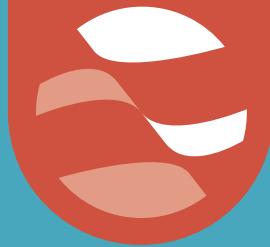


FATF



# Anti-money laundering and counter-terrorist financing measures

## Australia

### Mutual Evaluation Report

April 2015





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](http://www.fatf-gafi.org)

For more information about the APG, please visit the website: [www.apgml.org](http://www.apgml.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.

Citing reference:

FATF and APG (2015), *Anti-money laundering and counter-terrorist financing measures - Australia*, Fourth Round Mutual Evaluation Report, FATF, Paris and APG, Sydney  
[www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html](http://www.fatf-gafi.org/topics/mutualevaluations/documents/mer-australia-2015.html)

© 2015 FATF and APG. All rights reserved.

No reproduction or translation of this publication may be made without prior written permission.  
Applications for such permission, for all or part of this publication, should be made to  
the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France  
(fax: +33 1 44 30 61 37 or e-mail: [contact@fatf-gafi.org](mailto:contact@fatf-gafi.org)).

Photocredits coverphoto: ©Thinkstock

# Contents

<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
A <b>Key findings.....</b>	<b>5</b>
B <b>Risk and General Situation.....</b>	<b>7</b>
C <b>Overall level of compliance.....</b>	<b>7</b>
D <b>Priority actions .....</b>	<b>10</b>
<b>Table 1. Effective Implementation of Immediate Outcomes .....</b>	<b>12</b>
<b>Table 2. Compliance with FATF Recommendations.....</b>	<b>18</b>
<b>MUTUAL EVALUATION REPORT OF AUSTRALIA.....</b>	<b>27</b>
<b>Preface.....</b>	<b>27</b>
1. <b>ML/TF RISKS AND CONTEXT.....</b>	<b>29</b>
1.1    ML/TF Risks .....	29
1.2    Materiality.....	31
1.3    Structural Elements .....	31
1.4    Other Contextual Factors.....	31
1.5    Scoping of Higher-Risk Issues.....	32
2. <b>NATIONAL AML/CTF POLICIES AND COORDINATION.....</b>	<b>35</b>
2.1    Background and Context .....	36
2.2    Technical Compliance (R.1, R.2, R.33) .....	39
2.3    Effectiveness: Immediate Outcome 1 (Risk, Policy and Coordination) .....	39
2.4    Recommendations on National AML/CTF Policies and Coordination.....	44
3. <b>LEGAL SYSTEM AND OPERATIONAL ISSUES .....</b>	<b>47</b>
3.1    Background and Context .....	48
3.2    Technical Compliance (R.3, R.4, R.29-32) .....	48
3.3    Effectiveness: Immediate Outcome 6 (Financial intelligence) .....	48
3.4    Effectiveness: Immediate Outcome 7 (ML investigation and prosecution).....	55
3.5    Effectiveness: Immediate Outcome 8 (Confiscation) .....	61
3.6    Recommendations on legal system and operational issues.....	66
4. <b>TERRORIST FINANCING AND FINANCING OF PROLIFERATION .....</b>	<b>69</b>
4.1    Background and Context .....	70
4.2    Technical Compliance (R.5-8).....	70
4.3    Effectiveness: Immediate Outcome 9 (TF investigation and prosecution).....	70
4.4    Effectiveness: Immediate Outcome 10 (TF preventive measures and financial sanctions) .....	74
4.5    Effectiveness: Immediate Outcome 11 (PF financial sanctions) .....	78
4.6    Recommendations on Terrorist Financing and Financing of Proliferation .....	79
5. <b>PREVENTIVE MEASURES.....</b>	<b>81</b>
5.1    Background and Context .....	82
5.2    Technical Compliance (R.9-23).....	85
5.3    Effectiveness: Immediate Outcome 4 (Preventive Measures).....	86
5.4    Recommendations on Preventive Measures.....	91

<b>6. SUPERVISION .....</b>	<b>93</b>
6.1    Background and Context .....	94
6.2    Technical Compliance (R.26-28, R.34, R.35).....	94
6.3    Effectiveness: Immediate Outcome 3 (Supervision) .....	94
6.4    Recommendations on Supervision.....	103
<b>7. LEGAL PERSONS AND ARRANGEMENTS.....</b>	<b>105</b>
7.1    Background and Context .....	106
7.2    Technical Compliance (R.24, R.25).....	108
7.3    Effectiveness: Immediate Outcome 5 (Legal Persons and Arrangements) .....	108
7.4    Recommendations on Legal Persons and Arrangements .....	113
<b>8. INTERNATIONAL COOPERATION.....</b>	<b>115</b>
8.1    Background and Context .....	116
8.2    Technical Compliance (R.36-40) .....	116
8.3    Effectiveness: Immediate Outcome 2 (International Cooperation) .....	116
8.4    Recommendations on International Cooperation .....	120
<b>TECHNICAL COMPLIANCE ANNEX.....</b>	<b>121</b>
<b>1. INTRODUCTION.....</b>	<b>121</b>
<b>2. NATIONAL AML/CTF POLICIES AND COORDINATION.....</b>	<b>123</b>
Recommendation 1 – Assessing Risks and applying a Risk-Based Approach.....	123
Recommendation 2 – National Cooperation and Coordination.....	127
Recommendation 33 – Statistics .....	129
<b>3. LEGAL SYSTEM AND OPERATIONAL ISSUES .....</b>	<b>131</b>
Recommendation 3 – Money laundering criminalisation .....	131
Recommendation 4 – Confiscation and provisional measures.....	132
<b>Operational and Law Enforcement.....</b>	<b>133</b>
Recommendation 29 – Financial intelligence units .....	133
Recommendation 30 – Responsibilities of law enforcement and investigative authorities.....	135
Recommendation 31 – Powers of law enforcement and investigative authorities.....	136
Recommendation 32 – Cash Couriers.....	138
<b>4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION .....</b>	<b>141</b>
Recommendation 5 – Terrorist financing offence .....	141
Recommendation 6 – Targeted financial sanctions related to terrorism and terrorist financing.....	142
Recommendation 7 – Targeted financial sanctions related to proliferation.....	144
Recommendation 8 – Non-profit organisations .....	145
<b>5. PREVENTIVE MEASURES.....</b>	<b>147</b>
Recommendation 9 – Financial institution secrecy laws.....	150
<b>Customer due diligence and record-keeping .....</b>	<b>150</b>
Recommendation 10 – Customer due diligence .....	150
Recommendation 11 – Record-keeping.....	157
<b>Additional Measures for specific customers and activities .....</b>	<b>158</b>
Recommendation 12 – Politically exposed persons .....	158
Recommendation 13 – Correspondent banking .....	159
Recommendation 14 – Money or value transfer services .....	160
Recommendation 15 – New technologies.....	161
Recommendation 16 – Wire transfers .....	162

<b>Reliance, Controls and Financial Groups.....</b>	<b>162</b>
Recommendation 17 – Reliance on third parties.....	162
Recommendation 18 – Internal controls and foreign branches and subsidiaries .....	163
Recommendation 19 – Higher-risk countries.....	165
<b>Reporting of Suspicious Transactions .....</b>	<b>166</b>
Recommendation 20 – Reporting of suspicious transaction.....	166
Recommendation 21 – Tipping-off and confidentiality .....	167
<b>Designated non-financial businesses and professions .....</b>	<b>167</b>
Recommendation 22 – DNFBPs: Customer due diligence .....	168
Recommendation 23 – DNFBPs: Other measures.....	168
<b>6. SUPERVISION .....</b>	<b>169</b>
Recommendation 26 – Regulation and supervision of financial institutions.....	169
Recommendation 27 – Powers of supervisors .....	171
Recommendation 28 – Regulation and supervision of DNFBPs.....	173
Recommendation 34 – Guidance and feedback .....	173
Recommendation 35 – Sanctions .....	174
<b>7. LEGAL PERSONS AND ARRANGEMENTS.....</b>	<b>177</b>
Recommendation 24 – Transparency and beneficial ownership of legal persons.....	177
Recommendation 25 – Transparency and beneficial ownership of legal arrangements.....	180
<b>8. INTERNATIONAL COOPERATION .....</b>	<b>183</b>
Recommendation 36 – International instruments.....	183
Recommendation 37 – Mutual legal assistance.....	183
Recommendation 38 – Mutual legal assistance: freezing and confiscation .....	185
Recommendation 39 – Extradition.....	186
Recommendation 40 – Other forms of international cooperation.....	188
<b>Table of acronyms .....</b>	<b>193</b>



## Executive Summary

1. This report provides a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Australia as at the date of the on-site visit (30 July – 12 August 2014). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Australia's AML/CTF system, and provides recommendations on how the system could be strengthened.

### A. Key Findings

- Overall, Australian authorities have a good understanding of most of Australia's main money laundering (ML) risks but need to develop their understanding further in certain areas. They coordinate very well activities to address key aspects of the ML / terrorist financing (TF) risks but some key risks remain unaddressed, and an underlying concern remains that the authorities are addressing predicate crime rather than ML.
- Authorities have a good understanding of TF risks, and are addressing them accordingly. They assess that TF is largely motivated by international tensions and conflicts.
- Operationally, national AML/CTF coordination is very comprehensive, but demonstrating its overall success is challenging, although results from national taskforces are showing positive trends. A stronger focus is required on monitoring and measuring success.
- Australia develops and disseminates good quality financial intelligence to a range of law enforcement bodies, customs and tax authorities. The amount of financial transaction data in the Australian Transaction Reports and Analysis Centre (AUSTRAC) database, and the fact that all relevant competent authorities have access to this database and can use its integrated analytical tool, are strengths of Australia's AML/CTF system. However, the somewhat limited use of AUSTRAC information by law enforcement as a trigger to commence ML/TF investigations presents a weakness in the Australian AML/CTF system.
- Australia's main criminal justice policy objective is to disrupt and deter predicate crime, including if necessary through ML investigations/prosecutions. Australia focuses on what it considers to be the main three proceeds generating predicate threats (drugs, fraud and tax evasion). However, Australia should expand its focus to ensure that a greater number of cases of ML are being identified and investigated adequately.
- Confiscation of criminal proceeds, instrumentalities and property of equivalent value is being pursued as a policy objective; mainly in relation to drugs, and in relation to tax by the Australian Taxation Office (ATO). Competent authorities have increased their efforts to

confiscate proceeds of crime, particularly since the establishment of the national Criminal Assets Confiscation Taskforce. But it is unclear how successful confiscation measures are across all jurisdictions, and total recoveries remain relatively low in the context of the nature and scale of Australia's ML/TF risks and have only modestly increased over the past few years.

- Australia's legal framework to combat TF is comprehensive. Australia has undertaken several TF investigations and prosecutions, and secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable.
- Australia's legal framework to implement targeted financial sanctions is a good example for other countries. The automatic, direct legal obligation to freeze assets as soon as an entity is listed by the UN and the numerous designations made under the domestic regime are to be commended as best practices for other countries. However, effective implementation of the legal framework is difficult to confirm in the absence of freezing statistics, financial supervision, or supervisory experience and feedback on practical implementation by the private sector.
- Australia has not implemented a targeted approach nor has it exercised oversight in dealing with non-profit organisations (NPOs) that are at risk from the threat of terrorist abuse. Authorities have not undertaken a review of the NPO sector to identify the features and types of NPOs that are particularly at risk of being misused for TF.
- Most designated non-financial business and profession sectors are not subject to AML/CTF requirements, and did not demonstrate an adequate understanding of their ML/TF risks or have measures to mitigate them effectively. This includes real estate agents and lawyers, both of which have been identified to be of high ML risk in Australia's National Threat Assessment.
- The major reporting entities – including the big four domestic banks which dominate the financial sector – have a good understanding of their AML/CTF risks and obligations, but some AML/CTF controls, whilst compliant with Australian obligations, are not in line with FATF Standards<sup>1</sup>.
- AUSTRAC has done a good job in promoting compliance with the AML/CTF standards by the vast amount of entities under its supervision. Australia has set up and developed a risk-based approach to supervision, although further improvement is required relating to the risk picture of the supervised entities. In mitigating risks through supervision, Australia should focus more on effective supervision and enforcement of individual reporting entities' compliance with AML/CTF obligations within the various sectors.
- Australia has not conducted a formal risk assessment on TF risks associated with legal persons and arrangements. The majority of legal persons are registered with the Australian Securities and Investment Commission (federal) while others with State or Territory authorities. While the information seems to be largely available to competent authorities and to the public, very limited verification is conducted on the information that is registered. Information on the beneficial owner of legal persons and legal arrangements is not maintained and accessible to competent authorities in a timely manner.
- Australia cooperates well with other countries in MLA matters, including extradition. Informal cooperation is generally good across agencies.

<sup>1</sup> The FATF Standards comprise the FATF Recommendations and their Interpretive Notes.

## B Risk and General Situation

2. Australia has identified and assessed, and has a good understanding of most of, its main ML risks and has mechanisms in place to mitigate them. Domestic and foreign organised crime groups operate in Australia. The main sources of criminal proceeds are illicit drugs, frauds, and tax evasion. Australian drug markets are said to be some of the most profitable in the world, attracting interest from major syndicates in South East Asia and South America. Most laundering involves use of the banking sector, money remitters, and complex corporate structures, facilitated by gate-keepers. Australia is seen as an attractive destination for foreign proceeds, particularly corruption-related proceeds flowing into real estate, from the Asia-Pacific region. Outwards proceeds flows are directed mainly to major financial hubs in Asia and the Middle East, with tax proceeds also flowing to European havens.

3. Australia has properly identified and assessed, and has a good understanding of, its TF risk, and is addressing it accordingly. Globally, the amounts of funds generated to finance terrorism vary between groups. Funds raised by groups that are part of an international network can be significant in the TF context. These groups have the financial infrastructure to undertake sizeable fundraising and money transfer operations. Small domestic groups and lone wolf terrorists are also a significant TF risk. While the amounts raised by these radicalised groups or individuals are much smaller, their intent to undertake violent acts in Australia can pose a direct threat to the Australian community. The authorities have periodically and successfully disrupted domestic terrorism plots, and the associated funding. Recently, the emerging TF risk has involved some Australians funding travel from legitimate sources to fight in conflict zones. Some funds have also been raised through abusing registered and informal “pop-up” charities linked to humanitarian fund-raising.

