FATF

Anti-money laundering and counter-terrorist financing measures

Australia

4th Follow-Up Report & Technical Compliance Re-Rating

March 2024

Follow-up report

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard.

For more information about the FATF, please visit the website: **www.fatf-gafi.org**

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

The FATF Plenary adopted this report by written process in March 2024.

Citing reference:

FATF (2024), *Anti-money laundering and counter-terrorist financing measures – Australia, 4th Enhanced Follow-up Report,* FATF, Paris
https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Mutualevaluations/australia-fur-2024.html

Photo Credit - Cover: © Getty Images

Australia: 4th Enhanced Follow-up Report

Introduction

The FATF Plenary adopted the mutual evaluation report (MER) of Australia in April 2015[1]. Based on the MER results, Australia was placed into enhanced follow-up. This is Australia's 4th Enhanced Follow-up Report (FUR) with technical compliance re-ratings. This FUR analyses Australia's progress in addressing some of the technical compliance deficiencies identified in its MER. Re-ratings are given where progress has been made.

Overall, the expectation is that countries will have addressed most, if not all, technical compliance deficiencies by the end of the third year from the adoption of their MER. This report does not address what progress Australia has made to improve its effectiveness.

The following experts, supported by Ms. Lisa Kilduff, Policy Analyst from the FATF Secretariat, assessed Australia's request for technical compliance re-ratings:

- **Ms. Wingyiu Yuen**, Supervisor, Central Bank of the Netherlands.
- **Mr**. **Abdelsattar Elnajar**, General Manager, FIU of Egypt.

The second part of this report summarises Australia's progress in improving technical compliance while the third part sets out the conclusion and includes a table showing Australia's MER ratings and updated ratings based on this.

Progress to improve Technical Compliance

This section summarises Australia's progress to improve its technical compliance by addressing some of the technical compliance deficiencies identified in the MER (R.10, R.13, R.17, R.18, R.26).

Progress to address technical compliance deficiencies identified in the MER

Australia has made progress to address the technical compliance deficiencies identified in the MER in relation to Recommendations 10, 13, 17, 18 and 26. Because of this progress, Australia has been re-rated on these Recommendations. However, due to remaining deficiencies under R.2, Australia's rating of LC has been maintained for this Recommendation. Australia has been re-rated PC for Recommendation 15.

[1] www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-australia-2015.html

Recommendation 2

	Year	Rating
MER	**2015**	LC
FUR1	**2016**	LC (not re-assessed)
FUR2	**2017**	LC (not re-assessed)
FUR3	**2018**	LC (not re-assessed)
FUR4	**2023**	**LC**

a) **Criterion 2.1** (*Mostly Met)* The 2015 MER noted deficiencies regarding the lack of a national set of policies and strategies for combating ML/TF informed by the risks identified (See 2015 MER, c.2.1). The Australian Transaction Reports and Analysis Centre (AUSTRAC) is in the process of revising national ML/TF risk assessments, which will inform consideration of the subsequent development of a national AML/CFT strategy. As these changes are not yet in force, some of the shortcomings identified in 2015 remain. However, Australia has demonstrated progress since its previous FUR in 2018. Notably, AUSTRAC has conducted and released 13 Sectoral Risk Assessments (SRAs) and a risk assessment on traveler's cheques since 2018, and several further risk understanding products that were not made public. These were in addition to five SRAs, two regional risk assessments and a risk assessment on remittance corridors from Australia to Pacific Island countries that were completed since Australia's 2015 MER. These assessments examine ML/TF threats and vulnerabilities in specific parts of Australia's financial sector and are the basis for the development of policies and strategies for combating ML/TF. Australia has therefore demonstrated progress under c.2.1, with some deficiencies remaining due to the overarching national AML/CTF strategy being under consideration as of December 2023.

b) **Criterion 2.2** (*Met)* As set out in 2015, the Attorney-General's Department (AGD) is responsible for national AML/CFT policy.

c) **Criterion 2.3** (*Met)* As set out in 2015, Australia has appropriate mechanisms in place to coordinate domestically on AML/CFT policies and activities. Since its MER, Australia has put in place several forums, working groups and task forces to coordinate AML/CFT policy and operational activities.

d) **Criterion 2.4** (*Met)* As set out in 2015, the Department of Foreign Affairs and Trade (DFAT) chairs and services several counter-proliferation coordination groups, both at the senior policy level and working level. These groups bring together all relevant government agencies to share information and coordinate responses to current proliferation issues and meet monthly or at short notice when necessary.

e) **Criterion 2.5** *(Met)* Australia's Privacy Act 1988 is the country's central legislation on data protection and privacy that applies to most government agencies, including AML/CTF competent authorities, and organisations with an annual turnover of more than EUR 1.8 million (AUD 3 million). Subsection 6E(1A) of the Privacy Act specifies that the Privacy Act also applies to a small business (an organisation with annual turnover AUD 3 million or less) that is a reporting entity or an authorised agent of a reporting entity under the AML/CTF Act. This means that businesses that are required to comply with

the AML/CTF Act are also required to comply with the Privacy Act when handling personal information collected for the purposes of, or in connection with, activities or obligations relating to the AML/CTF Act or the AML/CTF Rules.

As per part 11 of the AML/CTF Act, AUSTRAC regulates the access, use and disclosure of AML/CFT information. AUSTRAC's data protection and privacy is regulated by obligations of the Privacy Act and the *Privacy (Australian Government Agencies – Governance) APP Code 2017*. In addition, in line with the privacy procedures undertaken by AUSTRAC, it employs technical, administrative, and physical procedures to protect personal information from misuse, interference and loss, as well as unauthorized access, modification or disclosure pursuant to the Privacy Act. Under section 212 of the AML/CTF Act, in performing the AUSTRAC CEO's functions, the AUSTRAC CEO must consult with the Australian Information Commissioner in relation to matters that relate to privacy functions (within the meaning of the Australian Information Commissioner Act 2010). This oversight function gives the Australian Information Commissioner visibility over the intersections between the Privacy Act and AML/CTF functions. The Privacy Consultative Committee is one of the ways in which the AUSTRAC CEO fulfils their obligations vis-à-vis ensuring compatibility of data privacy and use of data for AML/CFT purposes. Australia has met the requirements of this criterion.

f) **Weighting and conclusion:** Australia ensures the compatibility of AML/CFT requirements with Data Protection and Privacy (DPP) rules through the Privacy Act and the AML/CTF Act and Rules, and has cooperation mechanisms in place to ensure that AUSTRAC and the Australian Information Commissioner align on the handling of data for AML/CFT purposes. While Australia has demonstrated progress in how it identifies ML/TF risks, an overarching national AML/CFT strategy is still under consideration. As such, **Recommendation 2 remains rated Largely Compliant**.

Recommendation 10

	Year	Rating
MER	**2015**	PC
FUR1	**2016**	PC (not re-assessed)
FUR2	**2017**	PC (not re-assessed)
FUR3	**2018**	PC (not re-assessed)
FUR4	**2023**	↑ **LC**

a) **Criterion 10.1** (*Met)* As set out in 2015, Sections 139 and 140 of the AML/CTF Act prohibit the provision of a "designated service", including opening and operating an account as defined under section 6 of the AML/CTF Act, using a false customer name or customer anonymity. The penalty is two years imprisonment and/or 120 penalty units.

b) **Criterion 10.2** (*Mostly Met)* (a – e) The 2015 MER noted that there were exemptions from customer identification regarding: cheques drawn on a customer for less than AUD 5000 or AUD 1000 for cheques funded by cash; transactions below AUD 1000 relating to traveller's cheques (i.e., issuing, cashing or redeeming); and currency exchange below AUD 1 000. However,

these exemptions refer only to a designated service that involves issuing a cheque that an authorised deposit taking institution (ADI), bank or other institution draws on itself, as described in the definition of 'bill of exchange'. This definition explicitly excludes all other types of cheques and means that cheques drawn on a customer are not covered by the exemption and are subject to customer identification as a transaction on an account. This means there is no exemption from CDD for occasional transactions. This deficiency has been addressed. In addition, Australia has undertaken analysis of the use of cheques as part of a broader exercise, and concludes that there has been an almost 90 percent decline in the use of cheques in the last 10 years. The analysis also shows that most reported suspicious activity involving cheques is picked up in conjunction with other designated services that do not have a minimum value of threshold for CDD to be carried out.

c) The 2015 MER noted the absence of a requirement to perform CDD for occasional transactions below the threshold that appear to be linked (*i.e.*, structuring). As in 2015, reporting entities are required to detect structuring, as section 142 of the AML/CTF Act makes it an offence to structure transactions to avoid the reporting threshold (EUR 6 158, AUD 10 000). While this is only relevant in the scope of the reporting obligation of section 43, Chapter 15 of the AML/CTF Rules requires regulated entities to apply their Enhanced Customer Due Diligence (ECDD) programme where a suspicion has arisen for the purposes of section 41 of the Act, including where they have identified that a customer is attempting to structure transactions to avoid reporting thresholds (which is information relevant to investigation of an offence against the AML/CTF Act). Entities must also apply their ECDD programme where they have determined that the ML/TF risk is high, which may include where a customer is structuring their transactions to fit below an exemption threshold. Regarding signatories of FIs in domestic correspondent banking relationships, as in 2015, there is a general exemption in the AML/CTF Rules for the application of CDD. Australia notes that FIs are required to carry out an initial due diligence assessment on the other FI prior to entering into a correspondent banking relationship in line with Chapter 3 of the AML/CTF Rules. The 2015 MER found that the issuance of stored value cards is covered by the AML/CTF Act if the value stored on the card is more than AUD 1000 where whole or part of the monetary value stored on the card may be withdrawn in cash, or AUD 5000 if the value stored cannot be withdrawn in cash. These reloadable cards are not considered an occasional transaction and should therefore require that CDD be applied regardless of any threshold. Australia clarified that if the total value of the card when it issued or reloaded is less than AUD 1000, it is not a designated service and no CDD, ECDD or Suspicious Matter Reporting (SMR) obligations arise in relation to that transaction. As no changes have been made since the MER, the deficiencies under c.10.2(b) remain.

