also need to include whether any member of the reporting group discharges obligations on any other member, which members the obligations relate to, and the record-keeping requirements that relate to any of the discharged obligations.

There are civil penalty provisions if the policies are not mitigating and managing ML/TF risk, or the policies are not complied with.

Where 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. The intention there is to reduce the risk that reporting groups will be misused to structure out of liability for civil penalty contraventions.

Tipping off

Tipping off is to be streamlined to focus primarily on preventing disclosure of SMR information where it would or could prejudice an investigation. This means that both intentional and reckless disclosures may be considered tipping off. Reckless disclosure may eventuate in a situation where a lead entity of a business group failed to develop policies to prevent tipping off when sharing information within a business group. Certain exceptions to tipping off will continue.

Customer due diligence (CDD)

CDD requirements have changed to make them more outcomes-focussed and in response to the ML/TF risk faced by organisations from customers. To achieve this, the prescriptive 'applicable customer identification procedure' approach is to be replaced by an outcomes-focussed approach that will require organisations to know their customer and understand their ML/TF risk.

Initial CDD would need to be undertaken before providing a designated service to a customer, except in special cases. A civil penalty exists if a designated service is provided before initial CDD is undertaken.

Undertaking initial CDD involves establishing on reasonable grounds:

- the identity of the customer;
- 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;
- if the customer is not an individual—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:
  - a politically exposed person; or
  - a person designated for targeted financial sanctions; and
- the nature and purpose of the business relationship or occasional transaction

To establish reasonable grounds, businesses will have to:

- take reasonable steps to establish that the customer is who they claim to be;
- identify the ML/TF risk of the customer, based on KYC information about the customer that is reasonably available to them before commencing to provide a designated service;
- collect information about the customer appropriate to the ML/TF risk;
- verify the customer information using independent and reliable data that is appropriate to ML/TF risk.

Ongoing CDD will require monitoring of customers to identify, assess, manage and mitigate the ML/TF risks they may reasonably face in providing designated services.

Businesses must monitor for unusual transactions and behaviours of customers that may give rise to a suspicious matter reporting obligation. For customers who are deemed to have a business relationship with the business, they must also:

- review and where appropriate update the identification and assessment of the ML/TF risk of the customer if there is a significant change in the matters required to be used to assess risk, or if there are unusual transactions and behaviours that give rise to a suspicious matter; or
- review, update and reverify KYC information at a frequency appropriate to the customer's ML/TF risk if there are doubts about the adequacy or veracity of KYC information.

In cases of business relationships with pre-commencement customers, businesses must monitor for significant changes in the nature and purpose of the business relationship that may result in the ML/TF risk being medium or high.

There are civil penalty provisions for failing to monitor customers adequately.

Simplified CDD may be used during both initial and ongoing CDD, as long as the ML/TF risk is low and enhanced CDD is not triggered. AUSTRAC is to provide guidance clarifying when ML/TF risk can be determined to be low.

Enhanced CDD must be applied when:

- the ML/TF risk of the customer is high;
- if a suspicious matter reporting obligation arises in relation to the customer and you propose to continue to provide a designated service to the customer;
- the customer is a foreign politically exposed person;
- if the customer is an individual and is physically present in a high risk jurisdiction for which the Financial Action Task Force has called for enhanced due diligence to be applied or a body corporate or legal arrangement that was formed in such a jurisdiction;
- a designated service provided to the customer is provided as part of a nested services relationship.

Key contacts

Alice Saveneh-Murray | Partner

Alice is an experienced leader and trusted advisor to the financial crime risk community. Alice brings deep subject matter expertise and innovative strategies to support client engagements, Boards, and a wide range of industry initiatives. Drawing on her experience in both industry and consulting, she is known for her ability to solve complex regulatory challenges.

+61 3 8623 3433 | alice.murray@kordamentha.com

Rachel Waldren | Partner

Rachel has more than 30 years' experience in both the public and private sectors and has a proven reputation as a leader in the Financial Crime Risk, Compliance, Operational and Regulatory areas. She has worked in major banks as the Global Head of Financial Crime and Anti Money Laundering and Counter Terrorism Financing Compliance Officer. Rachel has been appointed as an AML/CFT expert in high-profile Australian litigation and Royal Commissions, and as an AML/CFT Independent Auditor.