## C Overall level of compliance

4. Australia has a strong institutional framework for combatting ML, TF, and proliferation financing. Australia's measures are particularly strong in legal, law enforcement, and operational areas, and targeted financial sanctions; some improvements are needed in the framework for preventive measures and supervision, in particular for designated non-financial businesses and professions. In terms of effectiveness, Australia has achieved high results in international cooperation, and substantial results in risk, policy and coordination, the use of financial intelligence and combating terrorist financing and proliferation financing. Only moderate or minor improvements are needed in these areas. Major improvements are needed in other areas, as noted below.

### *C.1 Assessment of risk, coordination, and policy setting*

5. Australia has a good understanding of most of its main ML risks and coordinates comprehensively to address most of them. However, some key risks remain unaddressed and, inconsistently with the FATF Standards, the authorities are focussed more on predicate crime rather than ML. TF risk is well understood and actions are being taken to mitigate it, particularly by disrupting domestic terrorist activities. Australia has produced a national report on each of its ML (the National Threat Assessment—NTA) and TF risks (the National Risk Assessment—NRA), which are supplemented by ongoing risk analysis efforts. Australia has used the results of the assessments to help shape aspects of how it combats ML and TF and has a national strategy for combating organised crime which identifies ML as an intrinsic enabler of organised crime.

6. Operational activities are coordinated using a mixture of standing committees and task forces that include federal and State and Territory agencies, which is salient as Australia is a federation. The objectives and activities of most of the competent authorities are generally consistent with the ML/TF risks, with the major exception being a lack of focus on addressing risks from abuse of complex corporate structures, real estate (including through regulating relevant designated non-financial businesses and professions (DNFBPs)).

7. Australia does not have a developed national policy setting out what the overall AML/CTF system is meant to achieve, or how its success should be monitored or measured, making it challenging to determine how well the ML/TF risks are being addressed. Accordingly, national metrics about how well the authorities' efforts are addressing ML/TF risks are limited, and the authorities were challenged to present convincing

## EXECUTIVE SUMMARY

evidence about what outcomes their efforts are achieving. Exemptions from requirements for reporting entities and the application of enhanced or simplified measures are not based primarily on the results of the NTA, NRA or other efforts to assess ML/TF risks. The authorities coordinate and cooperate to a large extent to combat the financing of proliferation of weapons of mass destruction.

### *C.2 Financial intelligence, ML, and confiscation*

8. Australia develops and disseminates good quality financial intelligence to a range of law enforcement bodies, customs and tax authorities. AUSTRAC is a well-functioning financial intelligence unit (FIU). The amount of financial transaction data in the AUSTRAC database, and the fact that all relevant competent authorities have access to this database, and can use its integrated analytical tool, is a strength of Australia's AML/CTF system. AUSTRAC information is accessed by federal law enforcement as a routine in most cases but less so by State and Territory police who conduct most predicate crime investigations, and this information assists in the investigation of predicate offences. However, the somewhat limited use of AUSTRAC information by law enforcement as a trigger to commence ML/TF investigations, presents a weakness in the Australian AML/CTF system and should be addressed. Broader use of the sound institutional structure for combating ML would mitigate ML/TF risks more effectively.

9. Australia's main policy objective is to disrupt and deter predicate crime, including, if necessary, through ML investigations/prosecutions. Australia focuses on what it considers to be the main three proceeds generating predicate risks (drugs, fraud, and tax evasion). At the federal level, the authorities charge stand-alone and third party ML offences, but legal issues have arisen in relation to the prosecution of self-laundering offences, and ML related to foreign predicates including corruption is not frequently prosecuted. At the State/Territory level, prosecutions for substantive ML offences, including third party laundering and stand-alone laundering charges, are less common.

10. Since the last assessment, Australia has improved in terms of obtaining ML convictions, and is achieving reasonable results in relation to the key risk and those geographic areas where Australia is focusing on ML, but the overall results are lower than they could be relative to the nature and scale of the risks. The authorities have applied a range of sanctions for ML offences to natural persons, but no corporations have been prosecuted for ML offences. The authorities apply other criminal justice measures to disrupt serious criminal activity, including ML offences, but in accordance with their policy of disruption of serious and organised crime such measures are applied whether or not it may be possible to secure a ML conviction.

11. Confiscation of criminal proceeds, instrumentalities, and property of equivalent value is being actively pursued as a policy objective in Australia. The competent authorities have enhanced their efforts since the last assessment with the amounts being restrained and confiscated increasing at the federal level, although overall the figures remain relatively modest in the context of the nature and scale of Australia's ML/TF risks. The majority of assets recovered to date have flowed from the drugs trade and also from tax evasion (using ATO recovery powers). The Criminal Asset Confiscation Taskforce (CACT) takes non-conviction based asset recovery proceedings in most cases, allowing for a lower civil standard of proof; however, cases can become difficult to pursue when complicated company or overseas structures are used or when foreign predicate offending is involved.

12. At the State and Territory level, the combined recoveries are about twice the value of recoveries made at the federal level due to the heavy emphasis on drug-related recoveries. Australia is taking some steps to target the cross-border movement of cash and bearer negotiable instruments (BNIs). Australia remains at significant risk of an inflow of illicit funds from persons in foreign countries who find Australia a suitable place to hold and invest funds, including in real estate.

### *C.3 Terrorist financing and proliferation financing*

13. It is positive to note that Australia has undertaken several TF investigations and prosecutions, and secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable. Australia had successfully disrupted two domestic terrorist plots (Pendennis and Neath) at the time of the on-site visit. Australia also uses these other measures to address the most relevant emerging TF risk – individuals

travelling to conflict zones to participate in or advocate terrorist activity. Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations and terrorist support networks. Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions applied has not been clearly demonstrated.

14. Despite the general risks identified by the authorities in the NRA, Australia has not undertaken a risk review of the NPO sector to identify the features and types of NPOs that are particularly at risk of being misused for TF. Subsequently, there is no TF-related outreach to, or TF-related monitoring of, this part of the sector that would be at risk and that account for a significant share of the sector's activities.

15. Australia has a sound legal framework for targeted financial sanctions relating to terrorism and proliferation, but it is difficult to determine the effectiveness of the system. Under the Australian legal framework, the legal obligation to freeze assets is automatic upon designation at the UN; no additional action by Australian authorities is needed to give legal effect to a designation (although email alerts are sent to subscribers). This is a best practice for other countries. The Department of Foreign Affairs and Trade (DFAT) has primary responsibility for compliance with sanction requirements. However, DFAT does not adequately monitor or supervise the financial sector for compliance with the requirements of the FATF Recommendations, as would be expected of a supervisory authority. In addition, no financial institutions are supervised or monitored for compliance with the targeted financial sanctions (TFS) requirements (as in financial supervision) by any other competent supervisory authority. The absence of freezing statistics, financial supervision, supervisory experience, and feedback on practical implementation by the private sector made it difficult to confirm the level of effectiveness of the system.

#### *C.4 Preventive measures and supervision*

16. Regulated entities generally have adopted preventive measures required under the Australian regime, but some controls are not yet in line with FATF Standards.

17. Australia's AML/CTF regime has changed significantly since the last mutual evaluation report in 2005. The regime, introduced in 2006, significantly expanded the number of businesses subject to AML/CTF obligations – known as reporting entities. Under the new AML/CTF regime, the preventive measures' requirements have been brought more in line with FATF Standards, although deficiencies remain. Except for gaming and bullion, other DNFBP sectors are not subject to AML/CTF obligations. Understanding of ML/TF risks and implementation of preventive measures is better among larger players and in the regulated sectors.

18. Within the remittance sector, effective implementation of AML/CTF controls varies, depending on the industry's size and resources. The banks, particularly domestic ones, account for a large share of banking sector assets and international funds transfers in the system, but do not fully implement preventive measures to the extent envisaged by the FATF, especially where they meet Australian domestic requirements which do not meet the FATF standard. Most DNFBPs, including real estate agents and legal professionals, are also not subject to AML/CTF controls or suspicious transaction reporting obligations, even though they are highlighted as being high-risk for ML activities.

19. To a large extent, licensing, registration and other controls implemented by Australia, adequately prevent criminals and their associates from entering the financial sector. An important factor AUSTRAC uses in identifying ML/TF risk at the Reporting Entity Group (REG) level is the volume and value of transaction reports (suspicious matter report (SMRs) and international fund transfer instructions (IFTIs)) as an indicator of the volume of funds flowing through an entity, the size of an entity as a proxy measure of the number of customers, products and distribution channels. It is not sufficiently clear that AUSTRAC, when risk profiling REGs or individual reporting entities, collects and uses sufficient information necessary to adequately determine the level of inherent risk of the REG and individual reporting entities, beyond the information from transaction reports.

20. AUSTRAC succeeds to a fair extent in promoting compliance with the AML/CTF requirements among the sectors it has engaged. The focus of supervision is targeting what AUSTRAC considers to be the

## EXECUTIVE SUMMARY

high-risk entities for enhanced supervisory activity, and to test the effectiveness of REG's/reporting entities' systems and controls in practice. However, the number of enforcement actions and the subjects of these actions do not convincingly demonstrate that reporting entities are subject to effective and proportionate sanctions.

### *C.5 Transparency and beneficial ownership*

21. Australia has undertaken an assessment of the ML risks associated with legal persons and arrangements but did not comprehensively assess all forms of legal persons (including foreign companies operating in Australia). Legal persons and trusts were assessed as medium to high risk for ML but limited measures exist to mitigate risk associated with legal persons and very limited measures exist to mitigate the ML risk associated with legal arrangements. Authorities are nevertheless aware that legal persons can be, or are being, misused for ML. Australia has not conducted a formal assessment of the TF risks associated with legal persons and arrangements.

22. Overall, there is good information on the creation and types of legal persons in Australia, but less information about legal arrangements. Federal and State/Territory registries are publically available for legal persons and what is recorded is available to competent authorities. However, measures need to be taken, including imposing AML/CTF obligations on those who create and register legal persons and arrangements, in order to strengthen the collection and availability of beneficial ownership information.

23. The existing measures and mechanisms are not sufficient to ensure that accurate and up-to-date information on beneficial owners is available in a timely manner. It is also not clear that information held on legal persons and legal arrangements is accurate and up-to-date. The authorities did not provide evidence that they apply effective sanctions against persons who do not comply with their information requirements. Overall, legal persons and arrangements remain very attractive for criminals to misuse for ML and TF.

### *C.6 International Cooperation*

24. Australia cooperates well with other countries in mutual legal assistance (MLA) matters. MLA requests are processed in a timely manner in accordance with a case prioritisation framework. Australia cooperates well in extradition. Both making and receiving requests in ML and TF related matters and informal cooperation is generally good across agencies. But the ability to provide beneficial ownership information for legal persons and trusts in relation to foreign requests is more limited. Nevertheless, Australia cooperates well in providing available beneficial ownership information for legal persons and trusts in relation to foreign requests.

25. Australia maintains comprehensive statistics in relation to MLA and extradition matters including in relation to ML and TF, although there are some limitations in relation to categorisation of ML offences within the case management framework. AUSTRAC cooperates well with its foreign counterparts. Informal cooperation is generally good across agencies.

## D Priority actions

26. The prioritised recommended actions for Australia, based on these findings, are:

- Undertake a re-assessment of Australia's ML risks in keeping with the requirements and guidance issued in relation to Recommendation 1, and formalise the ongoing processes for re-assessing risks. Australia should also identify metrics and processes for monitoring and measuring success.
- The authorities should place more emphasis on pursuing ML investigations and prosecutions at the federal as well as the State/Territory level. The authorities should increase efforts to address ML risks associated with:
  - predicate crimes other than drugs and tax, including foreign predicates;

- the abuse of legal persons and arrangements and the real estate sector;
  - identity fraud;
  - fraud; and
  - cash intensive activities.
- CACT should continue its good early work and demonstrate its effectiveness over time to confiscate the proceeds and instrumentalities of crime.
- AUSTRAC should incorporate more (inherent) risk factors besides data analysis from filed reports into identifying and assessing the risk of reporting entities. AUSTRAC should consider opportunities to further utilise its formal enforcement powers to promote further compliance by reporting entities through judicious use of its enforcing authority.
- Australia should ensure financial institutions are actively supervised for implementation of DFAT lists, most likely through a legislative amendment to the statute identifying and authorising the agency responsible for supervision.
- Australia should implement a targeted approach in relation to preventing NPOs from TF abuse. As a first step, Australia needs to undertake a thorough review of the TF risks that NPOs are facing (beyond the issues already covered in the NRA) and the potential vulnerabilities of the sector to terrorist activities.
- Ensure that lawyers, accountants, real estate agents, precious stones dealers, and trust and company service providers understand their ML/TF risks, and are required to effectively implement AML/CTF obligations and risk mitigating measures in line with the FATF Standards. Ensure that reporting entities implement as early as possible the obligations on enhanced customer due diligence (CDD), beneficial owners, and politically exposed persons introduced on 1 June 2014.
- Australia should assess the risks of TF posed by all forms of legal persons and arrangements. Australia should also take measures to ensure that beneficial ownership information for legal persons is collected and available. Trustees should be required to hold and maintain information on the constituent elements of a trust including the settlor and beneficiary.