As set out in 2015, there is no threshold for the identification and verification of the identity of the originator of wire transfers, regardless of the nature of the transfer. In the 2015 MER, the fact that Australia does not have any thresholds for wire transfers for CDD was characterised as a deficiency. However, Australia clarified that not having a threshold means CDD applies in all cases not subject to a threshold in line with how Australia was assessed in R.16, particularly c.16.3 rated "Not applicable". The deficiency under

c.10.2(c) has therefore been addressed. As set out in 2015, in case of suspicion of ML/TF, reporting entities are required under Paragraph 15.9 of the AML/CTF Rules to apply enhanced due diligence. Paragraph 15.10 specifies that measures taken in the context of enhanced CDD must be 'appropriate to [the] circumstances', which meets c.10.2(d). In 2015, there was no explicit obligation for reporting entities to conduct CDD when they have doubts about the veracity or adequacy of the previously obtained customer identification data. The *Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2021 (No. 1)* amended Chapter 6 of the AML/CTF Rules to address this deficiency. Part 6.1 of the Rules now specifies that reporting entities must obtain/update and verify know your customer information if they have doubts about the veracity or adequacy of previously obtained know your customer information. The deficiency under c.10.2(e) has therefore been addressed.

d) **Criterion 10.3** (*Met)* The 2015 MER identified shortcomings regarding the lack of direct requirements in legislation to identify and verify the identity of the customer. The *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020* repealed and substituted Section 32 of the AML/CTF Act to impose a direct obligation for regulated entities to identify and verify the identity of the customer. The deficiency under c.10.3 has therefore been addressed.

e) **Criterion 10.4** *(Met)* As set out in 2015, section 89 of the AML/CTF Act specifies that Part B of Financial Institutions' (FIs) AML/CTF programmes must apply to agents purporting to act on behalf of a customer although subject to the FI determining whether and how to apply it in line with risk.

f) **Criterion 10.5** *(Mostly Met)* As set out in 2015, the definition and obligations regarding beneficial owners are largely in line with the FATF Recommendation; however, the exception concerning natural persons, trusts that are registered and subject to regulatory oversight, and companies that are licensed and supervised, is not authorised by the Standard, as it is not completely clear who this applies to and the level and type of supervision that is applied. Australia advised that the decisions regarding trusts that are registered and subject to regulatory oversight and to companies that are licensed and regulated were made considering the existing high-level regulatory oversight, and that both categories of legal entities are low risk. No changes have been made since the MER and the deficiency remains.

g) **Criterion 10.6** *(Met)* The 2015 MER identified deficiencies regarding the use of the word 'enable' in the AML/CTF Rules, as it was deemed that it does not require a reporting entity to understand the nature and purpose of the business relationship. The Rules were accompanied by an Explanatory Statement issued by the AUSTRAC CEO. Explanatory Statements are admissible as evidence under the *Acts Interpretation Act 1901* as to the intention of the Rules. Item 2 of the Explanatory Statement that accompanied the AML/CTF Rules states that the amended text of Paragraph 8.1.5 requires reporting entities to understand the nature and purpose of their business relationships with their customers. The reference to 'customer types' used in this provision seems to deal with customers in general and does not contain

the specific obligation to understand the nature and purpose of the relationship with every single customer. On the contrary, Australia advised that 'customer types' is used in Paragraph 8.1.5 to make it clear to reporting entities that all customers are included in this requirement.

In 2018, the Federal Court of Australia found that the use of the word 'enable' imposes a mandatory and enforceable obligation on reporting entities to comply with the required elements of their AML/CTF programmes, including to understand the nature and purpose of the business relationship. With this clarification, the deficiency has been addressed and the criterion is now met.

h) **Criterion 10.7** *(Mostly Met)* (a – b) The 2015 MER identified deficiencies regarding the lack of guidance given for FIs on how to comply with CDD obligations. For example, there is no express reference to the KYC information and customers' profile. Paragraph 15.3 of the AML/CTF Rules requires reporting entities to undertake reasonable measures to keep, update and review the documents, data or information collected under the applicable customer identification procedures (ACIP) (particularly in relation to high-risk customers) and relating to the beneficial owner. The wording 'reasonable measures' is weaker than that of the criterion, which requires that CDD documents, data or information be kept up-to-date and relevant.

AUSTRAC has since published several guidance materials for FIs to help them in conducting CDD. These materials contain guidance on the required elements of an AML/CFT programme, KYC checks, reliable and independent documentation, debanking, and ongoing customer due diligence. These materials are accessible on AUSTRAC's website. The deficiency regarding lack of guidance for FIs as explanatory material to help them understand how to comply with CDD obligations (regardless of enforceability) has therefore been addressed. Regarding the wording 'reasonable measures', since the 2015 MER, guidance for FIs issued by AUSTRAC elaborates on what 'reasonable measures' implies; however, the wording criticised in the MER remains in the AML/CFT Rules and the deficiency has not been fully addressed.

i) **Criterion 10.8** *(Mostly Met)* The 2015 MER found that, for customers that are legal persons or legal arrangements, there was no explicit requirement in the AML/CTF Rules to understand the nature of their business and their ownership structure. This deficiency has been addressed to some extent and is mostly met because the AML/CTF Rules require reporting entities to understand the nature and purpose of the business relationship with its customer types (paragraph 8.1.5(1)), the control structure (paragraph 8.1.5(2)) and changes to the ML/TF risk arising from changes in the nature of the business relationship, control structure, or beneficial ownership of its customers (paragraph 8.1.5(3)(b)). Additionally, Part 4.12 of the AML/CTF Rules requires reporting entities to determine the beneficial owner of each customer, which includes legal persons and arrangements. The remaining deficiency is that there is no explicit requirement for reporting entities to understand the ownership structure of customers that are legal persons or arrangements, but this would be partly mitigated by the requirements in the AML/CTF Rules to understand the control structure, identify and respond to ML/TF risks arising from changes to the control structure, and to understand

beneficial ownership. With this remaining deficiency, the criterion is mostly met.

j) **Criterion 10.9** *(Mostly Met)* (a – c) As set out in 2015, for customers that are legal persons, not all required elements must be verified, in particular the powers to bind the legal person and, for companies, the names of senior management. The obligation to verify the information gathered does not cover the entire information that is required to be collected by the AML/CTF Rules and is therefore not in compliance with the Standard. However, the AML/CTF programmes must include risk-based systems and controls to determine if the information collected other than that for which the verification is mandatory should be verified. No changes have been made since the MER and the deficiency remains.

k) **Criterion 10.10** *(Met)* (a – c) As set out in 2015, the AML/CTF Rules contain the required measures to meet the sub-criteria (a-c).

l) **Criterion 10.11** *(Met)* (a – b) As set out in 2015, Part 4.4 of the AML/CTF Rules deals with the identification of trusts, and the provisions meet the requirements of the sub-criteria (a-b).

m) **Criterion 10.12** *(Met)* (a – c) The 2015 MER found that there was no applicable obligation in relation to the identity of the beneficiary of a life insurance policy as soon as the beneficiary is identified or designated. Australia notes that the AML/CTF Act and *Insurance Contracts Act 1984* operate to impose obligations in relation to the identity of the beneficiary of a life insurance policy as soon as the beneficiary is designated. Reporting entities that issue, undertake liability as the insurer under a life insurance policy, accept a premium in relation to a life insurance policy or make a payment to a person under a life insurance policy are regulated under the AML/CTF Act (subsection 6(2), Table 1, Items 37, 38 and 39). The Insurance Contracts Act also applies. Where a contract of life insurance is expressed to be for the benefit of a third-party beneficiary (who may be the life insured), the third-party beneficiary has a right to recover from the insurer any money that becomes payable under the contract even though they are not a party to the contract (under section 48A of the Insurance Contracts Act). This means that, at the time the contract of insurance is established, the beneficiary must be identified or designated under the contract, otherwise rights of the beneficiary are not enforceable. Furthermore, as described under c.10.3, the *Anti-Money Laundering* and *Counter-Terrorism Financing and Other Legislation Amendment Act 2020* repealed and substituted Section 32 of the AML/CTF Act to impose a direct obligation for regulated entities to identify and verify the identity of the customer. Therefore, before a pay-out is made on a life insurance policy, the beneficiary (recipient) must be identified and verified by the reporting entity. The deficiency has been addressed and the criterion is met.

n) **Criterion 10.13** *(Met)* As set out in 2015, the beneficiary of a life insurance policy is considered as being the customer of the paying reporting entity, which is required to apply enhanced due diligence to the customer in certain circumstances.

o) **Criterion 10.14/Criterion 10.15**[2] *(Met)* (c.10.14, a – c) While Australia broadly meets the requirements under c.10.14 and c.10.15, the deficiency identified in the 2015 MER concerns exemptions from ACIP. Section 32 of the AML/CTF Act prohibits the provision of financial services if the financial institution has not carried out the ACIP. This prohibition does not apply to existing customers (section 28), in case of 'low risk designated services' (section 30) and in the circumstances of Chapter 46 of the AML/CTF Act dealing with the acquisition or disposition of a security or a derivative or a foreign exchange contract (section 33). The AML/CTF Rules do not list any low-risk designated service and no designated services have been listed as 'low risk' since the enactment of the AML/CTF Act in 2006.