+61 3 8623 3441 | rachel.waldren@kordamentha.com

Grace Mason | Partner

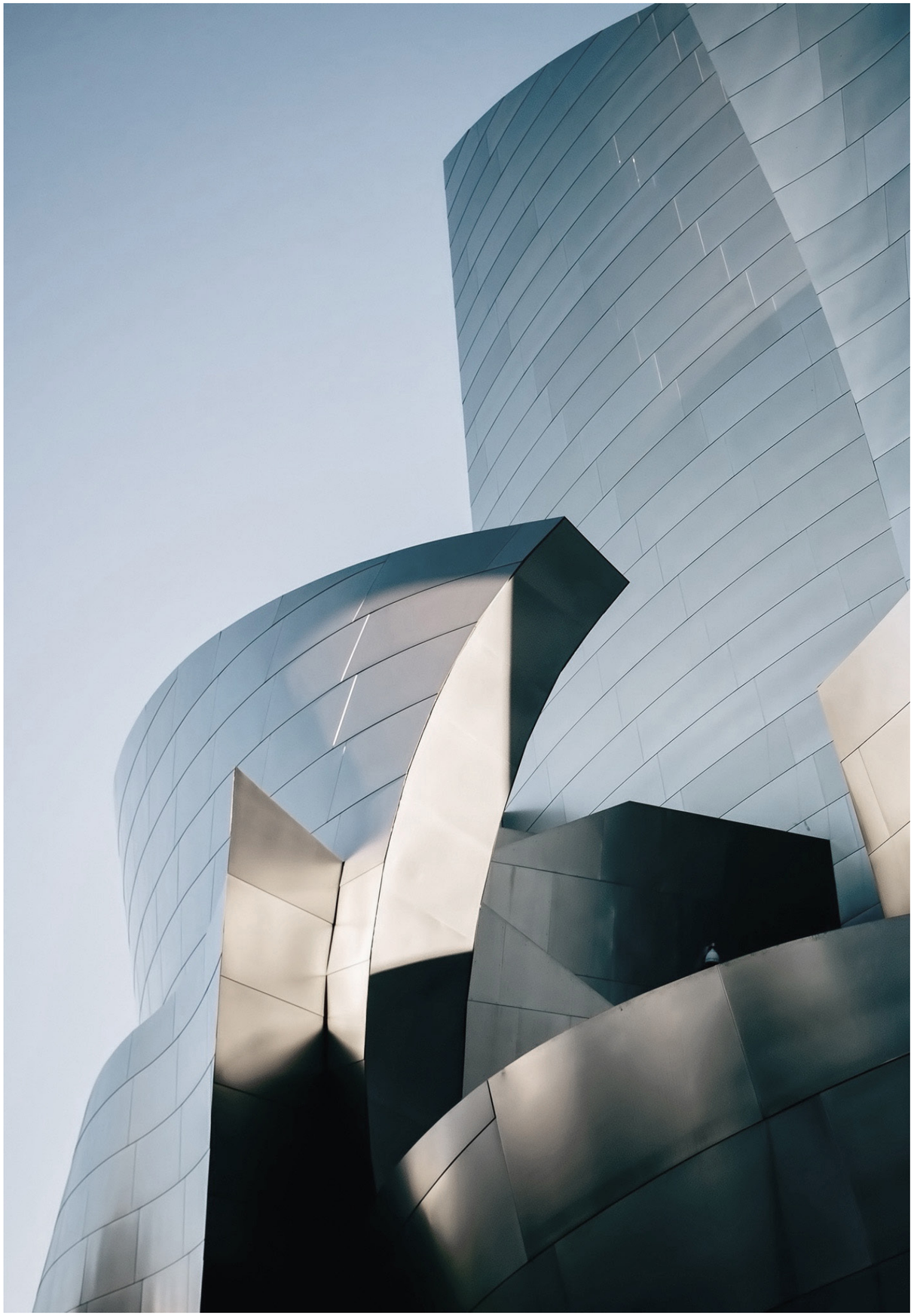
Grace has extensive financial crime experience and has been responsible for driving transformational change and navigating complexity in regulatory, intelligence and policy environments. With over a decade of experience at AUSTRAC, working across AML/CTF regulatory, financial crime and National Intelligence Community capabilities, Grace is a strategic thinker with strengths in communication, engagement, and collaboration.

+61 2 8257 3039 | grace.mason@kordamentha.com

Richard Lee | Executive Director

Richard is a pragmatic and insightful leader, with a broad career in financial crime prevention and detection. He has over 30 years' experience in financial crime regulation and investigation, including executive leadership roles with Australia's AML/CTF regulator, AUSTRAC. He has led teams responsible for enforcement, supervision, and education of a broad range of industry sectors, represented Australia at major international AML forums, and has acted as a financial crime expert on Asia Pacific Group mutual evaluations of member countries.

+61 3 9908 8936 | richard.lee@kordamentha.com



KordaMentha

Contact us

Auckland
+64 9976 4747

Brisbane
+61 7 3338 0222

Canberra
+61 2 6188 9277

Jakarta
+62 21 3972 7000

Melbourne
+61 3 8623 3333

Perth
+61 8 9220 9333

Singapore
+65 6593 9333

Sydney
+61 2 8257 3000

Townsville
+61 7 4724 9888

For more information visit
kordamentha.com