**Table 1. Effective Implementation of Immediate Outcomes**

<b>Effectiveness</b>	
<b>1. Risk, Policy and Coordination</b>	<b>Substantial</b>
<p>Australia is achieving Immediate Outcome 1 to a large extent as demonstrated by its good understanding of most of its major ML risks and of its TF risks, as well as its very good coordination of activities to address key aspects of the ML/TF risks. Australia identified and assessed most of its major ML risks but more attention needs to be paid to understanding foreign predicate risks, and vulnerabilities that impact its AML/CTF system. AML/CTF policies need to better address ML risks associated with foreign predicate offending the abuse of legal persons and arrangements, and laundering in the real estate sector, particularly through bringing all DNFBPs within the AML/CTF regime.</p> <p>More current information about ML/TF risks also needs to be communicated to the private sector. The identification of low or high ML/TF risks by the authorities should drive exemptions from requirements and strongly influence the application of enhanced or simplified measures for reporting entities. While cooperation, particularly on operational matters, is very good across relevant competent authorities, including for proliferation matters, Australia could better articulate an AML/CTF policy and maintain more comprehensive national statistics to demonstrate how efficient and effective its AML/CTF system is, including by developing ways to show that its disruption strategy for predicate crime addresses ML risks.</p>	
<b>2. International Cooperation</b>	<b>High</b>
<p>The Immediate Outcome is achieved to a very large extent. Australia uses robust systems for mutual legal assistance, as demonstrated by their statistics, although there are some limitations in relation to the categorisation of ML offences within the case management framework. Informal cooperation is generally good across agencies. Although diagonal cooperation does not appear to be permitted with the Australian Securities and Investment Commission (ASIC) and the Australian Prudential Regulation Authority (APRA), this is not a significant issue. Australia cooperates well in providing available beneficial ownership information for legal persons and trusts in relation to foreign requests, keeping in mind that what is not (required to be) available in Australia cannot be shared.</p>	
<b>3. Supervision</b>	<b>Moderate</b>
<p>In identifying ML/TF risk at the group level, an important factor on which AUSTRAC relies are the varying forms of reporting (i.e. SMRs, TTRs and IFTIs) and unverified self-reporting of compliance to determine reporting entity risks. Other risk factors should be considered and AUSTRAC supervisory practice should extend to more individual reporting entities. AUSTRAC's approach does not seem sufficiently nuanced to adequately account for the risks of individual reporting entities in a REG. More generally, AUSTRAC's graduated approach to supervision does not seem to be adequate to ensure compliance.</p> <p>The majority of deficiencies identified by AUSTRAC through its compliance activities are voluntarily remediated by REs based on recommendations and requirements issued by AUSTRAC after an assessment. No monetary penalties for violations of the AML/CTF preventive measure obligations have ever been pronounced. Rather, AUSTRAC had applied sanctions to a limited extent in the</p>	

## Effectiveness

form of enforceable undertaking, which amounts to – among other things – a formal agreement that the reporting entity will comply with AML/CTF requirements. The assessors concluded that the use of sanctions for non-compliance has had minimal impact on ensuring compliance among reporting entities not directly affected by the sanction. The private sector shared similar views about the depth, breadth, and effectiveness of the supervisory regime. In addition, there is no appropriate supervision or regulation of most higher-risk DNFBPs because they are not subject to AML/CTF requirements. Overall, the authorities were unable to demonstrate improving AML/CTF compliance by reporting entities or that they are successfully discouraging criminal abuse of the financial and DNFBP sectors.

<b>4. Preventive Measures</b>	<b>Moderate</b>
-------------------------------	-----------------

Australia exhibits some characteristics of an effective system for applying preventive measures in financial institutions and DNFBPs. The major reporting entities – including the big four domestic banks which dominate the financial sector – have a good understanding of their AML/CTF risks and obligations, as required by Australian obligations. These obligations are not in line with FATF Standards. In general, the major reporting entities and other high risk reporting entities subject to more regular supervisory engagement appear to have a reasonable understanding of ML/TF risks and preventive measures that comply with the Australian AML/CTF regime. Reporting entities have demonstrated that they are aware of their requirement to have AML/CTF programmes and reported having implemented the necessary internal AML/CTF controls. However, a number of aspects of the AML/CTF regime – including those that relate to internal controls, wire transfers, correspondent banking, etc. – do not meet FATF Standards. As a result, reporting entities' implementation of AML/CTF measures will not meet the FATF Standards if its internal controls are developed solely to meet the Australian requirements.

In addition, while the requirements have been revised with respect to CDD and politically exposed persons (PEPs), none of the reporting entities reported they were able to fully implement these requirements at the time of the on-site. As a result, at the time of the on-site visit, reporting entities were working to transition from the pre-June 1 AML/CTF Rules, which were not in line with the FATF Standards. At the same time, a lot of reliance is placed on the banking and financial sector as gatekeepers due to the absence of AML/CTF regulation and requirements on key high-risk DNFBPs such as lawyers, accountants, real estate agents and trust and company service providers. As a result of these factors, the effectiveness of the preventive measures in the financial system as a whole, and DNFBPs, is hence called into question to some extent.

<b>5. Legal Persons and Arrangements</b>	<b>Moderate</b>
--	-----------------

Legal persons and legal arrangements were identified as presenting medium to high risks for ML in the NTA of 2011 and the use of complex corporate structures in ML schemes was frequently cited by law enforcement spoken to by the assessment team. There is good information on the creation and types of legal persons in the country available publicly, but less information about legal arrangements. The ATO has made some improvements to the Australian Business Register (ABR) that involve collecting information on associates and trustees for new registrations from December 2013.

The authorities seem to appreciate the extent to which legal persons can be, or are being misused, for ML and had some awareness in relation to TF. They could do more to identify, assess, and understand the vulnerabilities of both for ML and TF, as past assessment efforts seem to have

### Effectiveness

focused more on underlying predicate crime. While Australia has implemented some measures to address the specific risk identified in the 2011 NTA to legal persons and legal arrangements, other measures need to be taken, including imposing AML/CTF obligations on those who create and register them to strengthen the collection and availability of beneficial ownership information.

Concerning beneficial owners of legal persons and legal arrangements, the existing measures and mechanisms are not sufficient to ensure that accurate and up-to-date information on beneficial owners is available in a timely manner. It is not clear that information held on legal persons and legal arrangements is accurate and up-to-date. The authorities did not provide evidence that they apply effective sanctions against persons who do not comply with their information requirements. Overall, legal persons and arrangements remain very attractive for criminals to misuse for ML and TF.

## 6. Financial Intelligence

Substantial

Australia's use of financial intelligence and other information for ML/TF and associated predicate offence investigations demonstrates to a large extent characteristics of an effective system. AUSTRAC and partner agencies collect and use a wide variety of financial intelligence and other information in close cooperation. This information is generally reliable, accurate, and up-to-date. Partner agencies have the expertise to use this information effectively to conduct analysis and financial investigations, identify and trace assets, and develop operational and strategic analysis. This is demonstrated particularly well in joint investigative task forces, and when tracing and seizing assets.

A large part of AUSTRAC analysis use relates to predicate crime and not to ML/TF, thus resulting in a relatively low number of ML cases. Although AUSTRAC information is said to be checked in most Australian Federal Police (AFP) predicate crime investigations, that is not the case for the majority of predicate crime investigations which are conducted at the State/Territory level. Both AUSTRAC and law enforcement authorities could raise their focus on ML cases to achieve a larger number of criminal cases in this area.

There are also some concerns with regard to the relatively low number of money laundering and terrorist financing investigations outside the framework of the task forces related to the abuse of tax or secrecy havens, use of alternative remittance/informal value transfer systems and asset seizure.

Although AUSTRAC information is regularly referred to as a catalyst for ML/TF and related predicate investigations, the ability for law enforcement to maintain details of outcomes that are attributed to financial intelligence could be improved.

## 7. ML Investigation and Prosecution

Moderate

Overall, Australia demonstrates some characteristics of an effective system for investigating, prosecuting, and sanctioning ML offences and activities. The focus remains on predicate offences, recovery of proceeds of crime, and disruption of criminal activity rather than the pursuit of convictions for ML offences or disruption of ML networks both at the Commonwealth and State/Territory levels. However, in the areas of identified risk, Australia is achieving reasonable results and the increase in the number of ML convictions over recent years is heartening. This demonstrates an increased focus on ML compared to the previous FATF/APG assessment.

## Effectiveness

It should be relatively easy to achieve a substantial or even high level of effectiveness by

- expanding the existing ML approach to other (foreign) predicate offences including corruption,
- focusing more on ML within task forces,
- being able to demonstrate the extent to which potential ML cases are identified and investigated,
- addressing investigative challenges associated with dealing with complex ML cases, including those using corporate structures,
- pursuing ML charges against legal entities, and
- ensuring that all States and Territories focus on substantive type ML.

## 8. Confiscation

**Moderate**

Overall, Australia demonstrates some characteristics of an effective system for confiscating the proceeds and instrumentalities of crime. The framework for police powers and provisional and confiscation measures is comprehensive and is being put to good use by the CACT, which is showing early signs of promise as the lead agency to pursue confiscation of criminal proceeds as a policy objective in Australia. At the State/Territory level, the focus has remained primarily on recovery of proceeds of drugs offences. Relatively modest amounts are being confiscated, which suggests that criminals retain much of their profits.

## 9. TF Investigation and Prosecution

**Substantial**

Australia exhibits most characteristics of an effective system for investigating, prosecuting, and sanctioning those involved in TF. It is positive to note that Australia has undertaken several TF investigations and prosecutions, and also secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable. Australia had successfully disrupted two domestic terrorist plots (Pendennis and Neath) at the time of the on-site visit.<sup>2</sup> Australia also uses these other measures to address the most relevant emerging TF risk – individuals travelling to conflict zones to participate in or advocate terrorist activity.

Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks. Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions applied has not been clearly demonstrated.

<sup>2</sup> Another plot was disrupted soon after the on-site visit. AUSTRAC also took action in November 2014 to cancel the registration of remittance dealer (Bisotel Rieh Pty Ltd) concerned that its continued registration may involve a TF risk. This followed a period of engagement and notification of action by AUSTRAC.

## Effectiveness

## **10. TF Preventive measures & financial sanctions**

## Moderate

Australia demonstrates some characteristics of an effective system in this area. Terrorists and terrorist organisations are being identified in an effort to deprive them of the resources and means to finance terrorist activities.

A strong area of technical compliance is in the legal framework for TFS against persons and entities designated by the United Nations Security Council (UNSC) (United Nations Security Council Resolution (UNSCR) 1267) and under Australia's sanctions law (for UNSCR 1373). Australia has co-sponsored designation proposals to the UNSCR 1267/1989 Committee and adopted very effective measures to ensure the proper implementation of UN designations without delay. Australia has also domestically listed individuals and entities pursuant to UNSCR 1373 (including most recently two Australians fighting overseas for terrorist entities) and received, considered and given effect to third party requests. Australia actively works to publicly identify terrorists and terrorist organisations.

Furthermore, the TFS regime is administered robustly. Australia has procedures for:

1. the identification of targets for listing,
  2. a regular review of listings, and
  3. the consideration of de-listing requests and sanctions permits.

The authorities make a concerted effort to sensitize the public to Australian sanctions laws and to assist potential asset holders in the implementation of their obligations.

However, the private sector is not supervised for compliance with TFS requirements and was unable to demonstrate that the legal framework is effectively implemented. Effective implementation is difficult to confirm in the absence of freezing statistics, financial supervision, supervisory experience and feedback on practical implementation by the private sector. Designating Australians previously convicted for terrorism or terrorist financing, who openly join designated terrorist organisations could improve the system's effectiveness.<sup>3</sup>

NPOs are an area for improved efforts and specific action. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a targeted TF review and subsequent targeted TF-related outreach and TF-related monitoring of NPOs leaves NPOs and Australia vulnerable to misuse by terrorist organisations. Since 2010 there has also been no effort directed at NPOs to sensitise them to the potential risk of misuse for TF. While the Australian Charities and Not-for-Profits Commission (ACNC) actively works to improve transparency, it has no specific TF mandate and it has not conducted outreach to the NPO sector regarding TF risks.

3 At the time of the on-site, two of these individuals were under consideration by the government for designation. Designation of these two persons subsequently took place on 13 November 2014, after the on-site.

**Effectiveness****11. PF Financial sanctions****Substantial**

Australia demonstrates to a large extent the characteristics of an effective system in this area. The issues listed under IO10 and that relate to UNSCR 1267 also apply to IO11.

Even though IO11 suffers from the same issues as IO10, IO10 has additional shortcomings in relation to NPOs that do not apply to IO11. In addition, the overall domestic cooperation in relation to country sanction programmes for Iran and DPRK seems sound, which may have a positive effect on the implementation of targeted financial sanctions that are related to these country programmes. This domestic cooperation benefit does not apply in the case of IO10 / UNSCR 1267, which is not a country programme.

**Table 2: Compliance with FATF Recommendations**

Compliance with FATF Recommendations			
Recommendation	Rating	Factor(s) underlying the rating	
<b>1. Assessing risks &amp; applying a risk-based approach</b>	PC	<ul style="list-style-type: none"> <li>Mitigation policies have not been taken to mitigate high risks identified in the NTA related to certain entities and services.</li> <li>Most main, but not all, ML risks were identified and properly assessed.</li> <li>Reporting entities are not required to mitigate or carry out enhanced measures for high risks, identified by the authorities.</li> <li>Exemptions, and the application of simplified measures, are not based solely on low risk but include other variables such as regulatory burden and the desirability of promoting the risk-based approach.</li> <li>Scope issue - accountants, lawyers, trust and company service providers, most dealers in precious metals &amp; stones, and real estate agents are not reporting entities and thus not subject to risk mitigation requirements.</li> </ul>	
<b>2. National cooperation and coordination</b>	LC	<ul style="list-style-type: none"> <li>Australia does not have a formalised AML/CTF policy that draws on risks identified in the NTA and NRA.</li> </ul>	
<b>3. Money laundering offence</b>	C	The Recommendation is fully met.	
<b>4. Confiscation and provisional measures</b>	C	The Recommendation is fully met.	
<b>5. Terrorist financing offence</b>	LC	<ul style="list-style-type: none"> <li>The Australian definition of 'terrorist act' is somewhat narrower than the definition in Articles 2(1)(a) and (b) of the TF Convention.</li> <li>The provision or collection of funds to be used by an individual terrorist for any purpose is not covered.</li> </ul>	
<b>6. Targeted financial sanctions related to terrorism &amp; TF</b>	C	The Recommendation is fully met.	
<b>7. Targeted financial sanctions related to proliferation</b>	C	The Recommendation is fully met.	

## Compliance with FATF Recommendations

Recommendation		Rating	Factor(s) underlying the rating
<b>8.</b>	<b>Non-profit organisations</b>	NC	<ul style="list-style-type: none"> <li>• No sectorial TF risk assessment.</li> <li>• Subsequently, no relevant outreach to NPOs.</li> <li>• Subsequently, no relevant measures applied to those NPOs that would be identified as high risk and that account for a significant portion of the financial resources and/or international activities.</li> </ul>
<b>9.</b>	<b>Financial institution secrecy laws</b>	C	The Recommendation is fully met.