Australia has reiterated that the provisions under section 30 of the AML/CTF Act to exempt low risk customers remain unused. ACIP is required for all designated services under the Act unless an exemption is provided. Section 30 of the Act gives the AUSTRAC CEO the power to make Rules to specify a designated service as low risk, which would exempt the service from ACIP; while this power exists, there is no obligation for the AUSTRAC CEO to make such Rules. No such Rules have been made, meaning no exemption has ever been in effect. The deficiency has therefore been addressed.

p) **Criterion 10.16** *(Met)* The 2015 MER identified deficiencies regarding how FIs apply CDD requirements to existing customers. It found that the mechanism did not seem to consider the risk presented by the customer and its objective focuses on the identity of the customer (i.e., it does not cover beneficial owner or the functioning of the account). Moreover, it did not seem to be fully consistent as the trigger event would most likely be a transaction (that raises suspicion), while the objective and measures to take deal with the identification of the customer.

Following amendments to the AML/CTF Rules, initial, on-going and enhanced due diligence obligations must now take into account the ML/TF risk presented by the customer, including beneficial owners, and the functioning of the customer's account. These apply to existing and pre-commencement customers. Part 4.1 of the AML/CTF Rules requires a reporting entity to consider various factors when identifying its ML/TF risk including its customers (beneficial owners of customers), its customers' sources of funds and wealth, the control structure of its non-individual customers, among others. Part 15 of the AML/CTF Rules requires a reporting entity to perform ongoing due diligence on customers based on risk-based systems and controls as included in the AML/CTF programme. It refers to the KYC information and beneficial owner information specified in Part 4, which need to be updated and reviewed. The identified deficiencies have been addressed and the criterion is met.

q) **Criterion 10.17** *(Met)* As set out in 2015, the AML/CTF Rules provide for the enhanced CDD programme and measures to implement when the reporting entity determines that the ML/TF risk is high, when the customer is a foreign

[2] Please note that c.10.14 and c.10.15 were assessed jointly in the MER and will therefore be re-assessed jointly in this FUR.

PEP, when a suspicion has arisen, or when the customer is located in a prescribed foreign country.

r) **Criterion 10.18** *(Partly Met)* As set out in 2015, the application of simplified measures to companies that are licensed and supervised is not justified nor authorised under the FATF Standards. Pursuant to Paragraph 4.4.8 of the AML/CTF Rules, simplified verification procedures may apply to trusts that are managed investment schemes registered by the Australian Securities and Investments Commission (ASIC), managed investment schemes that are not registered by ASIC under specific conditions, trusts registered and subject to the regulatory oversight of a Commonwealth statutory regulator, or a government superannuation fund established by legislation. Australia has not established that these cases have been identified through risk analysis. No changes have been made since the MER and the deficiency remains.

s) **Criterion 10.19** *(Met)* (a – b) The 2015 MER found that, where a financial institution is unable to comply with the relevant CDD measures, there is no requirement to not open the account/terminate the business relationship, or consider filing an SMR. If a reporting entity suspects on reasonable grounds that a customer is not the person who he/she/it claims to be, including because the reporting entity is not able to comply with the CDD measures, the reporting entity must file an SMR pursuant to subsections 41(1)(d) and (e) of the AML/CTF Act. This deficiency has been addressed by Section 32 of the AML/CTF Act, which specifies that a reporting entity must not commence the provision of a designated service to a customer unless it has carried out the relevant CDD measures. The criterion is met.

t) **Criterion 10.20** *(Mostly Met)* The 2015 MER found that there was no provision permitting FIs to not pursue the CDD process where there is a risk of tipping off, or requiring them to file an SMR in those cases (apart from the regular SMR obligation). While the AML/CTF Rules now clarify that a reporting entity is not required to take any measures that would contravene the tipping off offence in section 123 of the Act when carrying out verification of identity, there is no explicit provision requiring them to file an SMR in those cases. Although progress has been made, the deficiency has not been fully addressed and the criterion is mostly met.

u) **Weighting and conclusion**: Amendments to the AML/CTF Act after Australia's 2015 MER mean that there is a clear obligation for FIs to carry out ACIP before commencement of provision of a designated service, the lack of which previously was weighted heavily as a basic CDD obligation. A 2018 Federal Court of Australia ruling clarified that the use of the word 'enable' imposes a mandatory and enforceable obligation on reporting entities to comply with the required elements of their AML/CTF programmes, including to understand the nature and purpose of the business relationship. Australia has demonstrated that, before a payout is made on a life insurance policy, the beneficiary (recipient) must be identified and verified by the reporting entity, and amendments to the AML/CTF Rules mean that initial, ongoing, and enhanced due diligence obligations must now consider the ML/TF risk presented by the customer, including beneficial owners. The deficiency regarding lack of guidance for FIs has been rectified. Lastly, the AML/CTF

Rules now clarify that a reporting entity is not required to take any measures that would contravene the tipping off offence.

However, some deficiencies remain. Some exemptions to the application of CDD remain, notably regarding signatories of FIs in domestic correspondent banking relationships, reloadable stored value cards operating at a threshold and on occasional transactions below a threshold which appear linked. While guidance has helped clarify what is meant by 'reasonable measures' under c.10.7 regarding requirements for CDD documents, the wording remains, which was deemed weaker than that of the requirements under c.10.7 and the deficiency has not been fully addressed. There is no explicit provision requiring FIs to file an SMR in cases where they are unable to pursue the CDD process due to a risk of tipping off. Regarding the obligation for FIs to identify the beneficial owner, the exception concerning natural persons, trusts that are registered and subject to regulatory oversight, and companies that are licensed and supervised, remains. The 2015 MER concluded that this is a minor deficiency because these entities are already subject to regulatory oversight and these categories are considered low risk, and this continues to be the case. There is no explicit requirement for reporting entities to understand the ownership structure of customers that are legal persons or arrangements, although this would be partly mitigated by the requirement for FIs to understand the control structure. The obligation to verify the information gathered does not cover the entire information that is required to be collected by the AML/CTF Rules. The application of simplified measures to companies that are licensed and supervised is not justified nor authorised under the FATF Standards. Australia has made progress in ten out of the fourteen criteria that were not fully addressed at the time of the MER and has made significant progress in some areas, including the provision to conduct ACIP before providing a designated service. Considering this progress and the remaining deficiencies, **Recommendation 10 is re-rated Largely Compliant.**

Recommendation 13

	Year	Rating
MER	**2015**	NC
FUR1	**2016**	NC (not re-assessed)
FUR2	**2017**	NC (not re-assessed)
FUR3	**2018**	NC (not re-assessed)
FUR4	**2023**	↑ **C**

a) **Criterion 13.1** *(Met)* (a – d) The 2015 MER identified several deficiencies concerning the sub-criteria. For c.13.1(a), the information that reporting entities were required to gather and verify in the context of a correspondent banking relationship was insufficient as information on the AML/CTF regulation applicable to the correspondent bank. The information on the adequacy of its internal controls was questioned, and information on the ownership, etc. was gathered in the due diligence assessment, which a financial institution could conduct (or not) based upon the risk. Amendments made to the AML/CTF Act have rectified this deficiency. Section 96 requires FIs to carry out a due diligence assessment before entering a correspondent

banking relationship. The required information about a respondent institution is gathered to assess the ML/TF risks associated with entry into that correspondent banking relationship and covers all information in line with the requirements under c.13.1(a).

Under c.13.1(b), the MER notes that there was no reference to ML/TF supervision conducted in the country of the correspondent institution. Following the amendments mentioned previously to the AML/CTF Act, the AML/CTF Rules were also amended and now set out factors that must be considered when assessing risks when entering a correspondent banking relationship. This includes a reference to the existence and quality of any AML/CTF regulation and supervision in the country or countries where the respondent or any ultimate parent company operates, and the respondent's compliance practices in relation to those regulations. The amendments ensure that FIs must assess the adequacy and effectiveness of the respondent's AML/CTF systems and controls (para. 3.1.3). The deficiency under c.13.1(b) has been sufficiently addressed.

Under subsection 96(1) of the AML/CTF Act, a senior officer must approve entry into a correspondent banking relationship having regard to a range of matters specified in the AML/CTF Rules (c.13.1(c)). Regarding c.13.1(d), the MER found that there was no indication on the need to understand the respective AML/CFT responsibilities of each institution. The AML/CTF Rules were amended to ensure that FIs clearly understand their respective responsibilities in the correspondent banking relationship through subsection 96(2) which requires that, when a financial institution establishes a correspondent banking relationship with another financial institution, a written record setting out the responsibilities of both parties must be prepared within 20 business days of entering into the relationship. The deficiencies under c.13.1 have been addressed and the criterion is now met.

b) **Criterion 13.2** *(Met)* (a – b) The 2015 MER concluded that there was no requirement with respect to payable-through accounts, although AUSTRAC had previously issued guidance to assist FIs in implementing their obligations in relation to correspondent banking relationships, which provides an example of a payable-through account. Following amendments, the AML/CTF Rules provide that, where the correspondent maintains payable-through accounts, the correspondent must consider as part of the due diligence whether the respondent: conducts CDD and ongoing due diligence on those customers of payable-through accounts, and; is able to provide to the correspondent, on request, the documents, data or other information obtained when conducting CDD and ongoing CDD in relation to those customers (para.3.1.3(7)). Furthermore, under paragraph 3.1.5 of the AML/CTF Rules, if the correspondent maintains payable-through accounts, when approving entry into the correspondent banking relationship, the senior officer must be satisfied that the respondent: verifies the identify of, and conducts ongoing CDD in relation to, customers before they have access to those accounts, and; is able to provide the correspondent, on request, the documents, data, or other information obtained when conducting CDD and ongoing CDD in relation to the customers that have access to those accounts. The deficiency has been addressed and c.13.2 is now met.

c) **Criterion 13.3** *(Met)* The 2015 MER found that FIs are prohibited from entering into a correspondent banking relationship with a shell bank, or with another FI that has a correspondent banking relationship with a shell bank. However, it was unclear whether the prohibition extended to entering into a correspondent banking relationship with a financial institution that did not currently have a correspondent banking relationship with a shell bank but would theoretically be permitted to engage in such a relationship in the future. The provisions in the AML/CTF Act now include the prohibition to continue a correspondent banking relationship if a financial institution becomes aware that a correspondent banking relationship involves a shell bank after entering a relationship. The deficiency has therefore been addressed and the criterion is now met.

d) **Weighting and conclusion:** Australia has taken steps to ensure compliance with Recommendation 13, in particular through amendments made to the AML/CTF Act and AML/CTF Rules to strengthen CDD provisions for FIs vis-à-vis correspondent banking. **Recommendation 13 is re-rated Compliant**.