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
10. Customer due diligence	PC	<ul style="list-style-type: none"> <li>• Exemptions in operation within the AML/CTF Act and Rules may diminish the application of CDD in situations envisaged by the FATF Standard (e.g. signatories associated with an Australian correspondent banking relationship, no CDD requirements on reloadable stored value cards below a certain threshold or occasional transactions below nominated thresholds which appear to be linked).</li> <li>• There are deficiencies in the verification requirements in relation to an agent of a customer, trustees and beneficiaries.</li> <li>• Exemptions and simplified due diligence measures in relation to trusts that are registered and subject to regulatory oversight, and companies which are licensed and supervised, are not permitted by the standard and do not appear to be based on proven low risk.</li> <li>• There are deficiencies in the breadth of the identification information required across all legal persons / arrangements. Specifically, not all information specified in criterion 10.9 is required in each entity type and not all information collected is required to be verified.</li> <li>• There is no requirement to understand the control structure of non-individual customers, or understand the ownership structure.</li> <li>• There is no requirement to identify the beneficiary of a life insurance policy until payout.</li> <li>• Due to the wording of the requirements in relation to enhanced due diligence, a reporting entity may satisfy its enhanced CDD by completing identification which is considered normal due diligence.</li> <li>• There is no requirement in law to terminate the business relationship when the reporting entity is unable to comply with CDD requirements. The law does not permit reporting entities to stop performing CDD even if there is a risk of tipping off.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
11. <b>Record keeping</b>	LC	<ul style="list-style-type: none"> <li>• Certain customer-specific documents are exempt from record-keeping requirements.</li> <li>• There is no clear obligation in the AML/CTF Act that transaction records should be sufficient to permit reconstruction of individual transactions, although this is partly addressed by requirements in other legislation.</li> <li>• No formal requirement for reporting entities to ensure that the records be available swiftly to domestic competent authorities upon appropriate authority.</li> </ul>
12. <b>Politically exposed persons</b>	LC	<ul style="list-style-type: none"> <li>• The notions of close associate, which requires beneficial ownership of a legal person or arrangement, and of family members, which only apply to the spouse, parents and children, are too restrictive.</li> <li>• Important officials of political parties are not covered.</li> <li>• There is no specific requirement for life insurance.</li> </ul>
13. <b>Correspondent banking</b>	NC	<ul style="list-style-type: none"> <li>• The obligations to gather and verify information on the AML/CTF regulation applicable to the correspondent bank; the adequacy of its internal controls; information on the ownership, etc. only apply based on the risk evaluated by the reporting entity.</li> <li>• There are no specific obligations for payable-through accounts.</li> </ul>
14. <b>Money or value transfer services</b>	LC	<ul style="list-style-type: none"> <li>• There is no obligation for MTVS providers to include their agents in their AML/CTF programme, though it is permissible.</li> <li>• MTVS providers are not required to monitor their agents' compliance with the AML/CTF programme.</li> </ul>
15. <b>New technologies</b>	LC	<ul style="list-style-type: none"> <li>• There is no obligation specific to the identification, mitigation and management of the ML/TF risks posed by new technologies to reporting entities.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
<b>16. Wire transfers</b>	PC	<ul style="list-style-type: none"> <li>• The obligations in relation to the intermediary and the beneficiary financial institutions have not been updated to reflect FATF Recommendation 16.</li> <li>• MVTS providers are not required to apply the requirements of Recommendation 16 in the countries in which they operate.</li> <li>• No freezing action is undertaken in the context of Recommendation 16.</li> </ul>
<b>17. Reliance on third parties</b>	PC	<ul style="list-style-type: none"> <li>• It is not explicitly provided that the reporting entity relying on a third party remains ultimately responsible for CDD measures.</li> <li>• There is no obligation to gather information 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.</li> <li>• The geographic risk has not been taken into account when determining in which countries the third parties can be based.</li> </ul>
<b>18. Internal controls and foreign branches and subsidiaries</b>	PC	<ul style="list-style-type: none"> <li>• There is no obligation beyond the nomination at management level of a compliance officer, the audit function is limited and there is no indication of the frequency of the audit or guarantee of its independence.</li> <li>• These deficiencies also apply at the group level.</li> <li>• With respect to branches and subsidiaries located abroad, there is no obligation for financial institutions to apply the higher standard or Australia regime to the extent possible. There is 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/CTF measures consistent with Australia's AML/CTF regime</li> </ul>

### Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
<b>19. Higher-risk countries</b>	PC	<ul style="list-style-type: none"> <li>Reporting entities are required to apply enhanced due diligence to their relationships and transactions with DPRK despite the FATF's call to do so.</li> <li>Among the measures for enhanced due diligence listed in the Rules, some address normal due diligence rather than enhanced due diligence. See Recommendation 10.</li> </ul>
<b>20. Reporting of suspicious transaction</b>	C	The Recommendation is fully met.
<b>21. Tipping-off and confidentiality</b>	C	The Recommendation is fully met.
<b>22. DNFBPs: Customer due diligence</b>	NC	<ul style="list-style-type: none"> <li>Scope issue: DNFBPs other than casinos and bullion dealers are not subject to AML/CTF obligations.</li> <li>Casinos: The identification threshold exceeds that set forth in the Recommendation 22.</li> <li>See Recommendations 10, 11, 12, 15 and 17.</li> </ul>
<b>23. DNFBPs: Other measures</b>	NC	<ul style="list-style-type: none"> <li>Scope issue: DNFBPs other than casinos and bullion dealers are not subject to AML/CTF obligations.</li> <li>See Recommendations 18, 19, 20 and 21.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
24. Transparency and beneficial ownership of legal persons	PC	<ul style="list-style-type: none"> <li>• There is no clear process for the obtaining or recording of companies' beneficial ownership information. The processes for the creation and the public availability of information (including on beneficial ownership) relating to legal persons, other than companies and entities incorporated at State and Territory levels, vary throughout the country.</li> <li>• There is no mechanism to ensure that information on the registers kept by companies is accurate.</li> <li>• There is no requirement for companies or company registers to obtain and hold up-to-date information to determine the ultimate natural person who is the beneficial owner beyond the immediate shareholder. Companies are not required to take reasonable measures to obtain and hold this information.</li> <li>• Bearer share warrants are not prohibited and may be permissible.</li> <li>• There is not a general disclosure obligation regarding nominee shareholders.</li> <li>• Australia does not monitor the quality of assistance received from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad.</li> </ul>
25. Transparency and beneficial ownership of legal arrangements	NC	<ul style="list-style-type: none"> <li>• There is no obligation for trustees to hold and maintain information on trusts.</li> <li>• There is no obligation for trustees to keep this information up-to-date and accurate.</li> <li>• There is no obligation for trustees to disclose their status to financial institutions and DNFBPs.</li> <li>• There are no proportionate and dissuasive sanctions available to enforce the requirement to exchange information with competent authorities in a timely manner.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
26. <b>Regulation and supervision of financial institutions</b>	PC	<ul style="list-style-type: none"> <li>Absence of fit and proper obligations for currency exchange businesses.</li> <li>ML/TF risks of individual reporting entities are not adequately identified through AUSTRAC's risk-based approach</li> <li>The ML/TF risk profile relies too much on the amounts of the transactions reported.</li> </ul>
27. <b>Powers of supervisors</b>	PC	<ul style="list-style-type: none"> <li>AUSTRAC's powers (inspection and production of documents) are conditional upon the consent of the reporting entity. In absence of such consent, a court order is needed.</li> <li>Sanctions for the violation of AML/CTF obligations are civil and criminal penalties (fines and imprisonment). With the exception of remitters, AUSTRAC does not have the power to withdraw, restrict or suspend the reporting entity's licence. This power resides with the prudential regulator, who can only revoke a license for breaches of the Banking Act, its regulations, or the Financial Sector (Collection of Data) Act.</li> <li>Sanctions do not extend to directors and senior management.</li> </ul>
28. <b>Regulation and supervision of DNFBPs</b>	NC	<ul style="list-style-type: none"> <li>Scope issue: Only casinos and bullion dealers are subject to AML/CTF obligations.</li> <li>Casinos: State and Territory licensing authorities do not have express AML/CTF responsibilities to qualify as competent authorities. In addition, not all legislation requires the licensing authority to consider the associates of the applicants.</li> <li>See Recommendation 26.</li> </ul>
29. <b>Financial intelligence units</b>	C	The Recommendation is fully met.
30. <b>Responsibilities of law enforcement and investigative authorities</b>	LC	<ul style="list-style-type: none"> <li>In Queensland, ML prosecutions need to be authorised by the Queensland Attorney-General.</li> </ul>
31. <b>Powers of law enforcement and investigative authorities</b>	LC	<ul style="list-style-type: none"> <li>There is no mechanism in place to identify in a timely manner whether natural or legal persons own or control accounts.</li> </ul>

## Compliance with FATF Recommendations

Recommendation	Rating	Factor(s) underlying the rating
32. <b>Cash couriers</b>	LC	<ul style="list-style-type: none"> <li>Lack of either dissuasive or proportionate sanctions for cash couriers, inconsistent with overall risk and context.</li> </ul>
33. <b>Statistics</b>	LC	<ul style="list-style-type: none"> <li>Some statistics crucial to tracking the overall effectiveness and efficiency of the system related to investigations, prosecutions, convictions, and property confiscated are not maintained nationally, reflective of the wide range of agencies involved at the federal and State and Territory levels.</li> </ul>
34. <b>Guidance and feedback</b>	LC	<ul style="list-style-type: none"> <li>None of the guidance applies to most DNFBPs.</li> <li>Limited guidance available for identifying high risk customers or situations.</li> </ul>
35. <b>Sanctions</b>	PC	<ul style="list-style-type: none"> <li>The only sanctions available for violation of AML/CTF obligations are civil and criminal penalties (fines and imprisonment) imposed by a court. The range of fines is sufficiently broad to be viewed as allowing proportionate and dissuasive sanctions.</li> <li>Sanctions do not apply to most DNFBPs as they are not regulated by competent authorities.</li> <li>Sanctions do not extend to directors and senior management if it is the reporting entities that breach the AML/CTF Act or rules.</li> </ul>
36. <b>International instruments</b>	LC	<ul style="list-style-type: none"> <li>Deficiencies in the TF offence (i.e. the scope of terrorist acts covered in the TF Convention) affect the implementation of this convention.</li> </ul>
37. <b>Mutual legal assistance</b>	C	The Recommendation is fully met.
38. <b>Mutual legal assistance: freezing and confiscation</b>	C	The Recommendation is fully met.
39. <b>Extradition</b>	C	The Recommendation is fully met.
40. <b>Other forms of international cooperation</b>	C	The Recommendation is fully met.

# Mutual Evaluation of Australia

## Preface

This report summarises the AML/CTF measures in place in Australia as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Australia's AML/CTF system, and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by Australia, and information obtained by the evaluation team during its on-site visit to Australia from 30 July to 12 August 2014 and during a face-to-face meeting with Australia from 7 to 9 January 2015.

The evaluation was conducted by an assessment team consisting of:

- Mr. Cheng Khai LIM, Monetary Authority of Singapore (financial expert)
- Mr. Marijn RIDDERIKHOF, Dutch Central Bank, the Netherlands (financial expert)
- Ms. Erin SCHENCK, Department of the Treasury, the United States (financial expert)
- Ms. Anne-Mette WADMAN, Økokrim (the FIU), Norway (law enforcement expert)
- Mr. Wayne WALSH, Department of Justice, Hong Kong, China (legal expert)
- Mr. Steve DAWE, International Monetary Fund
- Mr. Kevin VANDERGRIFT, senior policy analyst, Mr. Richard BERKHOUT and Ms. Alexandra ECKERT, policy analysts, FATF Secretariat
- Mr. Gordon HOOK, Executive Secretary of Asia-Pacific Group

The report was reviewed by Mr. Nigel BARTLETT, World Bank; Mr. Ian MATTHEWS, Financial Conduct Authority, the United Kingdom; Ms. Josée NADEAU, Department of Finance, Canada; and Mr. Pieter SMIT, Financial Intelligence Centre, South Africa.

Australia previously underwent a FATF Mutual Evaluation in 2005, conducted according to the 2004 FATF Methodology. The 2005 evaluation has been published and is available at [www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Australia%20full.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/mer/MER%20Australia%20full.pdf). For the sake of brevity, on those topics where there has not been any material change in the situation of Australia or in the requirements of the FATF Recommendations, this evaluation does not repeat the analysis conducted in the previous evaluation, but includes a cross-reference to the detailed analysis in the previous report.

Australia's 2005 Mutual Evaluation concluded that the country was compliant with 12 Recommendations; largely compliant with 14; partially compliant with 13; and non-compliant with 10. Australia was rated compliant or largely compliant with 13 of the 16 Core and Key Recommendations. Australia was placed under the regular follow-up process immediately after the adoption of its 3<sup>rd</sup> round Mutual Evaluation Report; however, due to the lack of progress, it was placed under the enhanced follow-up process in February 2012. Australia exited the follow-up process in June 2014 as it had achieved a satisfactory level of compliance with all Core and Key Recommendations.



# 1. ML/TF RISKS AND CONTEXT

1

1.1. The Commonwealth of Australia occupies a land area of about 7.7 million square kilometres, making it the 6th largest country in the world. Australia's population is currently about 23.5 million. More than a quarter of Australians were born overseas. Australian territory cannot be reached by land. Neighbouring countries are Indonesia, East Timor and Papua New Guinea to the north; the Solomon Islands, Vanuatu and France (French Caledonia) to the north-east; and New Zealand to the south-east. Papua New Guinea was a Territory of Australia between 1949 and 1975; close (economic) ties remain until today. The remaining (self-governing) external territories of Australia are Norfolk Island, Christmas Island and Cocos (Keeling) Islands. Other (mostly) uninhabited Australian territories are Ashmore and Cartier Islands, the Coral Sea Territory, Heard Island and McDonald Islands. Australia claims a piece of Antarctica.

1.2. Australia has a federal system of government that consists of the Federal government, six State governments, and two Territory governments. The main criminal law powers rest with the States and Territories. Federal legislation is generally restricted to criminal activity against federal interests. The Australian Parliament's role in making legislation is limited to specific "heads of power" issues including, trade and commerce with other countries, and among the States; taxation; currency, banking, other than State banking; external affairs; and other matters referred to the Australian Parliament by the States. State and Territory legislation relates to criminal activity against any non-federal interests located within the geographical area of the particular State or Territory. Accordingly, the majority of criminal law proceedings in Australia are State or Territory proceedings.

1.3. Australia's federal Parliament consists of two houses, a Senate and a House of Representatives. The Australian Constitution also established a High Court of Australia, which can decide cases in first instance and on appeal from other federal courts or State or Territory courts. There is also a system of federal courts below the High Court, established by legislation. The establishment of a federal judiciary did not significantly affect the State judiciaries; each State continues to have its own Supreme Court and inferior courts.

1.4. Australia is a wealthy G20 member with the world's 12th largest economy (GDP was about USD 1.5 trillion in 2013) and 7th highest average income per capita (about USD 67 000). The national currency is the Australian dollar (AUD), which is also the currency used in Kiribati, Nauru, and Tuvalu.

## 1.1 ML/TF Risks

1.5. This section of the report presents a summary of the assessment team's understanding of the ML/TF risks in Australia. Australia's assessment and understanding of the risk is set out in Chapter 2. The summary is based on material provided by Australia, open source material, as well as discussions with competent authorities and the private sector during the on-site visit. This includes consideration of Australia's 2011 National Threat Assessment on Money Laundering (NTA)<sup>1</sup> and National Risk Assessment on Terrorist Financing 2014 (NRA)<sup>2</sup>. The NTA's scope, inputs, and focus limits its value to assess ML risks whereas the NRA reliably assesses TF risks (see Chapter 2).

1 Austrac (2011).

2 Austrac (2014).

- The NTA identified illicit narcotics, and tax frauds (and other frauds) as the major predicate crimes for ML. Drug trafficking and tax evasion generate the most significant amount of the illicit proceeds investigated by authorities. However, there is no current estimate of proceeds generating crime in Australia. The authorities utilize a conservative estimate, based on 2009 material, that organised crime costs the Australian economy 1.5% of GDP; however authorities do not have an estimated figure for the amount of criminal proceeds. For general context (but not for comparison) it is noted that Australia convicts around 135 000 offenders annually for predicate crimes (see chart at paragraph 2.28).<sup>3</sup> The main predicate crimes where convictions are obtained are illicit drug offences, theft, and fraud or deception offences.
- The channels that were identified as highly vulnerable to ML activity were the banking sector, money remitters (both licensed and underground operators), gatekeepers, and the abuse of corporate vehicles. The risks are exacerbated by launderers often using false identity documents.
- Australian drug markets are said to be some of the world's most profitable and most drugs can be obtained. They are a serious and growing issue. In 2012-13, drug seizures and arrests were at record or decade highs for nearly all drug types.<sup>4</sup> Cannabis dominates domestically, but the drugs of greatest concern are amphetamine-type stimulants. Drug trafficking in Australia is linked to transnational organised crime groups, particularly from South East Asia and South America.
- Authorities have found that organised criminal groups use complex corporate vehicles to conceal and launder proceeds, which are often sent out of Australia as part of the laundering process or to fund more drug-related activity. Trade-based ML may also be an emerging threat to Australia.
- China; Hong Kong, China; Macao, China; Singapore and the United Arab Emirates were seen as major source, destination, and/or transit jurisdictions for proceeds of crime laundered into and out of Australia. Large amounts are suspected to be laundered out of China into the Australian real estate market. China and other countries within the Asia-Pacific region were also seen as likely sources of corruption proceeds that are laundered in Australia.
- Authorities consider that international laundering of tax crime proceeds is primarily outwards, involving havens in Europe as well as Vanuatu in the Pacific although many such proceeds eventually return to Australia. Overall the authorities' view may downplay potential inwards laundering from the United States, the United Kingdom, and other parts of Europe, and outwards laundering in New Zealand, Canada, and the United States as evidenced by recent ML and proceeds related mutual legal assistance requests.
- TF risk is largely influenced by international tensions and conflicts, in particular Syria and Iraq. The main domestic risks involve small-scale collection and use of legitimate and illegitimate funds by domestic cells aligned with or sympathetic to radicalised Islamic jihadist groups abroad, for the purposes of committing domestic terrorist acts.
- The authorities have periodically and successfully disrupted domestic terrorism plots and associated funding (albeit involving relatively low levels of funds) although this remains a constant risk. In addition, in recent years and on isolated occasions, ransoms have been paid by families and businesses to release Australians held hostage by terrorists.
- The most significant emerging TF risk is the potential for groups as well as other individuals to send money, directly or indirectly, or raise money for, or otherwise support Australians travelling to conflicts zones abroad (especially Syria and Iraq) to support foreign terrorist groups and terrorist

<sup>3</sup> Some crimes committed within crime categories that are predicates for money laundering may not generate proceeds. Accordingly, this contextual data has not been used to compare results of ML efforts.

<sup>4</sup> Australian Crime Commission ( 2014).

acts, both abroad and domestically. In this context, the primary destinations for current TF flows from Australia were understood to be Syria and Iraq, with the funds often passing through other jurisdictions en route. Some Australians have funded travel for themselves from legitimate sources to fight in conflict zones, and some funds have also been raised through abusing registered and informal “pop-up” charities linked to humanitarian fund-raising.

- Charities and other NPOs are a channel of higher risk for use to raise funds for TF in or from Australia, although identified misuse of NPOs is low. However, the lack of a comprehensive sectorial risk assessment, the lack of subsequent outreach in relation to TF to the sector, and the lack of adequate preventive requirements or a supervisory framework that cover all relevant NPOs, leave them vulnerable to misuse by terrorist organisations.

## 1.2 Materiality

1.6. The Australian economy has performed well relative to many other advanced economies since the global financial crisis, with recent trend growth of around 3%. Australia has low unemployment, low inflation, and a highly skilled workforce. The services sector accounts for around 70% of the Australian economy and four out of five jobs, with the largest service-based industries being financial and insurance services. Of the non-services sector, the largest industry is mining. Australia's exports are dominated by goods exports, in particular resources, rural commodities and manufactured goods (around 60%, 11%, and 13% of total exports respectively). Most trade is with Asia, particularly China, Japan, the Republic of Korea, India, and ASEAN countries. Australia also has other strong links with Asia, being home to around two million people born in Asia. Similar numbers of Australians visit Asia yearly, and about three-quarters of international students in Australian higher education were born in Asia.

1.7. Australia's financial sector is large and mature with assets totalling 340% of GDP (indicating that financial institutions provide substantial services to non-residents). The sector is dominated by four large banks. The IMF's 2012 Financial Sector Assessment Program found Australia's financial system to be sound and well managed, with the financial prudential regulatory and supervisory framework exhibiting a high degree of compliance with international standards.

## 1.3 Structural Elements

1.8. The key structural elements for effective AML/CTF controls appear to be present in Australia. Political and institutional stability, accountability, and rule of law are all present. There is a professional and independent judicial system, both at State/Territory and federal level. Most States have Independent Corruption Commissions (ICC), some with far reaching powers, which also aim to counter corruption at the political level. In 2012, the review of Australia's compliance with the United Nations Convention Against Corruption commended Australia for its comprehensive and proactive anti-corruption arrangements. The federal government's approach to combating corruption is based on a multi-agency model, which vests specialised functions and responsibilities in a number of agencies. There is no federal ICC. The institutional AML/CTF framework is centred around AUSTRAC, an independent agency within the federal Attorney-General's portfolio. For a full overview of the institutional framework see Section 2.1(b).

## 1.4 Other Contextual Factors

1.9. Australia has a mature and sophisticated AML/CTF regime, with a correspondingly well-developed legal and institutional framework.

1.10. Combating corruption is a key priority for the public and the government, with corruption cases pursued by independent corruption commissions (at the State level), law enforcement (all levels), royal commissions, and the media. Close ties between business/labour unions and politicians and the absence of comprehensive party funding may be a specific vulnerability. Media and law enforcement attention for

corruption is widespread, public tolerance for corruption and corruption-related issues seems to be low, and there is no evidence that corruption is widespread in Australia.

## 1.5 Scoping of Higher-Risk Issues

1.11. In deciding on issues to prioritise, the assessment team reviewed material submitted by Australia on national ML and TF risks, and from open sources. During the on-site, the assessment team gave increased focus to the areas below. The issues listed present not only areas of higher ML/TF risks (including threats and vulnerabilities), but also contain issues that were of significant interest or concern to the assessment team based on material provided before and during the on-site visit.

### *Legal/operational issues*

1.12. **Federal – State/Territory coverage, co-operation, and targeting ML and proceeds of crime, including confiscation:** While the Commonwealth level has the lead on AML/CTF issues, many of the predicate offences are criminalised only at the State/Territory level. The information provided to the assessors by federal agencies almost exclusively focuses on the federal level, reflecting the federal system of government. The evaluation team explored with investigators and prosecutors at both federal and State/Territory level to find out how those parts of the system are cooperating and performing, and the priority they give to pursuing ML rather than predicate offences as the data provided on ML convictions suggest these are low relative to predicate crime convictions.

1.13. **Predicate offences:** The magnitude of organised crime, narcotics, fraud, robbery/theft and, and foreign predicates, in particular corruption. Having reviewed other material that does not seem to have been factored into the NTA<sup>5</sup> on the predicate crimes producing significant proceeds, the team explored the nature of the ML threat in Australia, and relative magnitude across crime types, and how authorities are pursuing ML cases related to these offences to consider whether sufficient priority is being given to the pursuit of ML investigations and prosecutions.

1.14. **Misuse of corporate vehicles, trusts, and NPOs:** Measures to prevent the misuse of legal persons and legal arrangements may not be adequate, and Australia's NTA identifies numerous ML schemes using corporate vehicles. However, it is not clear whether Australia has fully assessed the ML/TF risks posed by these vehicles. The team therefore explored the extent to which authorities can obtain accurate and up-to-date information on beneficial ownership in a timely manner. **Non-profit organisations** have also been identified as a channel to raise and move terrorism funds in Australia<sup>6</sup>, and the team explored the adequacy of oversight of the NPO sector.

### *Financial and DNFBP sector vulnerabilities*

1.15. **Effectiveness of the AML/CTF regulatory and supervisory framework:** AUSTRAC is Australia's AML/CTF supervisor. Australia's regulatory framework is very complex, and the team explored how well the various parts of the financial sector and DNFBPs (where they do have AML/CTF obligations) were aware of and understand their obligations and were adequately identifying, assessing, and mitigating ML/FT risk. The team further explored the adequacy of AUSTRAC's risk analyses for the various sectors, including exemptions from AML/CTF obligations. The team also examined on-site and off-site supervisory programmes, feedback, and follow-up, including sanctions and other corrective measures to enhance AML/CTF compliance and mitigate ML/TF risk.

5 E.g. Australian Institute of Criminology (AIC) Counting the costs of crime in Australia a 2005 update, 2008 (which suggests substantial proceeds from cannabis and fraud); Australian Bureau of Statistics The Non-Observed Economy and Australia's GDP, 2012 (which also suggests substantial proceeds from cannabis).

6 AIC (2012), pp. 19-20.

1.16. **Gatekeepers and other DNFBPs (in particular lawyers, accountants, notaries, and real estate):** Lawyers and accountants are identified in Australia's NTA as facilitating the establishment of legal structures and advice to facilitate ML by organised crime groups. The NTA also particularly indicates that overseas-based crime groups buy real estate (as well as other high-value goods) in Australia to conceal their criminal proceeds. Most DNFBPs do not have comprehensive AML/CTF obligations, so the team explored the policy, legal, budgetary or other reasons for their non-coverage.

## References

- AIC (2012), *Money Laundering and Terrorism financing risks to Australian non-profit organisations*, Australian Institute of Criminology, Canberra,  
[www.aic.gov.au/publications/current%20series/rpp/100-120/rpp114.html](http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp114.html)
- AUSTRAC (2011), Money Laundering in Australia 2011, Commonwealth of Australia, West Chatswood,  
[www.austrac.gov.au/sites/default/files/documents/money\\_laundering\\_in\\_australia\\_2011.pdf](http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf)
- AUSTRAC (2014), Terrorism financing in Australia 2014, Commonwealth of Australia, West Chatswood,  
[www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf](http://www.austrac.gov.au/sites/default/files/documents/terrorism-financing-in-australia-2014.pdf)
- Australian Crime Commission (2014), *Illicit Drug Report 2012-13*, Australian Crime Commission, Canberra,  
[www.crimecommission.gov.au/sites/default/files/290414-IDDR-2012-13.pdf](http://www.crimecommission.gov.au/sites/default/files/290414-IDDR-2012-13.pdf)

1



## 2. NATIONAL AML/CTF POLICIES AND COORDINATION

2

### Key Findings

**Overall, Australian authorities have a good understanding of most of Australia's main ML risks but need to develop their understanding further in certain areas.** They coordinate very well activities to address key aspects of the ML/TF risks **but there remain some key risks unaddressed, and an underlying concern that the authorities are addressing predicate crime rather than ML.**

Australia recognises the need to continue to update and take further measures to fully identify, understand, address, and communicate to the relevant sectors the full range of ML risks now occurring in Australia.

**Australia needs to take further actions to address the risk of gatekeepers and corporate vehicles as channels to facilitate ML**, as identified in the NTA , including by bringing all DNFBPs within the scope of the AML/CTF regime (and as required by the FATF Recommendations).

**Authorities have a good understanding of their TF risks and are addressing them. They assess that TF is largely motivated by international tensions and conflicts.**

**National AML/CTF coordination at the operational level is very comprehensive, but demonstrating its overall success is challenging, although results from national task forces are showing positive trends.** There is not enough focus on how to monitor and measure success, and there are limited national mechanisms or metrics actively in place to measure how effective or efficient the AML/CTF system is.

## 2.1 Background and Context

### (a) Overview of AML/CTF strategy

2.1. Australia has no articulated AML/CTF policy or strategy but does have a national strategy for combating organised crime – the Commonwealth Organised Crime Strategic Framework – which identifies ML as an intrinsic enabler of organised crime. The key elements of that Framework are the Australia Crime Commission's (ACC) biennial Organised Crime Threat Assessment (OCTA) that provides a picture of the most significant threats and harms arising from organised criminal activity; a National Organised Crime Response Plan (NOCRP) which includes strategies and priorities for national and multi-jurisdictional approaches to key risks within the organised crime environment; and multi-agency responses to develop and deliver operational, policy, regulatory and legislative responses to organised crime. Australia also has an AML/CTF interdepartmental committee (AML IDC) (see TC Annex) at the federal level that sets priorities through an annual work plan. The most recent work plan's priorities include improving customer due diligence measures, reviewing the operation of AML/CTF legislation, enhancing data matching to improve the intelligence value of AUSTRAC information, and expanding the range of agencies that can access and use AUSTRAC information. More directly related to combating national ML/TF risks are the plans of individual agencies and task forces but these tend to focus on combating the underlying predicate crimes or terrorism rather than ML or TF, reflecting Australia's focus on crime disruption (see below). TF risks are addressed as part of AML/CTF policy and national security and counter-terrorism strategies as appropriate.