Recommendation 15

	Year	Rating
MER	**2015**	LC
FUR1	**2016**	LC (not re-assessed)
FUR2	**2017**	LC (not re-assessed)
FUR3	**2018**	**↑ C**
FUR4	**2023**	**↓ PC**

a) **Criterion 15.1/Criterion 15.2**[3] *(Met)* (c.15.2, a – b) Amendments made to the AML/CTF Rules in 2018 to subparagraph 8.1.5(a) of Chapter 8 and subparagraph 9.1.5(a) of Chapter 9 made the identification, mitigation and management of ML/TF risk a general requirement in respect to new designated services, new methods of delivering designated services, new technologies and changes (See 2018 FUR).

b) **Criterion 15.3** *(Partly Met)* (a – c) Australia has developed various products to identify and assess ML/TF risks emerging from virtual asset activities and virtual asset services providers (VASPs) to some extent. There is a scope deficiency that affects several criteria under R.15: Australia has regulated digital currency exchange (DCE) providers for AML/CFT purposes that carry out exchange between virtual currencies and fiat currencies, but does not extend obligations to the other activities covered by the FATF Standards[4].

[3] Please note that c.15.1 and c.15.2 were assessed jointly in Australia's previous FUR and are therefore assessed jointly in this FUR.

[4] Activities included in the FATF Standards: exchange between virtual currencies and fiat currencies; exchange between one or more forms of virtual assets; transfer of virtual assets; safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; or participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset. Australia is working on proposed legislative reforms to expand the scope of AML/CTF regulation of DCEs to align with the requirements under R.15.

During 2022-23, AUSTRAC produced four strategic analysis products relating to digital currencies and DCEs, which were classified and disseminated to domestic partner agencies. Two of the reports were sanitised and disseminated to select partner FIUs. In September 2022, AUSTRAC produced a regulatory insights assessment identifying business models operating in the global cryptocurrency industry to map them against the regulated DCE population operating in Australia to understand the AML/CTF compliance risks and vulnerabilities of the different models. While AUSTRAC has also issued some guidance for regulated businesses to identify ML/TF risks, it has not yet identified the risk rating of the overall ML/TF risks emerging from virtual assets activities and VASPs (c.15.3(a)).

To ensure greater regulatory focus on high and emerging risks, a new Branch structure was adopted by Regulatory Operations, AUSTRAC in July 2023. The branch includes dedicated teams to target domestic banks, casinos, remitters, DCEs, payment platforms, and bullion dealers. Teams were grouped based on shared characteristics in each sector to ensure that decision making, actions and interactions with partners are consistent and aligned. This grouping has resulted in four sector-based supervisory streams. To assist in strengthening reporting entities' compliance with AML/CTF obligations, the AUSTRAC CEO is empowered to make decisions regarding the registration of remittance service providers and DCE providers. The primary considerations associated with the CEO decisions focus upon whether registration would involve a significant ML/TF or serious crime risk. Between 1 July 2023 and 31 October 2023, AUSTRAC issued five registration refusals, nine registration suspensions and one registration cancellation. Six of these decisions related to DCEs and nine to remittance services. Despite these actions, the scope gap for covered activities under R.15 means that it is difficult to determine to what extent Australia applies a risk-based approach to VASPs and virtual asset activity (c.15.3(b)). DCE providers that carry out the activity of exchanging between virtual currencies and fiat currencies are required, according to Paragraphs 8.1.5 and 9.1.5 of the AML/CTF rules and subsection 84(2) of the AML/CTF Act, to identify, assess, manage, and mitigate ML/TF risks (c.15.3(c)).

c) **Criterion 15.4** *(Partly Met)* (a – b) Under section 76A of the AML/CTF Act, DCEs must not provide designated services related to digital currency exchange unless they are registered with AUSTRAC. The AUSTRAC CEO is required to maintain a Digital Currency Exchange Register, and DCEs are required to register with AUSTRAC whether an individual resident or established in Australia, in line with c.15.4(a). There are measures to prevent criminals or their associates from holding or being the beneficial owners or controlling interest or holding management function in DCEs, which include criminal checks, but not covering all activities of VASPs as outlined under c.15.3 (c.15.4(b)).

d) **Criterion 15.5** *(Met)* AUSTRAC identifies unregistered activity from a range of sources, including analysis of suspicious matter reports (SMRs), tip-offs from other providers, the general public, and from data analysis. Australia has

both criminal sanctions and civil penalties under the AML/CTF Act for unregistered DCE activity, which is both a criminal offence and a civil penalty provision, allowing a range of proportionate sanctions to be applied. Subsections 76A(3) to (10) of the AML/CTF Act prescribe the applicable criminal sanctions for carrying out registerable DCE activities without registering. The minimum penalties are: minimum of 500 penalty units (from 1 July 2023, a penalty unit is EUR 190 (AUD 313), making the minimum financial sanction EUR 94 900 (AUD 156 500)); and/or minimum 2 years imprisonment. Section 76A(11) also makes 76A(1) and (2) both civil penalty provisions, where the civil penalty regime also applies. A civil penalty is a Court imposed pecuniary penalty payable to the Commonwealth as part of civil proceedings. During 2022-23, AUSTRAC investigated eight matters relating to potential unregistered DCE activity. These matters were sourced from internal referrals within AUSTRAC, from the public via the AUSTRAC Contact Centre and from partner agencies. A range of actions were taken as a result, including engagement with entities to request further information on potential unregistered DCE services, the issuance of warning letters to cease and desist providing unregistered DCE services and the monitoring of an entity while it was under external administration. AUSTRAC also applies ongoing scrutiny of financial activity conducted by higher-risk entities who have withdrawn their registration applications after being unable to demonstrate a practical understanding of their AML/CTF obligations or who are of interest for involvement in ML/TF and serious financial crime activity. AUSTRAC has shared the results of this post-registration monitoring of withdrawn DCE and remittance applications with partner agencies and has engaged with three entities who had previously applied for DCE registration, and which were identified in financial transaction activity indicating provision of unregistered DCE services. As such, this criterion is met.

e) **Criterion 15.6** *(Met)* (a – b) AUSTRAC supervises DCEs in accordance with the functions of the AUSTRAC CEO under section 190 of the AML/CTF Act, which requires the AUSTRAC CEO to monitor compliance by reporting entities with their obligations under the AML/CTF Act (c.15.6(a)). Under the AML/CTF Act, AUSTRAC has adequate powers to supervise VASPs and monitor their compliance with ML/TF requirements and has the authority to conduct inspections, compel the production of information and impose a range of disciplinary and financial sanctions, including the power to withdraw, restrict or suspend the VASP's license or registration, where applicable (c.15.6(b)). This criterion is met.

f) **Criterion 15.7** *(Met)* AUSTRAC has issued specific guidance to DCEs including on how to register and how to prepare and implement an AML/CFT programme. AUSTRAC has worked with members of the Fintel Alliance to develop a Criminal Abuse of Digital Currencies Financial Crime Guide and brings together six DCE providers and eight law enforcements partners through the Fintel Alliance Virtual Assets working group (VAWG). The VAWG focuses on trends, methodologies, and observations in the virtual assets sector. In December 2023, AUSTRAC's Fintel Alliance released a new threat alert about the financial crime risks of money mules. This was developed in consultation with the VAWG participants and has been shared with the DCE sector, Fintel Alliance partners, and across government partners. AUSTRAC

has also created a risk management methodology fact sheet specifically for DCE providers. These are accompanied by broader guidance in the AUSTRAC Compliance Guide on CDD, reporting, record keeping and the risk-based approach. Regarding specific feedback, AUSTRAC provides feedback on SMRs to DCEs as part of compliance assessments and ongoing regulatory engagement and delivered webinars when DCEs were brought into the regime. Criterion 15.7 is met.

g) **Criterion 15.8** *(Partly Met)* (a – b) DCEs are reporting entities, which means that they are subject to the available sanctions applied to all reporting entities for breaches of AML/CTF obligations under the AML/CTF Act and Rules. Sanctions available to AUSTRAC that refer specifically to DCE services include: a range of civil and criminal sanctions under section 76A of the AML/CTF Act for providing DCE services without registering with AUSTRAC or breaching a condition of registration as a DCE; civil penalties under section 76P of the AML/CTF Act for failing to notify AUSTRAC of changes in circumstances that could affect the person's registration, and; administrative sanctions as identified under c.15.6(b), where the AUSTRAC CEO has powers to impose conditions on, suspend and cancel a person's registration. However, the scope deficiency applies here (c.15.8(a)). Under section 174 of the AML/CTF Act, civil penalties apply to individuals who are, directly or indirectly, knowingly concerned in a reporting entity's contravention of a civil penalty provision. This provision applies in relation to directors or senior managers (c.15.8(b)). Criterion 15.8 is partly met due to the deficiency regarding the gaps in coverage of VASP activity.

h) **Criterion 15.9** *(Partly Met)* (a – b) As DCEs are reporting entities, they are subject to the same compliance requirements as all reporting entities under the AML/CTF Act and Rules. The AML/CTF obligations and deficiencies under R.10-21 apply similarly, and the scope gap concerning VASP activity applies here (c.15.9(a)). The shortcomings are considered moderate on the basis that Australia complies or largely complies overall with R.10-21, and while the scope gap applies, DCEs represent the most material sector in terms of VASP activity. The requirements of c.15.9(b) are not met. Australia notes that these matters are being considered as part of upcoming legislative reform.

i) **Criterion 15.10** *(Met)* All persons subject to Australian jurisdiction, including reporting entities, are subject to Australian sanctions laws, including those implementing targeted financial sanctions (TFS). TFS obligations under Australian law apply to all natural and legal persons and therefore apply to all VASPs, including those that are not considered under the definition of a DCE. Australia was rated compliant with Recommendations 6 and 7 in its MER and meets the requirements outlined under c.15.10. This criterion is met.

j) **Criterion 15.11** *(Met)* AUSTRAC can provide a wide range of international cooperation, including exchanging AUSTRAC information[5]. This is broadly

[5] AUSTRAC information is broadly defined under section 5 of the AML/CTF Act to include all information obtained or generated by AUSTRAC for the purposes of the AML/CTF Act, under any law of the Commonwealth, State or Territory or from another government body, and

defined under section 5 of the AML/CTF Act to include all information obtained or generated by AUSTRAC for the purposes of the AML/CTF Act, under any law of the Commonwealth, State or Territory or from another government body, and includes information obtained or generated relating to money laundering, predicate offences, and terrorist financing relating to virtual assets. Section 127 of the AML/CTF Act provides that the AUSTRAC CEO can disclose AUSTRAC information to the government of a foreign country or a foreign agency if the CEO is satisfied that, where appropriate, the government of the foreign country or the foreign agency has given an undertaking regarding the confidentiality, use and disclosure of the information and that it is appropriate in the circumstances to share the information. AUSTRAC can share information with any foreign agency and is not limited to sharing with other FIUs or AML/CTF supervisors, or by differences in the nomenclature or status of VASPs (AML/CTF Act, division 5, part 11,). For other competent authorities, the measures in place in the 2015 MER Australia for international cooperation apply to virtual assets. Australia was rated compliant with R.37-40. Criterion 15.11 is met.

k) **Weighting and conclusion:** AUSTRAC identifies unregistered VASP activity from a range of sources and there are a range of appropriate sanctions that can, and have been applied, although they do not apply to all activities covered by the FATF Standards. AUSTRAC has issued specific guidance to DCEs and brings together DCE providers and law enforcements partners through the VAWG. Australia ensures that communication mechanisms, reporting obligations and monitoring referred to under elements of R.6/7 apply to DCEs, and AUSTRAC can provide a wide range of international cooperation, including exchanging AUSTRAC information. However, some deficiencies remain. As noted in the analysis, there is a scope gap that affects several criteria under R.15, as Australia has regulated DCE providers for AML/CTF purposes that carry out exchange between virtual currencies and fiat currencies but does not extend obligations to the other activities covered by the FATF Standards. DCEs are required to register with AUSTRAC and there are measures to prevent criminals or their associates from holding or being the beneficial owners or controlling interest or holding management function in DCEs, which include criminal checks, but not covering all activities of VASPs. Neither the AML/CTF Act or Rules specify that originating VASPs must obtain and hold originator and beneficiary information, including on virtual asset transfers. There are no obligations for VASPs regarding the requirements of R.16, or for sending virtual asset transfers on behalf of a customer, although these deficiencies will be addressed through upcoming legislation. Considering the scope gap in coverage of VASP activity and the identified deficiencies, **Recommendation 15 is re-rated Partially Compliant.**

includes information obtained or generated relating to money laundering, predicate offences, and terrorist financing relating to virtual assets.

Recommendation 17

	Year	Rating
MER	**2015**	PC
FUR1	**2016**	PC (not re-assessed)
FUR2	**2017**	PC (not re-assessed)
FUR3	**2018**	PC (not re-assessed)
FUR4	**2023**	↑ **C**

a) **Criterion 17.1** *(Met)* (a – c) The 2015 MER found that it was not explicitly stated that the reporting entity relying on a third party remains ultimately responsible for CDD measures. When the reporting entity relying on a third party is a financial adviser or reporting entity belonging to the same Designated Business Group (DBG) as the third party, Chapter 7 of the AML/CTF Rules requires that the reporting entity relying on a third party has obtained a copy of the record made by the third party, or has access to it and has determined that it is appropriate to rely on the ACIP carried out by the third party having regard to the ML/TF risk. There was no obligation in relation to the regulation and supervision of the third party located abroad or on the existence of measures in line with Recommendations 10 and 11 for the third parties located abroad and regulated by foreign laws.

Amendments to the AML/CTF Act and AML/CTF Rules have addressed this deficiency. The ultimate responsibility for CDD measures of the reporting entity relying on a third party follows from Section 38 of the AML/CTF Act and the Explanatory Memorandum to the Amendment Bill. The reporting entity is responsible and liable for any failure of carrying out CDD measures. The obligation regarding the regulation and supervision of the third party located abroad or on the existence of measures, in line with Recommendations 10 and 11, is included in the AML/CTF Rules. Pursuant to paragraph 7.2.2(3)(b), a third party being a foreign entity must be regulated by one or more laws of a foreign country giving effect to the FATF Recommendations relating to CDD and record keeping (equivalent CDD and record keeping obligations). Paragraph 7.2.2(5) states that the foreign entity must also have measures in place to comply with the equivalent CDD and record keeping obligations. The deficiencies have been addressed and the criterion is met.

b) **Criterion 17.2** *(Met)* The 2015 MER found that Australia had not demonstrated that the ML/TF risk presented by New Zealand FIs was considered when the declaration expanding the scope of third parties to New Zealand FIs was issued. The Declaration of 16 March 2009 made it the responsibility of the reporting entity "to ascertain that under its risk-based procedure that the relevant ACIP has been carried out under an AML/CTF regime, which is comparable to the Australian AML/CTF Act". The AML/CTF Rules were amended in 2021 to require that the level of country risk be considered as part of determining which countries third parties can be based for reliance purposes. Whether third party reliance is on a case-by-case basis or under a written agreement or arrangement, the Rules require the reporting entity to consider the level of ML/TF or other serious crime risks in the country or countries (including New Zealand) in which the third party operates or resides (paragraphs 7.3.2 and 7.3.3, and subparagraph

7.2.2(2)(c), Rules). The deficiency has been addressed and the criterion is met.

c) **Criterion 17.3** *(Met)* (a – c) At the time of the 2015 MER, reliance on third parties was limited to those located in Australia and on the subsidiaries of Australian reporting entities located abroad, as mentioned previously. The Rules were amended in 2021 to expand reliance on third parties within designated business groups to include those located abroad. Paragraph 7.3.5 of the Rules specifies conditions that must be met for a reporting entity to rely on CDD carried out by another person who is a member of the same corporate group or designated business group. These include: the reporting entity and other person apply and implement a joint AML/CTF program or other group-wide measures relating to CDD and record keeping; any higher ML/TF or serious crime risks in the country or countries in which the other person operates or resides are adequately identified, mitigated and managed by the joint AML/CTF program and risk-based systems and controls of the corporate group or designated business group; the implementation of the risk based system and controls are supervised and monitored at a group level. The deficiency has been addressed and the criterion is met.

d) **Weighting and conclusion:** Amendments to the AML/CTF Act and the AML/CTF Rules mean that FIs now have clear requirements regarding reliance on third-party FIs for CDD, and the level of country risk must be considered as part of determining in which countries third parties can be based for reliance purposes. Australia has expanded reliance on third parties within designated business groups to include those located abroad and amended the AML/CTF Rules accordingly. The deficiencies identified in 2015 have therefore been addressed and **Recommendation 17 is re-rated Compliant.**

Recommendation 18

	Year	Rating
MER	**2015**	PC
FUR1	**2016**	PC (not re-assessed)
FUR2	**2017**	PC (not re-assessed)
FUR3	**2018**	PC (not re-assessed)
FUR4	**2023**	↑ **LC**

a) **Criterion 18.1** *(Met)* (a – d) The 2015 MER identified several deficiencies under c.18.1, including few obligations for compliance management arrangements at the group or reporting entity level beyond the nomination of a compliance officer, and that the role and functions of the compliance officer were not detailed (c.18.1(a)). The MER found that screening may be conducted in case of transfer or promotion of an employee, but that screening of potential employees was based on risk, so it may not be performed (c.18.1(b)). While an AML/CTF programme must include a risk awareness training programme, the 2015 MER found that the wording around the objective of the training programme, 'to enable employees to understand' AML/CTF obligations, was weaker than requiring that the employee understands the obligations (c.18.1(c)). The 2015 MER identified deficiencies

regarding c.18.1(d), namely that AML/CTF programmes must be subject to a regular independent review by an internal or external party. However, there were no indications as to the frequency of the "regular" review, or how to guarantee the independence of an internal audit.

Regarding c.18.1(a), AUSTRAC published guidance in 2019 to provide further detail on the authority and resources a compliance officer should have to carry out their responsibilities effectively. It states that an AML/CTF compliance officer is expected to have overall responsibility for the operation of the AML/CTF programme, and provides further examples of duties they may perform. The guidance specifies how the role of compliance officer should be fulfilled for DBGs. As amended in the Anti-Money Laundering and Counter-Terrorism Financing Rules Amendment Instrument 2018 (No.1), Part 8.7.1 of the AML/CTF Rules requires that reporting entities must take into account any applicable guidance material disseminated or published by AUSTRAC and any feedback provided by AUSTRAC in respect of the reporting entity or the industry it operates in that is relevant to the identification, mitigation, and management of ML/TF risk arising from the provision of a designated service by that entity. If a reporting entity fails to comply with paragraph 8.7.1 of the AML/CTF Rules by not taking into account guidance disseminated or published by AUSTRAC and/or any feedback provided in respect of the reporting entity, or its industry, as required by section 84(2)(c) of the AML/CTF Act, the conduct of the reporting entity could constitute a breach of the requirements to adopt and maintain an AML/CTF programme (section 81(1)) and the reporting entity could be subject to a civil penalty. As such, the deficiencies under c.18.1(a) have been addressed.