### (b) The institutional framework

2.2. The following are the main ministries, agencies, and authorities responsible for formulating and implementing the federal government's AML/CTF policies:

- **Attorney General's Department (AGD)** — has policy responsibility for AML/CTF. It is also Australia's central authority for extradition and mutual legal assistance in criminal matters.
- **Australian Crime Commission (ACC)** — is Australia's national criminal intelligence agency - focused on understanding and combating serious and organised crime of national significance. Its Board is chaired by the Australian Federal Police (AFP) Commissioner and includes all State and Territory Police Commissioners, the Secretary of AGD, the Director-General of Australian Security Intelligence Organisation (ASIO), the CEO of the Australian Customs and Border Protection Service (ACBPS), the Commissioner of Taxation and the Chair of the Australian Securities and Investment Commission (ASIC); AUSTRAC's CEO is an observer.
- **Australian Customs and Border Protection Service (ACBPS)** — monitors and detects the illegal movement of people, goods, and illicit cash across the border. It also administers border controls on UN sanctioned goods to prevent activities that may contribute to the proliferation of weapons of mass destruction.
- **Australian Federal Police (AFP)** — is responsible for investigating serious and complex crime against the federal government. It heads up the multi-agency Criminal Asset Confiscation Taskforce (CACT) and the Terrorism Financing Investigations Unit (TFIU).
- **Australian Intelligence Community (AIC) agencies<sup>1</sup>** — have intelligence and operational roles for aspects of ML/TF matters, as well as counter-proliferation.

1 The Australian Intelligence Community, or AIC, is an informal term used to describe the six Australian security and intelligence agencies: The Office of National Assessments; Australian Security Intelligence Organisation; Australian Secret Intelligence Service; Australian Signals Directorate; Defence Intelligence Organisation; and Australian Geospatial Intelligence Organisation.

- **Australian Prudential Regulation Authority (APRA)** — is Australia's prudential supervisor for authorised deposit-taking institutions (banks, building societies and credit unions), life and general insurance and reinsurance companies, friendly societies and superannuation funds (excluding self-managed funds).
- **Australian Securities and Investment Commission (ASIC)** — is responsible for financial market integrity, business conduct and disclosure, and consumer protection in the financial system. It registers Australian companies and regulates financial markets, financial services organisations, and professionals who deal and advise in investments, superannuation, insurance, deposit taking and credit.
- **Australian Taxation Office (ATO)** — is the federal government's principal revenue collection agency. It investigates tax crimes and provides information to law enforcement to assist with investigations into other crimes.
- **Australian Transaction Reports and Analysis Centre (AUSTRAC)** — Australia's AML/CTF regulator and financial intelligence unit (FIU).
- **Commonwealth Director of Public Prosecutions (CDPP)** — prosecutes offences against federal law, which includes ML and TF offences.
- **Department of Foreign Affairs and Trade (DFAT)** is responsible for the implementation and administration of Australia's targeted financial sanctions.
- **Australian Charities and Not-for-Profits Commission (ACNC)** seeks to maintain, protect and enhance public trust and confidence in the NPO sector.
- Each State and Territory also has its own police force and DPP. Most States and Territories also have specialist crime commissions and some have anti-corruption commissions.

### (c) *Coordination and cooperation arrangements*

2.3. **Australia has a wide range of arrangements in place for AML/CTF coordination and cooperation at both the policy and operational levels.** The main federal coordinating body is the AML IDC which meets to share information and inform the strategic direction and priority setting of federal agencies working on domestic AML/CTF initiatives.<sup>2</sup> Coordination of AML/CTF-related activities also occurs through the NOCRP and other inter-departmental fora that coordinate law enforcement policy issues.<sup>3</sup>

2.4. **Operational activities are coordinated using a mixture of standing committees and task forces that include federal and State/Territory agencies.** A key body is the ACC Board described above. The Board determines national criminal intelligence priorities and special operations and investigations. Task forces are used as a mechanism to coordinate operational activities. These task forces target specific areas of concern where laundering activity is involved such as the remittance sector (Eligo National Task Force), criminal gangs (Task Force Attero), tax crimes (Project Wickenby), serious and organised investment fraud (Task Force Galilee), and asset confiscation (CACT). The use of criminal intelligence is also coordinated via the ACC National Criminal Intelligence Fusion Capability and via AUSTRAC providing online access to its transaction reports database as well as posting liaison officers in some partner agencies. In addition, Joint Management Groups (JMGs) operate in each of Australia's States/Territories to coordinate operational interaction between federal and State/Territory law enforcement and regulatory agencies.

<sup>2</sup> The AML IDC is chaired by the AGD and also comprises representatives from AUSTRAC, the AFP, the ACC, DFAT, Customs, the Treasury, the ATO and the CDPP. It meets two to three times each year as needed.

<sup>3</sup> E.g. the Heads of Operational Commonwealth Law Enforcement Agencies – meets twice-yearly and serves as the primary forum for 14 federal agencies to discuss law-enforcement policy issues.

2.5. CTF policy is coordinated by the AML IDC as well as broader counter-terrorism coordinating bodies, led by the Australia-New Zealand Counter-Terrorism Committee. CTF operational matters are coordinated through a multi-agency Terrorism Financing Investigations Unit.

2.6. **DFAT chairs and services a number of counter-proliferation coordination groups.** The main group comprises: DFAT (Chair), Department of Prime Minister and Cabinet, Department of Defence, AGD, ACBPS, the AIC agencies, and other agencies co-opted as necessary.

*(d) Country's assessment of risk*

2.7. **Australia has produced two reports on its national ML/TF risks, which are supplemented by ongoing risk analysis efforts.** Those efforts include an Organised Crime Threat Assessment (OCTA) (produced by the ACC every two years) that focuses on aspects of the predicate crime environment, dynamic analysis processes stemming from strong inter-agency cooperation and joint-task forces, as well as studies into specific risk areas.

2.8. **Australia conducted its first National Threat Assessment on Money Laundering (NTA) in 2011 and published a summarised version.** The NTA assesses ML threats and also assesses high-risk countries that influence Australia's ML environment. It was produced prior to FATF adopting Recommendation1 or publishing guidance on assessing ML/TF risk. The NTA tends to follow an approach similar to FATF's Money Laundering and Terrorist Financing Global Threat Assessment 2010, focusing mainly on the channels identified as vulnerable to laundering proceeds in the private sector. It is primarily a qualitative assessment using federal law enforcement cases and information in the AUSTRAC database to identify ML channels and typologies. While the NTA identifies and assesses most of the main risks, the assessors question whether the scope, inputs, and focus limit the analysis in relation to some other ML risk areas.

2.9. **The NTA's conclusions reasonably reflect most of Australia's main risks (which likely still prevail), but the NTA is now three years old and assessors are not confident that it is current for all risks, including where subsequent assessments have superseded it in some areas (e.g. on cryptocurrencies, TBML and financial and investment sector fraud).** The NTA, in particular, looked at some but not all potential AML/CTF regime vulnerabilities. It may not have identified or assessed new and emerging risks reflected in the latest FATF Standards, and potentially failed to identify some risks (e.g. foreign predicate risk). The NTA relied on the 2010 OCTA and other criminal intelligence for setting the broader crime environment. However, not all of the predicate crimes producing significant proceeds (such as the large domestic cannabis market) are assessed or examined as ML risks as fully as may have been expected. Nevertheless, Australia's understanding of risk has since been supplemented by other mechanisms as set out in paragraph 2.1 above, for example the biennial OCTA. In addition, the ACC has produced many intelligence products which deal with either ML/TF specifically or are ML/TF related.

2.10. **Australia has used the results of the NTA to help shape aspects of how it combats ML.** The AML/CTF regime is calibrated around mitigating risks from organised and serious crimes with the regulatory focus on banks, the gaming sector, and remitters – seen in the NTA as the main channels for ML (and also TF for the latter). Specifically, the NTA appears to have been a substantial driver for the creation of a remittance task force in December 2012.

2.11. **The NRA focuses on TF risks which impact on Australia's domestic environment.** It assesses the risk associated with the methods and financial channels used to raise or transfer funds for TF. High-risk countries which influence TF in Australia are also examined. It was coordinated by AUSTRAC, finalised in April 2014, and prepared with input from intelligence held across law enforcement and national security agencies. The methodology used, which drew on the NTA and modified it to take into account the FATF guidance on conducting ML/TF risk assessment, was superior to that used for the NTA such that the assessors are confident that it more likely identifies and assesses the TF risks in Australia. The NRA is being used to help guide agencies on how to combat TF in Australia.

## 2.2 Technical Compliance (R.1, R.2, R.33)

2.12. See for the full narrative the technical compliance annex:

- **Recommendation 1 (assessing risks and applying a risk-based approach) is rated partially compliant.**
- **Recommendation 2 (national cooperation and coordination) is rated largely compliant.**
- **Recommendation 33 (statistics) is rated largely compliant.**

2

## 2.3 Effectiveness: Immediate Outcome 1 (Risk, Policy and Coordination)

2.13. **Australia exhibits many characteristics of an effective system** but needs to implement moderate improvements in the way that it formulates and implements its AML/CTF policies and activities. This includes moving beyond the current primary focus on predicate crime to formulating and implementing policies more specifically aimed at mitigating the ML/TF risks.

### *Understanding risk*

2.14. **Overall, the authorities demonstrated a good understanding of most of Australia's main ML risks but need to develop their understanding further in certain areas.** Due to the dynamic ongoing risk analysis processes employed, the authorities' understanding of Australia's ML risks is not reliant solely on the NTA. They demonstrated very good understanding of aspects of the risks associated with the predicate crime environment, domestic geography, aspects of cross-border flows, the channels most vulnerable to laundering, and customer risks (including involving complex corporate structures), but somewhat less understanding of risks linked to system vulnerabilities. While having a comprehensive understanding of some aspects of nature and size of the proceeds of crime environment, the authorities acknowledged that they could improve the depth of their understanding particularly in State and Territory police agencies. Recent OCTAs have focused on improving the understanding of a wide range of "serious and organised" crime markets. The ACC was working on, and finalised after the on-site, a Financial Crime Risk Assessment, which should provide greater depth and detail about complex financial crimes and which can inform future ML risk assessments. Sydney and Melbourne were universally understood as the primary sources of domestic proceeds as well as the favoured geographic zones for domestic laundering.

2.15. **There seemed to be a fairly good and universal understanding in relation to specific aspects of cross-border illicit flows.** Australian authorities have largely focused on outgoing high-risk funds but recognise, based on recent operational findings, among other things, that more attention needs to be paid to understanding potential incoming laundered flows. In addition, the authorities demonstrated differing views about the extent to which Australia is exposed to trade-based ML, although they have taken some steps to begin addressing the issue.

2.16. **There was also a very good and almost universal understanding of most channels that were identified as highly vulnerable to ML activity in the NTA.** The authorities demonstrated a very good understanding of placement risk associated with mainly drug crime, as well as risks associated with more sophisticated aspects of laundering activity. However, while the gaming sector, high value goods, and real estate were identified as high threat in the NTA, the authorities did not convey that same understanding of their risk levels in their meetings with the assessment team – particularly at the federal level (but a number of case studies show they have successfully investigated ML involving these sectors)..

2.17. **There was insufficient understanding demonstrated of the extent to which Australia could be exposed to ML or TF risk through potential vulnerabilities such as gaps in the AML/CTF laws and regulations, weaknesses in the way that the authorities carried out their roles, or a lack of resources in AML/CTF agencies.**

2.18. **Australia could possibly forge a stronger consensus about the understanding of risks by formalising its ongoing efforts to analyse risk understanding.** Understanding ML risks has been supplemented since the NTA through ongoing dialogue amongst Australian authorities but their views about some of those risks vary. While some variance is expected, there could be merit in having the AML IDC formally adopt future NTAs and findings that updated parts of Australia's ML risk profile in between iterations of the NTA. Moreover, this would also help spread ownership of the NTA to assist AUSTRAC to engage more agencies nationally to contribute to the assessment.

2.19. **The authorities demonstrated a deeper understanding of the TF risk than was contained in the public version of the NRA.<sup>4</sup>** They assessed that TF is largely motivated by international tensions and conflicts. The primary destinations for current TF flows from Australia were understood to be Syria and Iraq, with the funds often passing through other jurisdictions *en route*. The authorities did not see any evidence that TF funds were flowing into Australia to fund domestic terrorism or to be re-directed to other countries. "Lone-wolf" operators and small domestic groups (sympathetic with foreign Jihadist groups) were understood as the primary terrorism, and thus TF, risk both domestically and trans-nationally. Sydney and Melbourne were seen as the most likely fund-raising locations. Funds move out of Australia through banks or remitters or travel with those moving to conflict zones. There had also been a small number of incidents of Australian businesses paying ransoms to terrorist groups in Africa.

### *Addressing risks*

2.20. **The authorities demonstrated areas where national policies and activities were addressing Australia's main ML risks and that they are largely addressing TF risks** (particularly by disrupting domestic terrorist activities, as discussed in Chapter 4 below), **but there remain some key risks unaddressed, and an underlying concern that the authorities are addressing predicate crime rather than ML.** The main criminal threats universally identified where national policies pursued ML, were drug trafficking and tax evasion, but the authorities did not demonstrate that their policies focused much attention on addressing laundering activity from other crimes (including foreign predicates). National policies to address drugs and tax crimes have led to the establishment of the ATO-led Project Wickenby in 2006, the Criminal Assets Confiscation Taskforce in 2011, and the Eligio National Task Force in 2012. Fraud was a high-risk predicate in the NTA and while national policies exist focusing on the predicate crime (e.g. the ACC-led Task Force Galilee was established in 2011 to address serious and organised investment fraud), the ML risk could be better addressed, including by having investigative agencies place more emphasis on pursuing criminal ML charges for large frauds and recovering the related proceeds using criminal processes. Present policies emphasise assisting some victims of large frauds to pursue stolen assets using civil processes (see IO7 and IO8). And while some laundering activity is being disrupted, investigators shared frustrations at being unable to effectively pierce complex corporate structures and suggested that this may be contributing to challenges in securing substantive ML or other convictions against senior members of major drug or ML networks, and the low level of proceeds confiscations relative to the estimated size of drug markets (see IO5, IO7, and IO8). Thus, Australia's AML/CTF efforts could be enhanced by addressing risks associated with the abuse of companies and trusts, including by developing improved legal mechanisms to obtain beneficial ownership of companies and trusts. In particular, the authorities would probably benefit from a central register of trusts. Further areas where Australia could do more to calibrate its policies to address its risks are discussed below and in greater detail under each relevant IO).