Regarding employee screening, AUSTRAC also published guidance in 2019 (updated in 2023) that outlines which employees to screen and re-screen, and how to conduct such screening. The guidance advises that it is best practice to screen and re-screen all employees but to focus particular attention for more rigorous screening for high-risk roles. The guidance supplements Parts 8.3 and 9.3 of the AML/CTF Rules, which require implementation of employee due diligence programmes to screen prospective employees who, if employed, may be able to facilitate commission of a ML/TF offence connected with the provision of a designated service. Each employee in such a position is screened in the first instance to understand the level of risk that may be posed, and the frequency and process of screening and re-screening such employees, at all levels, is based on the reporting entity's risk assessment. The deficiency under c.18.1(b) has been resolved. Regarding c.18.1(c), AUSTRAC published guidance (revised in 2023) regarding employee AML/CTF risk awareness training, which states that employees who work in roles that pose ML/TF risk must be provided training 'to ensure they understand' obligations under the AML/CTF Act and Rules, amongst other elements. The guidance constitutes enforceable means, as set out in the analysis for c.18.1(a). The deficiency under c.18.1(c) has therefore been addressed.

Lastly, amendments to the AML/CTF Rules have strengthened the requirements for independent review of standard and joint AML/CTF programmes. Notably, paragraphs 8.6.1 and 9.6.1 of the Rules state that Part A of a reporting entity's AML/CTF programme must be subject to regular independent review. The purpose of this review, as outlined in paragraphs 8.6.5 and 9.6.5, is to assess: the effectiveness of an AML/CTF programme with

regard to the ML/TF risk of the reporting entity; the AML/CTF programme's compliance with the AML/CTF Rules; the effectiveness the AML/CTF programme's implementation, and; the compliance of the reporting entity with its AML/CTF programme. Paragraphs 8.6.2 and 9.6.2 stipulate how the frequency of the review should be determined. Paragraphs 8.6.3 and 9.6.3 state that while the review may be carried out by either an internal or external party, the person appointed to conduct the review must not have been involved in undertaking any of the functions or measures being reviewed, including the design, implementation, or maintenance of Part A of a reporting entity's AML/CTF programme or the development of a reporting entity's risk assessment or related internal controls. Paragraphs 8.6.4 and 9.6.4 require that the reporting entity or designated business group must be able to demonstrate the independence of the reviewer. In 2019, AUSTRAC published guidance to provide further clarity for reporting entities regarding regular and independent reviews of AML/CTF programmes. The deficiency under c.18.1(d) has been addressed and criterion 18.1 is met.

b) **Criterion 18.2** *(Mostly Met)* (a – c) Regarding c.18.2(a), the 2015 MER found that the AML/CTF Act allows any member of a DBG to discharge certain obligations on behalf of other members. Subsection 123(7AB) of the AML/CTF Act is an exception to the tipping-off prohibition as it allows a member of a DBG with a joint AML/CTF programme to disclose information about one of its customers to another reporting entity within that DBG, in order to inform the other reporting entity about the risks involved in dealing with the customer (the same applies to corporate groups under subsection 123(7)). Regarding c.18.2(b), the 2015 MER identified deficiencies regarding obligations for DBGs. While Section 207(3) of the AML/CTF Act allows a member of a DBG to disclose to the other members that an information notice pursuant to section 202 of the Act has been given, there are no further obligations for group-wide programmes to include measures for the sharing of specific information from a branch or subsidiary across the broader DBG, and vice versa. This deficiency has not been addressed.

Regarding c.18.2(c), the 2015 MER found that members of a DBG may, under certain circumstances, disclose information in relation to a SMR to other members of the group. The financial institution to which information has been disclosed is prohibited to disclose it unless the disclosure is made to another member of the DBG for the purpose of informing about the ML/TF risk. However, there were no further obligations in relation to confidentiality and use of information exchanged. The insertion of Subsection 123(7AB) of the AML/CTF Act ensures protection of confidentiality of information and that the information will be used only for the purposes for which it is disclosed (the same applies to corporate groups under subsection 123(7)). The deficiency under c.18.2(c) has been addressed, while the deficiency under c.18.2(b) remains.

c) **Criterion 18.3** *(Partly Met)* As outlined in 2015, except for section 6(6) of the AML/CTF Act, there are no provisions applicable to subsidiaries located abroad. There is no obligation for FIs with respect to the adequacy of the AML/CTF regime of host countries; and no obligation to apply the higher standard or Australia regime to the extent possible. There is also no obligation to apply measures to manage ML/TF risks and to inform AUSTRAC when the

host country does not permit the proper implementation of AML/CFT measures consistent with Australia's AML/CFT regime. While no changes have been made the AML/CTF Act or Rules, changes to obligations regarding applying the higher standard of AML/CFT regime to subsidiaries located abroad are being considered in future legislative reform. The deficiency has therefore not been addressed.

d) **Weighting and conclusion:** Australia has sufficiently clarified the expectations regarding the role of compliance officer at both the level of reporting entities and DBGs, which is set out in guidance that constitutes enforceable means. AUSTRAC guidance on employee screening has been strengthened to help reporting entities determine when screening should be undertaken for employees in roles that may pose ML/TF risk. Australia's approach to screening employees requires a preliminary consideration of each employee to understand the level of risk that may be posed. In revising the wording regarding the objectives of AML/CTF risk awareness training, AUSTRAC has addressed the deficiency identified in the MER and brought the language in line with Recommendation 18. Furthermore, amendments to the AML/CTF Rules have strengthened the requirements for independent review of standard and joint AML/CTF programmes. Regarding disclosure of information on SMRs between members of a DBG, confidentiality of information is now ensured. Despite this progress, some deficiencies remain. Changes to the AML/CTF Act mean that a member of a DBG can disclose to the other members that an information notice has been given, but there are no further obligations for group-wide programmes to include measures for the sharing of specific information from a branch or subsidiary. Australia notes that future legislative reform will address the deficiencies regarding the lack of AML/CFT provisions applicable to subsidiaries located abroad. Australia meets all criteria of R.18 to some degree and has made progress specifically regarding the requirement for reporting entities to submit to regular independent review following regulatory changes. While Australia has a significant presence in the Pacific region, where the minimum AML/CFT requirements in some of the host countries are less strict than those in Australia, it is not a major exporter of financial services globally. As such, the deficiency under c.18.3 has been weighted less heavily overall and in light of progress made particularly under c18.1. **Recommendation 18 is re-rated Largely Compliant.**

Recommendation 26

	Year	Rating
MER	**2015**	PC
FUR1	**2016**	PC (not re-assessed)
FUR2	**2017**	PC (not re-assessed)
FUR3	**2018**	PC (not re-assessed)
FUR4	**2023**	↑ **LC**

a) **Criterion 26.1** *(Met)* As outlined in the 2015 MER, pursuant to sections 212 and 229 of the AML/CTF Act, AUSTRAC is responsible for promoting compliance with the Act, regulations and AML/CTF Rules of all FIs, and is empowered to make rules prescribing matters required or permitted by the AML/CTF Act to be prescribed by AML/CTF Rules.

b) **Criterion 26.2** *(Met)* As stated in 2015, core principles FIs and other financial institutions must be licenced under relevant legislation, and the licencing process precludes the establishment or the operation of shell banks (See 2015 MER, c.26.2 for detailed outline of provisions).

c) **Criterion 26.3** *(Mostly Met)* The 2015 MER identified several deficiencies, including the lack of fitness and propriety as conditions for licencing under the Banking Act. Australia has clarified that, while the Banking Act does not include fitness and propriety as conditions for licencing, Section 11AF of the Banking Act provides that APRA (Australian Prudential Regulation Authority) may make prudential standards for Authorised Deposit-taking Institutions (ADIs) that are binding legislative instruments. APRA is also the licencing body for banking, insurance and superannuation businesses. APRA's Banking, Insurance, Life Insurance and Health Insurance (Prudential Standard) determination No.2 of 2018 (Prudential Standard CPS 520), issued after the MER, sets the Fit and Proper standard which applies to ADIs and insurers. The criteria include whether the person possesses the diligence, honesty, and integrity to perform properly the duties, with additional requirements for specific rules (i.e., auditors, actuaries). APRA needs to be satisfied that an applicant for a banking authority will comply with this instrument at the time of granting the authority, and section 9A(2)(b)(iii) of the Banking Act provides that APRA may revoke the licence of an ADI that has failed to comply. This determination is enforceable through the Banking Act, the Insurance Act 1973, the Life Insurance Act 1995 and the Private Health Insurance (Prudential Supervision) Act 2015. Considering this clarification and the issuance of Prudential Standard CPS 520, which is a legally binding determination, the deficiency identified in the 2015 MER has been addressed.

The 2015 MER also found that shareholders were not subject to fit and proper obligations but noted the ADI Authorisation Guidelines issued by APRA state that 'all substantial shareholders are required to demonstrate that they are 'fit and proper' in the sense of being well-established and financially sound entities of standing and substance' (see 2015 MER, c.26.3). In 2018, streamlined additional applications based solely on fitness and propriety were introduced into the Financial Sector (Shareholdings) Act 1998 (FSSA) for shareholders. Section 14A of the FSSA was introduced, which provides that a person applying for approval to hold a stake of more than 20% in a

financial sector company (ADI, authorised insurer or a holding company of an ADI or authorised insurer) must apply for approval under a "national interest" test or a "fit and proper person" test. The deficiency has therefore been addressed to some extent. However, some weaknesses remain, as these obligations apply only to those with a 20% stake or more in a financial sector company, and therefore do not necessarily extend to the ultimate beneficial owner or those with other types of control; controls also do not cover associates. Application of these obligations include: (a) the honesty, integrity and reputation of the person; (b) the competence and capability of the person, having regard to the degree of control or influence that the person has over the financial sector company; (c) the financial soundness of the person; and (d) whether there are reasonable grounds for suspecting the person has committed, or is at risk of committing, a financial crime, including money laundering or terrorism financing.