2.21. **The authorities claim that their policy of disrupting organised and serious crime addresses ML/TF risk but assessors were not presented with convincing evidence of how effective disruption was at combating ML.** Australia considers that ML investigations form one component of a holistic strategy to prevent, deter and interrupt criminal activity and that predicate offending and money laundering are not mutually exclusive. Australia argues that following the money results in the investigation of money laundering offences also provides a benefit for investigating predicate offences. Thus, due to the transnational nature of most predicate crimes generating substantial proceeds in Australia, Australia has responded by prioritising

<sup>4</sup> A sanitised version of the NRA was published on 11 September 2014, too late after the on-site visit to be taken into account for the purposes of determining ratings.

an international disruption strategy that involves arrest and prosecution of those involved in serious and organised crime (often for the predicate offence) but also international collaboration to target criminal syndicates and their senior controllers as key parts of responding to crime. This strategy is presented as partly explaining why domestic ML convictions might be lower than could be expected, relative to Australia's ML risk profile. Challenges remain in demonstrating how successful the strategy is. In addition, the assessors note that while this policy of disruption does not fit within the "alternative measures" approach contemplated in Core Issue 7.5 of the Methodology (see IO.7), but disruption strategies can fit under IO.1 if assessors are convinced that it contributes to combating ML.

2

**2.22. Authorities pointed to areas where disruption had hardened the environment and forced criminals to move offshore and change ML methodologies, as illustrating that the disruption strategy was addressing the ML risks. However, the assessors were not convinced that changing rather than reducing behaviour amounts to addressing or mitigating ML risks.** Examples of criminals changing their *modus operandi* include some organised criminal syndicate principles moving offshore to avoid detection and arrest, and their use of "clean-skin" non-resident mules who quickly carry out structured deposits. These make it difficult for law enforcement to take action before the mules have left the country and the funds have moved offshore, into untraceable corporate structures, or both. While the authorities cited intelligence that pointed to launderers changing to other methods due to disruption activity, some law enforcement and the private sector said that financial crime, including money laundering, was not decreasing, instead, the criminals were just changing their behaviours. This is a major challenge in an area of criminal activity where perpetrators adapt, regroup, and shift their methodologies.

**2.23. The authorities have addressed some vulnerabilities in the regulatory framework by introducing new CDD requirements and regulation and supervision focuses on addressing risks in banks, the gaming sector, and remitters consistent with the NTA, but need to take further measures to address the ML risks associated with gatekeepers and corporate vehicles, as identified in the NTA (and as required by the FATF Recommendations).** Australia's AML/CTF regime was strengthened in 2014 by the introduction of new CDD and PEP requirements for reporting entities. In 2011, amendments to the AML/CTF Act introduced new obligations to address the ML/TF risk associated with remitters. As discussed in IO3, AUSTRAC's risk-based supervision policy focuses on the higher risk reporting entities currently within the AML/CTF regime. Robust enforcement of the new CDD requirements, coupled with other predicate crime policies<sup>5</sup> should also enhance efforts to combat the use of fraudulent identities in ML/TF, which discussions with law enforcement and the private sector suggested occurred frequently. Identity fraud was identified as a high-risk issue in the NTA, which indicated identity crime/fraud as both a crime risk and an enabler to ML. However, there are limited measures in place to mitigate high ML/TF risks identified by the authorities associated with the abuse of legal persons and arrangements or the real estate sector. Professional facilitators (lawyers, accountants, TCSPs – especially from lower tier firms) were almost universally understood as a major ML risk - but the authorities have not addressed that risk by including them within the scope of the AML regime. Obligations to record details about beneficial ownership of customers, companies, and trusts by professional facilitators as well as report suspicions to AUSTRAC may enhance detection of ML/TF activity as well as facilitate the timely tracing of criminal assets. This is particularly relevant for the latter where the authorities indicated that tracing proceeds is often frustrated through the use of complex corporate structures (see IO4, IO5, and IO8).

**2.24. The authorities could also do more to pro-actively address the ML risk from foreign proceeds, including by regulating real estate agents, one of the DNFBPs most exposed to the activity, and by law enforcement more actively pursuing foreign predicates crime.** The laundering of foreign proceeds of crime in Australia (particularly in the real estate sector) was acknowledged by some of the authorities and much of the private sector as a high ML risk, but assessors' attention was not drawn to any national policies explicitly targeting or prioritising this risk. Of great concern is that Australia has not brought real estate agents within the AML/CTF regime. Furthermore, while authorities have taken some proceeds of crime action in relation to foreign proceeds, they do not always pursue such cases, nor receive good cooperation from other countries to get admissible supporting evidence to demonstrate foreign offending or that money

5 See the National Identity Security Strategy, at [www.ag.gov.au/identitysecurity](http://www.ag.gov.au/identitysecurity).

in Australia is the proceeds of crime, which therefore limits Australia's ability to take action. The AFP works closely with AGD and foreign law enforcement agencies to help ensure that foreign orders can be registered in Australia. Nevertheless, authorities indicated that the receipt of a foreign restraining order was not usually a trigger to commence an Australian investigation to pursue criminal charges against those carrying out the laundering activity in Australia. Overall, the assessors were left with the impression that law enforcement efforts to pursue the laundering of foreign proceeds might be given a higher priority if there was an explicit national policy to address this risk (See IO4 and IO7).

2.25. **The authorities could do more to address ML/TF in cash-intensive businesses.** Cash is clearly understood as a major risk - but cash intensive businesses do not seem to be a focus for the authorities and, other than being mentioned in the NTA, it is not clear that the authorities have policies that proactively address the risks associated with them.

2.26. **Australian authorities' understanding of its TF risk has also informed the development of its national CTF policies and activities.** The introduction of remittance registration obligations in 2011 has assisted in addressing the TF risks posed by the remittance sector, a key channel for TF in Australia. The authorities' ability to investigate TF and disrupt terrorism plots has been greatly enhanced by the creation of a specific Terrorism Financing Investigations Unit in the AFP in 2010. **More generally, Australia does not have a developed national policy setting out what the overall AML/CTF system is meant to achieve, or how its success should be monitored or measured, making it challenging to determine how well the ML/TF risks are being addressed.** Most AML/CTF agencies have key performance indicators (KPIs) but few relate to AML/CTF, and those are too micro to help determine what the system overall is achieving. Thus, there are very limited mechanisms or metrics actively in place to measure how efficient or effective the AML/CTF system is, including how well it addresses ML/TF risks. Related to this, there are challenges producing some key national level AML/CTF related statistics for the system's criminal justice outcomes (see TC Annex).<sup>6</sup>

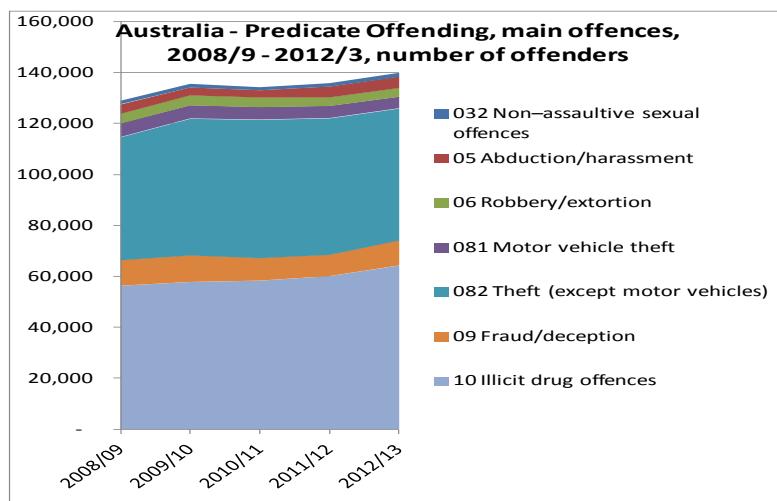
2.27. **Accordingly, metrics about how well the authorities' efforts are addressing ML/TF risks are limited, and the authorities were challenged to present convincing evidence about what outcomes their efforts are achieving.**<sup>7</sup> While law enforcement's strategic focus is on disrupting predicate crime, including through confiscating criminal assets, rather than pursuing ML offences, there was not sufficient evidence that this strategy was reducing the level of offending or taking enough proceeds away from criminals to make crime unprofitable (see IO.7 and IO.8). Official crime statistics and other reports indicate that, while predicate crimes may be decreasing in some areas (e.g. some frauds), the overall incidence, particularly for drug trafficking (the main threat), is not (see chart below). Consistent with this, drug seizures and arrests are substantially higher than since the last assessment and at record highs<sup>8</sup>. Some law enforcement indicated that the value of property taken from criminals each year was small compared to what the criminals generated (see IO.8 for more on what is confiscated annually). Moreover, the authorities only take action to freeze or seize proceeds of crime in a small number of predicate crime cases, suggesting that more could be done to address ML risks.<sup>9</sup>

<sup>6</sup> A contributing factor may be that criminal justice statistics are maintained according to the highest ranked offence that an offender is charged with or convicted for. The ML offence ranks 79th, behind many predicate offences (and below all major profit generating offences identified in the NTA). This limits an ability to accurately track how many offenders are convicted for ML or what sanctions were imposed on them for ML.

<sup>7</sup> See IO.6, IO.7, and IO.8 for more information about outputs of various operational task forces.

<sup>8</sup> Australian Crime Commission (2014).

<sup>9</sup> The ratio is around 2%. Note, however, that it is unrealistic to expect any country to prosecute 100% of its predicate crime offenders for money laundering or recover 100% of proceeds generated.



### *Objectives and activities of competent authorities*

2.28. The objectives and activities of most of the competent authorities are generally consistent with the ML/TF risks, with the major exception being a lack of focus on addressing risks from abuse of complex corporate structures and real estate (including through regulating relevant DNFBPs). And, while there may be alignment, as discussed above, moderate improvement is needed in some areas to address the ML risks. On the preventive front, regulation of financial institutions but not DNFBPs matches the main risks and AUSTRAC's stated areas of supervisory focus are fairly well aligned with the high risk channels identified in the NTA, and guided by sector and entity-type risk analysis. But AUSTRAC's actual supervisory practice does not adequately align with the risks in the regulated sectors and is not sufficiently nuanced to account for variance and risk between the REs within a single Reporting Entity Group (REG). As mentioned, there is no specific national AML/CTF policy or strategy for the authorities to align their objectives and activities with.

### *Exemptions, enhanced, and simplified measures*

2.29. Exemptions from requirements, and the application of enhanced or simplified measures, are not based primarily on the results of the NTA, NRA or other efforts to assess ML/TF risks. The regulatory framework does not require reporting entities to apply enhanced measures based on the findings of the NTA or NRA, and exemptions are often driven by a combination of parameters such as regulatory burden imposed on regulated entities relative to their risks and other matters, rather than primarily on a proven low risk of ML and TF.

### *National coordination and cooperation*

2.30. National coordination across the operational chain is very comprehensive, but demonstrating that it is focused on combating ML and TF rather than predicate crimes and terrorism is challenging. As mentioned, Australia has many arrangements in place for AML/CTF coordination and cooperation, underpinned by OCTA, NOCRP, NTA and NRA (see IO6, IO7, and IO8 for more information about the results being produced by various operational task forces). These result in regular dialogue between relevant agencies, particularly on operational matters. Overall, however, none of the material cited by the authorities flowing from these arrangements set out any policy or strategy for combating laundering *per se* or going after those that facilitate it – the target of most of the material is organised crime rather than money launderers. However, the authorities said much of their effort focuses on following the money trail overseas to identify the key ML syndicate organisers - the 'super controllers' or 'super facilitators' - and to engage foreign authorities to take joint action against these targets. As previously mentioned and elaborated below in Chapters 3 and 4, the authorities' focus is on disrupting predicate crime and terrorism rather than ML/TF. As discussed in Chapter 6, AUSTRAC, as AML/CTF supervisor, seems to coordinate well with law enforcement, but could make more effort to coordinate with prudential supervisors.

2.31. **The authorities coordinate and cooperate to a large extent to combat the financing of proliferation of weapons of mass destruction.**

2

### *Communicating ML/TF risks*

2.32. **Australia has been proactive in directly communicating some aspects of ML risk outcomes, particularly to major reporting groups, but could enhance communication of customer and country risks to all reporting entities, and improve overall communication to the lower-tier reporting entities.** A sanitised version of the NTA on ML was published that contains only cursory material about the predicate crime threat, cross-border or country risks, and very little about customer risks. Very general information about predicate crime threats and sometimes their links with ML are also communicated through the ACC's sanitised OCTA and other publications, but more focus on the size and nature of the predicate crime environment in future sanitised NTAs would help the private sector to better understand the broader ML risk environment. The NRA on TF had not been shared with the private sector at the time of the on-site. A sanitised version shared with the assessors, while identifying high-risk countries and the main areas exposed to risk, seems high level and would be improved if it provided more practical information to the private sector about Australia's TF risks.<sup>10</sup> The authorities have also shared more details on ML/TF risks in AUSTRAC's major reporters and industry forums. Many in the private sector indicated that the extent of their knowledge about the authorities' views of ML/TF risks was limited, and that they would benefit from having more information than what is available in the published material, including more current information on areas of concern.

## **Overall conclusions on Immediate Outcome 1**

2.33. **Australia is achieving Immediate Outcome 1 to a large extent as demonstrated by its good understanding of most of its major ML risks and of its TF risks, as well as its very good coordination of activities to address key aspects of the ML/TF risks.** Australia identified and assessed most of its major ML risks, but needs to pay more attention to understanding foreign predicate risks, and vulnerabilities that impact its AML/CTF system. The system has started to achieve some mitigation of ML risks (e.g. for some fraud and tax crime), but the major drug crime threat is highly resilient to the authorities' efforts. AML/CTF policies need to better address ML risks associated with foreign predicate offending, the abuse of legal persons and arrangements, and laundering in the real estate sector, particularly through bringing all DNFBPs within the AML/CTF regime. More current information about ML/TF risks also needs to be communicated to the private sector. The identification of low or high ML/TF risks by the authorities should drive exemptions from requirements and strongly influence the application of enhanced or simplified measures for reporting entities. While cooperation, particularly on operational matters, is very good across relevant competent authorities, including for proliferation matters, Australia could better articulate an AML/CTF policy and maintain more comprehensive national statistics to demonstrate how efficient and effective its AML/CTF system is, including by developing ways to show that its disruption strategy for predicate crime addresses ML risks. **The rating for Immediate Outcome 1 is substantially effective.**

## **2.4 Recommendations on National AML/CTF Policies and Coordination**

2.34. The authorities are recommended to:

- Develop and implement more aggressive policies to combat ML, particularly drug related, but also other ML beyond the current primary focus on the predicate crime, including aimed at pursuing sophisticated and complex ML schemes in order to disrupt major ML networks and facilitators.