The 2015 MER also identified deficiencies regarding fit and proper requirements for Australian Credit Licence (ACL) holders and currency exchange businesses. Until 2020, ACL holders were required to lodge annual compliance certificates which may be verified by the Australian Securities and Investment Commission (ASIC) but had no direct obligations regarding fitness and propriety. Australia issued the Stronger Regulators Act in February 2020, which repealed and substituted sections 37 and introduced 37A of the *National Consumer Credit Protection Act 2009*, providing that fit and proper requirements apply in relation to ASIC granting credit licences (other than credit licence applications from ADIs) where they did not apply previously. Regarding currency exchange businesses, Australia explained that due to a shift in context with market drivers since the MER, these providers are now also providing money remittance services. Foreign currency exchange is a designated service under the AML/CTF Act, and as such, currency exchange businesses providing such services are required to enrol with AUSTRAC. They are also required to register with AUSTRAC under section 74 of the AML/CTF Act. This means that market entry controls for all currency exchanges are completed by AUSTRAC as part of the registration requirements for remitters under Part 6 of the AML/CTF Act. This includes an assessment as to whether the registration would involve a significant ML/TF or people smuggling risk if conducted, including the fact that key personnel have been charged or convicted for offences and risks deriving from beneficial ownership arrangements. No deficiencies were identified with the registration process for remitters under R.26 as part of the 2015 MER. The deficiencies regarding fit and proper requirements for ACL holders and currency exchange businesses have been addressed, with the remaining deficiency under c.26.3 concerning checks for shareholders, as outlined above.

d) **Criterion 26.4** *(Met)* (a – b) As set out in 2015, AUSTRAC continues to regulate and supervise all reporting entities under the AML/CTF Act for AML/CTF purposes, including Core Principles financial institutions, money remitters, '*bureaux de change*' (or currency exchange businesses), bullion dealers, gambling service providers and, since 2017, digital currency exchanges. These sectors, as providers of designated services, are under a legal obligation to enrol with AUSTRAC for supervision. AUSTRAC focuses on AML/CTF supervision of reporting entities at a corporate group level.

Designated services, which are the trigger for regulation, are defined in section 6 of the AML/CTF Act.

e) **Criterion 26.5** *(Met)* (a – c) Regarding the frequency and intensity of AML/CFT supervision, the 2015 MER found that AUSTRAC only applied a risk-based approach in its supervision of reporting entities to a certain extent at a corporate group level, and that inherent ML/TF risks were only considered to a certain extent. Since its MER, Australia has taken steps to improve how risk-based supervision is undertaken in the financial sector. AUSTRAC determines the frequency and intensity of AML/CFT supervision based on a range of internal and external inputs, including the supervised entity's ML/TF risks. In 2021, AUSTRAC developed and implemented the Targeting and Prioritisation (TAP) Model to inform its supervisory activities. The TAP Model utilises inputs from different sources to assign an overall level of compliance, including the inherent ML/TF risks of the reporting entity, and takes into consideration the size and complexity of a reporting entity, services offered, how they are offered and to whom (PEPs, high risk customers, etc.). The reporting entity's inherent risk and behavioural assessment is then scaled by a Business Activity rating, reflecting the larger scope for ML/TF threats in businesses that are more active and with more points of access. The report derived for the TAP Model provides AUSTRAC with a basis upon which it can determine the frequency and intensity of its supervisory activities. In addition, the TAP Model collects generated Overall Compliance Concern Ratings (OCCR) for individual reporting entities and collates them in accordance with relevant reporting entity groups (REG), which provides an overview of the risk picture for the REG. This is also possible at a sectoral and business activity level. Considering these developments and the progress made since its 2015 MER, Australia has now met the requirements of c.26.5.

f) **Criterion 26.6** *(Met)* At the time of the 2015 MER, AUSTRAC did not fully assess or re-assess the REG's risk profile, and reviewed to a limited extent the risk profiles of groups and reporting entities outside of high-risk groups are undertaken (See 2015 MER, c.26.6). Under AUSTRAC's TAP model (mentioned under c.26.5), AUSTRAC updates OCCRs for all reporting entities as part of an annual TAP model review. In confidential documentation provided to the FATF Secretariat and expert reviewers, AUSTRAC has demonstrated that it uses the TAP model to review the assessment of the ML/TF risk profile of a financial institution or group periodically, and when there are major events or developments in the management and operations of the financial institution or group. As such, the deficiency has been addressed and Australia meets the requirements of c.26.6.

g) **Weighting and conclusion:** Australia ensures that fitness and propriety are conditions for licencing through the APRA-issued Prudential Standard CPS 520 and has taken steps to improve how risk-based supervision is undertaken in the financial sector. Notably, AUSTRAC determines the frequency and intensity of AML/CFT supervision based on a range of sources, and implemented the TAP Model to inform its supervisory activities. AUSTRAC reviews the ML/TF risk profile of a financial institution or group periodically, and when there are major events or developments in the management and operations of the financial institution or group. However, a deficiency remains

regarding fit and proper checks for shareholders, as these obligations apply only to those with a 20% stake or more in a financial sector company, and therefore do not necessarily extend to the ultimate beneficial owner or those with other types of control; controls also do not cover associates. As such, **Recommendation 26 is re-rated Largely Compliant.**

Conclusion

Overall, Australia has made progress in addressing some of its technical compliance deficiencies. It has been re-rated on Recommendations 10, 13, 17, 18 and 26. The rating of Recommendation 2 has been maintained, and Recommendation 15 has been re-rated PC.

The table below shows Australia's MER ratings and reflects the progress it has made, and any re-ratings based on this and previous FURs:

Table 1. Technical compliance ratings, February 2024

R.1	R.2	R.3	R.4	R.5
PC	LC	C	C	***C*** ***(FUR 2018)***
R.6	**R.7**	**R.8**	**R.9**	**R.10**
C	C	***LC*** ***(FUR 2018)***	C	***LC*** ***(FUR 2024)***
R.11	**R.12**	**R.13**	**R.14**	**R.15**
LC	LC	***C*** ***(FUR 2024)***	LC	***PC*** ***(FUR 2024)***
R.16	**R.17**	**R.18**	**R.19**	**R.20**
PC	***C*** ***(FUR 2024)***	***LC*** ***(FUR 2024)***	***LC*** ***(FUR 2018)***	C
R.21	**R.22**	**R.23**	**R.24**	**R.25**
C	NC	NC	PC	NC
R.26	**R.27**	**R.28**	**R.29**	**R.30**
LC ***(FUR 2024)***	PC	NC	C	***C*** ***(FUR 2018)***
R.31	**R.32**	**R.33**	**R.34**	**R.35**
LC	***C*** ***(FUR 2018)***	LC	LC	PC
R.36	**R.37**	**R.38**	**R.39**	**R.40**
C ***(FUR 2018)***	C	C	C	C

Note: There are four possible levels of technical compliance: compliant (C), largely compliant (LC), partially compliant (PC), and non-compliant (NC).

Australia has six Recommendations rated PC and four Recommendations rated NC. Australia will report back to the FATF on progress achieved in improving the implementation of its AML/CFT measures in its 5th round mutual evaluation.

Annex to the FUR

Summary of Technical Compliance –Deficiencies underlying the ratings

Recommendations	Rating	Factor(s) underlying the rating[6]
1. Assessing risks & applying a risk-based approach	PC	• Australia's NTA suffers from limitations that likely mean that most but not all ML risks were identified, nor properly assessed. • Many high-risk entities and services identified in the NTA are not regulated under Australia's AML/CTF regime. • Reporting entities that are regulated must have programs that include a risk assessment and that mitigate the risks that they identify – but they are not required to mitigate other risks, nor carry out enhanced measures for high risks, identified in the NTA or NRA.
2. National co-operation and co-ordination	LC	• Australia does not have an overarching national AML/CFT strategy.
3. Money laundering offences	C	All criteria are met.
4. Confiscation and provisional measures	C	All criteria are met.
5. Terrorist financing offence	C (FUR 2018)	All criteria are met.
6. Targeted financial sanctions related to terrorism & TF	C	All criteria are met.
7. Targeted financial sanctions related to proliferation	C	All criteria are met.
8. Non-profit organisations	LC (FUR 2018)	• There is room for more TF-specific best practice and there are concerns that some smaller, potentially high-risk charities are not subject to adequate monitoring. • Available sanctions outside a criminal case are limited. • Membership to the NPO-Risk Working Group means that suspicions on NPOs outside the supervision of the ACNC and the ATO may be less likely to be raised.
9. Financial institution secrecy laws	C	All criteria are met.
10. Customer due diligence	LC (FUR 2024)	• There is no explicit provision requiring FIs to file an SMR in cases where they are unable to pursue the CDD process due to a risk of tipping off. • Regarding the obligation for FIs to identify the beneficial owner, the exception concerning natural persons, trusts that are registered and subject to regulatory oversight, and companies that are licensed and supervised, is not authorised by the Standard. • There is no explicit requirement for reporting entities to understand the ownership structure of customers that

[6] Deficiencies listed are those identified in the MER unless marked as having been identified in a subsequent FUR.

Recommendations	Rating	Factor(s) underlying the rating[6]
		are legal persons or arrangements, and the obligation to verify the information gathered does not cover the entire information that is required to be collected by the AML/CTF Rules. • The application of simplified measures to companies that are licensed and supervised is not justified nor authorised under the FATF Standards.
11. Record keeping	LC	• Certain customer-specific documents are exempt from record-keeping requirements. • There is no requirement that the records kept be sufficient to permit the reconstruction of the transactions. • Reporting entities are not legally required to ensure that the records are available to all competent authorities.
12. Politically exposed persons	LC	• The notions of close associate and of family members are too restrictive. • Important officials of political parties are not covered and there is no specific requirement for life insurance.
13. Correspondent banking	C (FUR 2024)	All criteria are met.
14. Money or value transfer services	LC	• Agents of an MVTS provider can be included the provider's AML/CTF programme, but this is not an obligation. • Their compliance with the AML/CTF programmes is not monitored by the MVTS provider.
15. New technologies	PC (FUR 2024)	• Australia has regulated DCE providers for AML/CTF purposes that carry out exchange between virtual currencies and fiat currencies but does not extend obligations to the other activities covered by the FATF Standards. • DCEs are required to register with AUSTRAC and there are measures to prevent criminals or their associates from holding or being the beneficial owners or controlling interest or holding management function in DCEs, which include criminal checks, but not covering all activities of VASPs.
16. Wire transfers	PC	• The intermediary, beneficiary, verification, MSB and targeted financial sanctions elements have not yet been updated in line with R.16.
17. Reliance on third parties	C (FUR 2024)	All criteria are met.
18. Internal controls and foreign branches and subsidiaries	LC (FUR 2024)	• While changes to the AML/CTF Act mean that a member of a DBG can disclose to the other members that an information notice has been given, there are no further obligations for group-wide programmes to include measures for the sharing of specific information from a branch or subsidiary. • There is a lack of AML/CFT provisions applicable to subsidiaries located abroad.
19. Higher-risk countries	LC (FUR 2018)	• The EDD measures listed in the AML/CFT Rules still include normal CDD measures (e.g., the clarification and updating of KYC information).
20. Reporting of suspicious transaction	C	All criteria are met.
21. Tipping-off and confidentiality	C	All criteria are met.

Recommendations	Rating	Factor(s) underlying the rating[6]
22. DNFBPs: Customer due diligence	NC	• Only casinos and bullion dealers are subject to AML/CTF obligations. • The AML/CTF Act provides exemptions for casinos and lawyers, though these two sectors have been identified as high ML threat in the NTA. • The identification threshold for casinos exceeds that set forth in the Recommendation.
23. DNFBPs: Other measures	NC	• Most DNFPBs are not subject to AML/CTF requirements on suspicious transaction reporting, instituting internal controls and complying with higher risk countries requirements, and the deficiencies identified under Recommendations 18 and 19 apply for DNFBPs that are subject to the requirements.
24. Transparency and beneficial ownership of legal persons	PC	• Australia relies exclusively on ASIC to trace beneficial ownership of shares, which only deals with public listed companies – no such mechanism exists for private companies, or legal persons established under State/Territory legislation.
25. Transparency and beneficial ownership of legal arrangements	NC	• There is no obligation for trustees to hold and maintain information on trusts or to keep this information up-to-date and accurate. In the absence of such obligations, the transparency of legal arrangements cannot be guaranteed.
26. Regulation and supervision of financial institutions	LC (FUR 2024)	• Regarding fit and proper checks for shareholders, obligations apply only to those with a 20% stake or more in a financial sector company, and therefore do not necessarily extend to the ultimate beneficial owner or those with other types of control; controls also do not cover associates.
27. Powers of supervisors	PC	• AUSTRAC's powers to supervise and ensure compliance are conditional upon the consent of the reporting entity. • The Act permits a reporting entity to at any time revoke the access of AUSTRACs authorised officers to its premises. A warrant is then necessary for AUSTRAC to execute its powers.
28. Regulation and supervision of DNFBPs	NC	• Only casinos, gaming outlets, and bullion dealers are supervised for AML/CTF compliance.
29. Financial intelligence units	C	All criteria are met.
30. Responsibilities of law enforcement and investigative authorities	C (FUR 2018)	All criteria are met.
31. Powers of law enforcement and investigative authorities	LC	• There is no mechanism in place to identify in a timely manner whether natural or legal persons own or control accounts (such as a register of accounts, or asking all account holding financial institutions at the same time if they have certain account holders).
32. Cash couriers	C (FUR 2018)	All criteria are met.
33. Statistics	LC	• Australia is often challenged to produce statistics at the national level. • Some statistics crucial to tracking the overall effectiveness and efficiency of the system related to ML investigations, prosecutions, convictions, and property confiscated are not maintained nationally, reflective of the wide range of agencies involved at the federal and State/Territory levels.

Recommendations	Rating	Factor(s) underlying the rating[6]
34. Guidance and feedback	LC	• A concern is the limited guidance available for identifying high risk customers or situations. In addition, none of the guidance applies to most DNFBPs.
35. Sanctions	PC	• AML/CTF requirements in Recommendations 6, and 8 to 23 do not apply to DNFBPs. • The range of sanctions for AML/CTF breaches is limited, particularly what can be directly applied by AUSTRAC. • Sanctions do not apply to all the DNFBPs that are regulated by competent authorities, and do not extend to directors and senior management if it is the reporting entity that breach the AML/CTF Act or the Rules.
36. International instruments	C (FUR 2018)	All criteria are met.
37. Mutual legal assistance	C	All criteria are met.
38. Mutual legal assistance: freezing and confiscation	C	All criteria are met.
39. Extradition	C	All criteria are met.
40. International Co-operation	C	All criteria are met.

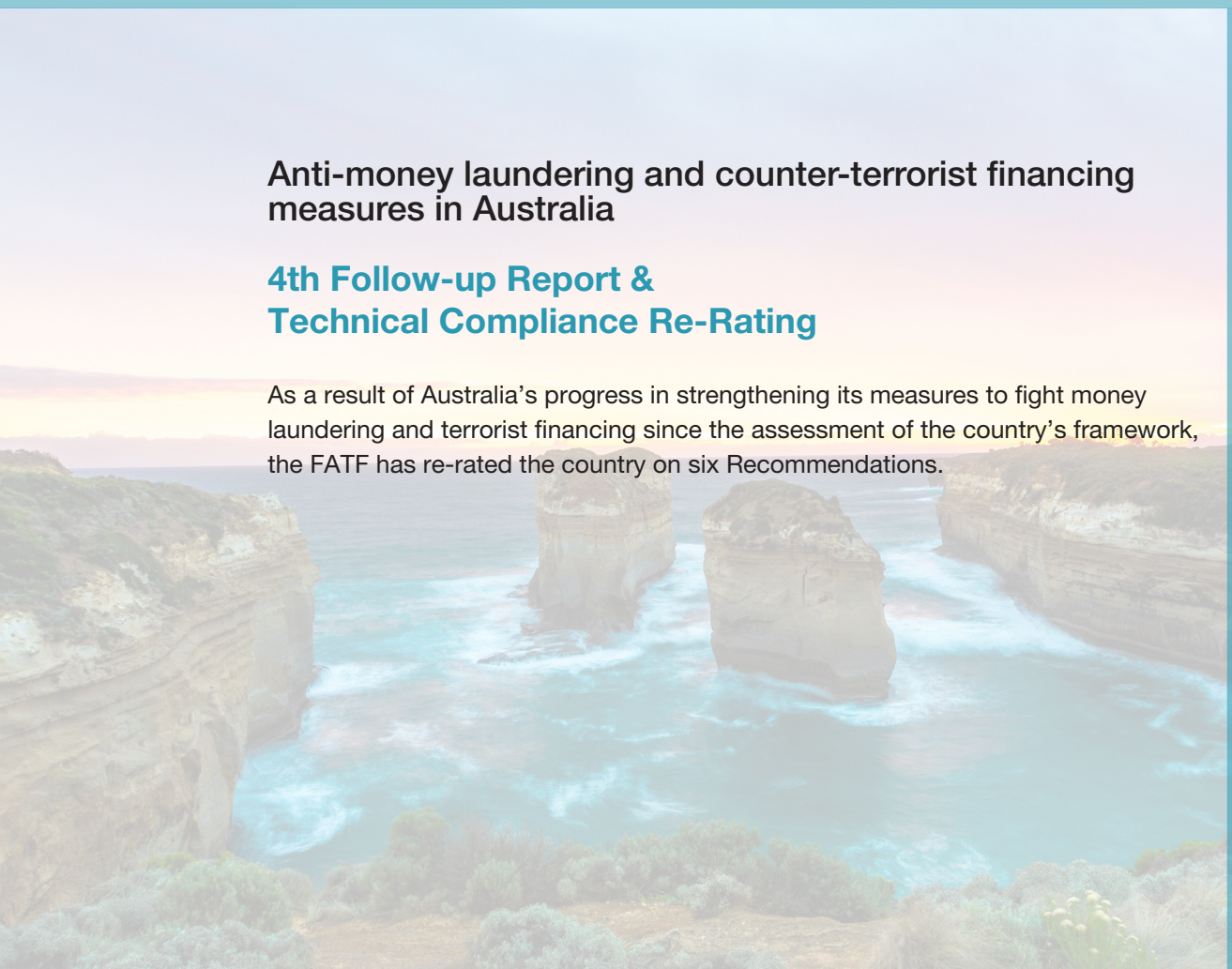
www.fatf-gafi.org

March 2024

Anti-money laundering and counter-terrorist financing measures in Australia

4th Follow-up Report & Technical Compliance Re-Rating

As a result of Australia's progress in strengthening its measures to fight money laundering and terrorist financing since the assessment of the country's framework, the FATF has re-rated the country on six Recommendations.



Follow-up report