<sup>10</sup> A sanitised version of the NRA was published on September 11, 2014, too late after the onsite visit to be taken into account for the purposes of determining ratings.

- Better address ML risks associated with:
  - predicate crimes other than drugs and tax, including foreign predicates;
  - the abuse of legal persons and arrangements and the real estate sector;
  - identity fraud;
  - fraud; and
  - cash intensive activities, including by extending AML/CTF requirements to lawyers, accountants, trust and company service providers, and real estate agents.
- Articulate and then implement clear and more granular strategies for combating ML and TF, including identifying metrics and processes for monitoring and measuring success.
- Establish processes to collect and maintain the main national level statistics needed to measure success in implementing a national AML/CTF strategy, particularly those related to investigations, prosecutions, convictions, and property confiscated.
- Undertake a re-assessment of Australia's ML risks in keeping with the requirements and guidance issued in relation to Recommendation 1, and formalise the ongoing processes for re-assessing risks.
- Share more information with the private sector about ML/TF risks and consider having private sector input into the assessment of those risks.
- Amend the AML/CTF Act and Rules to ensure that exemptions and the application of simplified preventive measures must be based primarily on low ML and TF risk.

## References

Australian Crime Commission (2014), *Illicit Drug Report 2012-13*, Australian Crime Commission, Canberra, [www.crimecommission.gov.au/sites/default/files/290414-IDDR-2012-13.pdf](http://www.crimecommission.gov.au/sites/default/files/290414-IDDR-2012-13.pdf).



### 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3

#### Key Findings

**Australia develops and disseminates good quality financial intelligence to a range of law enforcement bodies, customs, and tax authorities.** AUSTRAC is a well-functioning FIU. The amount of financial transaction data in the AUSTRAC database, and the fact that all relevant competent authorities have access to this database and can use its integrated analytical tool, are strengths of Australia's AML/CTF system. AUSTRAC information is accessed by federal law enforcement as a routine in most cases but less so by State and Territory police who conduct most predicate crime investigations, and this information assists in the investigation of predicate offences.

**However, the overall limited use of AUSTRAC information by law enforcement as a trigger to commence ML/TF investigations presents a weakness in the Australian AML/CTF system** and should be addressed as a priority. Broader use of the sound institutional structure for combating ML would more effectively mitigate ML/TF risks.

**Australia's main criminal justice policy objective is to disrupt and deter predicate crime, including if necessary through ML investigations/prosecutions.** Australia focuses on what it considers to be the main three proceeds-generating predicate threats (drugs, fraud and tax evasion). Australia should expand its focus to ensure that a greater number of cases of ML are being identified and investigated adequately.

**Stand-alone and third party ML offences are regularly prosecuted.** However, legal issues have arisen in relation to the prosecution of self-laundering offences and ML of foreign predicates is not frequently prosecuted. **The level of convictions for ML at the federal level and in Victoria is encouraging, but the level in the other States and Territories is lower than is warranted by their size and risks.** Effective, proportionate and dissuasive sanctions have been applied to natural persons. However, no corporations have been prosecuted for ML offences and it appears that this option is not seriously considered or pursued – which is inconsistent with the risk profile.

**The Australian authorities apply a range of criminal justice measures to disrupt serious criminal activity, including ML offences, as an alternative to pursuing the ML offence, but such measures are applied whether or not it may be possible to secure a ML conviction.**

**Confiscation of criminal proceeds, instrumentalities, and property of equivalent value is being pursued as a policy objective; mainly in relation to drugs** and in relation to tax by the ATO. Competent authorities have increased their efforts to confiscate proceeds of crime, particularly since the establishment of the federal Criminal Assets Confiscation Taskforce. But it is unclear how successful confiscation measures are across all jurisdictions and total recoveries remain relatively modest.

**The movement of undeclared currency ("cash smuggling") is identified as an increasing high risk in Australia and some steps have been taken to target cross-border movement of cash and bearer negotiable instruments (BNIs).**

**The focus of Australia's confiscation efforts are consistent with the primary risk identified in the NTA to the extent that the majority of assets recovered to date have flowed from the drugs trade and also from tax evasion.** Australia is also at significant risk of an inflow of illicit funds from persons in foreign countries who find Australia a suitable place to hold and invest funds, including in real estate.

### 3.1 Background and Context

#### *Legal System and Offences*

3.1. The *Criminal Code Act 1995* (CC) contains Division 400, which contains the federal ML offences. Australia follows an all-crime approach for predicates, including State, Territory and foreign predicates. States have also criminalised ML. Federal seizure and confiscation provisions, both for ML and TF, are in the *Proceeds of Crimes Act 2002* (POCA). States and Territories have corresponding, but different, sets of laws.

3.2. AUSTRAC is the financial intelligence unit (FIU) for Australia. It is an administrative FIU in the AGD portfolio. The FIU branch in AUSTRAC is responsible for monitoring and analysing financial transactions report data, producing intelligence products and working with domestic agencies and international counterpart FIUs. AUSTRAC has been a member of the EGMONT Group since 1995.

3.3. The AFP is the federal police force. It works in coordination with the State and Territory police forces. AFP is responsible for federal crimes, which cover about half of the predicate offences and ML, as well as TF. The State and Territory police forces are responsible for non-federal predicates, which cover the majority of predicates, and ML. There is overlap in predicate-coverage between the federal and state/territory level, but together, both levels cover all predicates.

### 3.2 Technical Compliance (R.3, R.4, R.29-32)

3.4. See for the full narrative the technical compliance annex:

- **Recommendation 3 (money laundering offence) is rated compliant.**
- **Recommendation 4 (confiscation and provisional measures) is rated compliant.**
- **Recommendation 29 (financial intelligence unit) is rated compliant.**
- **Recommendation 30 (responsibilities of law enforcement and investigative authorities) is rated largely compliant.**
- **Recommendation 31 (powers of law enforcement and investigative authorities) is rated largely compliant.**
- **Recommendation 32 (cash couriers) is rated largely compliant.**

### 3.3 Effectiveness: Immediate Outcome 6 (Financial intelligence)

#### a) *Types of reports received and requested (information to the FIU)*

3.5. AUSTRAC receives a wide range of financial transactions reports. The following table summarises the report types AUSTRAC has received and subsequently analysed in recent years (see Table 3.1).

3.6. The number of reports that AUSTRAC receives is high because of the requirement to report all international fund transfers instructions (IFTIs). AUSTRAC also receives suspicious matter reports (SMRs) and considers that these reports are of a relatively high quality when it comes to the description of the suspicion that caused the reporting. The vastly larger volume and immediate filing of IFTIs and TTRs can make them more useful for intelligence and longer running operations, allowing larger money trails to be followed and wider networks to be identified. However, law enforcement found that SMRs can at times take longer to be submitted to AUSTRAC (up to 10 days).

3.7. AUSTRAC stores all transactions in a highly advanced and sophisticated database for receiving, storing and analysing financial transactions and related information: the Transaction Reports Analysis and Query (TRAQ) database. AUSTRAC can also request additional information from financial institutions (making two such requests in 2013-14). AUSTRAC has direct access to a wide range of information. AUSTRAC also has indirect access to information held by the AFP. This information may be entered manually into TRAQ as an external source of information and thereby serve the purposes of analysis. AUSTRAC may benefit by increasing the sources for its analysis; such databases could be information related to criminal convictions.

3

**Table 3.1. Report types received and analysed by AUSTRCAC**

Reports received by Austrac	2009-10	2010-11	2011-12	2012-13
IFTI (international funds transfer instruction reports)	18 095 756	35 666 743	53 770 266	79 334 421
SMR/SUSTR (suspicious transaction reports)	47 386	44 775	48 155	44 062
TTR/SCTR (threshold and significant cash transaction reports)	3 375 447	8 325 621	5 395 630	5 224 751
CBM/PC (cross-border movement of cash declarations)	35 527	30 342	29 525	30 725
CBM/BNI (cross-border movement of BNIs disclosures)	918	850	659	655
<b>Total</b>	<b>21 555 034</b>	<b>44 068 331</b>	<b>59 244 235</b>	<b>84 634 614</b>
<b>SMR/SUSTR per FIU FTE staff member *</b>	<b>615</b>	<b>533</b>	<b>573</b>	<b>595</b>
<b>Total reports per FIU FTE staff member</b>	<b>279 936</b>	<b>524 623</b>	<b>705 289</b>	<b>1 143 711</b>

\* AUSTRAC staff dedicated to the FIU function.

### *Customs (ACBPS)*

3.8. AUSTRAC also receives and inputs into its database the cross-border currency declarations and cross-border BNI disclosures that ACBPS collects from travellers.

#### *b) Use and dissemination of financial information (Information from the FIU to law enforcement)*

3.9. The Australian approach to the use and dissemination of financial intelligence and information is by 1) allowing direct access to the AUSTRAC database by partner agencies, thus giving them direct access to the raw data that it contains and specific reports from the database; and also by 2) disseminating analysis conducted by AUSTRAC.

##### *i) Direct use of financial information and other relevant information*

3.10. **A large number of Australian authorities access and use a broad range of financial and other relevant information in the FIU database to develop evidence and trace criminal proceeds, especially in relation to predicate offences.** Main sources used to identify predicate offences and potential ML and TF offences are intelligence, financial flows, human sources and use of coercive powers.

3.11. Authorised partner agencies access the AUSTRAC database directly online through the TRAQ Enquiry System (TES) – based on MOUs concluded with each partner agency. The MOUs govern the number of personnel from each agency permitted to use TES and the level of access granted to each user. The 41 agencies include all major federal, State and Territory law enforcement bodies. In 2012/13, these agencies had a total of approximately 3 200 personnel with access to TES. All use of the AUSTRAC information can be audited for security reasons. In each of the previous five years, over 2 million manual searches (more than 7000 each day of the year) have been conducted in the AUSTRAC database. Other access is role-based

(different agency staff with different levels of security or operational responsibility have differing levels of access to the AUSTRAC system). Some agencies, such as the AFP, have full online access to all data held by AUSTRAC. Other agencies, such as ATO, automatically receive copies of all SMRs.

3.12. AUSTRAC also forwards potential high risk reports, such as some SMRs, automatically to certain partner agencies within one hour of receipt, based on dynamic red flags that are set in coordination with each partner agency. Other flagged reports are made available within 24 hours. AUSTRAC refers and sends these SMRs to partner agencies based on the nature of the alleged offence, risk or other material fact.

3.13. **The amount of financial transaction data in the AUSTRAC database, and the fact that all relevant competent authorities have access to this database and can use its integrated analytical tool, are strengths of Australia's AML/CTF system.**

3.14. Access to information is also achieved through a network of AUSTRAC senior liaison officers (ASLOs). The network promotes the use of AUSTRAC financial intelligence by partner agencies. AUSTRAC data is also used as input for the ACC Fusion database that generates law enforcement intelligence.

3.15. Much of the use of financial information in investigations takes place through joint task forces, such as the ATO-led Project Wickenby and the AUSTRAC/ACC-led Eligo National Task Force (see also IO7).

### Box 3.1. Joint task forces

**Project Wickenby** is consistently cited by all authorities as the best example of successful use of AUSTRAC information. Wickenby has existed since 2006. It aims to prevent people from promoting or participating in the abuse of tax or secrecy havens and to improve taxpayers' willingness to comply with their taxation obligations. The success of Wickenby is regularly communicated to the general public, and publicly measured by the amount of AUD that have been discovered and the number of successful prosecutions. Since 2006, 44 persons have been convicted for serious offences as a result of Wickenby, 3 of these were ML convictions. The total amount of money recouped under Project Wickenby since 2006 is over AUD 851 million. This includes over AUD 500 million in cash collections (payments of tax liabilities). This equates to about 5-6 convictions and the recovery of about over AUD 100 million annually. AUSTRAC information is said to be key to the success of Wickenby. In 2012 – 2013 AUSTRAC provided 55 intelligence reports to Wickenby (including international funds transfer pattern reports).

**Eligo National Task Force** is an ACC-led special investigation into the use of alternative remittance and informal value transfer systems by serious and organised crime. Eligo's aim is to put in place long-term prevention strategies, using criminal intelligence insights to disrupt ML, drive greater sector professionalism and make it harder for organised crime to exploit this sector. AUSTRAC is an active participant, as the FIU and as the financial regulator. Eligo is actively cited as an example of the use of financial intelligence to prevent and disrupt criminal activity. Despite efforts, law enforcement officials expressed frustration with the continued operation of apparently criminal, although registered, remittance businesses. Moreover, abuse of remittance businesses was cited as one of the most common methods used to launder, particularly, drug proceeds, Australia's largest ML threat.

### Customs (ACBPS)

3.16. Because all international wire transfers are reported to AUSTRAC, smuggling cash and BNIs is considered an attractive alternative to bring illicit funds in and out of Australia without the certainty of being reported. AUSTRAC and all law enforcement agencies indicated that illicit cash coming from abroad (for example to buy real estate) - is a major typology in Australia despite the fact that, for example, buying real estate with cash would trigger a significant cash transaction report. Cash flowing out of Australia, mainly drugs proceeds that are used for the next transport of drugs, is also a high risk according to authorities.

3.17. Since 2011, ACBPS detected an average of AUD 10.5 million of undeclared cash per year. In 2012-2013, ACBPS detected 308 cases of undeclared currency at the border, amounting to AUD 7.6 million. Of these detections, 230 were incoming and 78 were outgoing. 107 fines were issued and two convictions obtained for offences relating to failing to declare cash. An additional 14 convictions were obtained in 2013-2014.

**Table 3.2. Convictions for failing to report movement of cash over the threshold and BNIs when requested into and out of Australia**

	2011-12	2012-13	2013-14	Total
Failure to report movement of cash over threshold into Australia	0	1	4	5
Failure to report movement of cash over threshold out of Australia	7	1	10	18
Receives cash moved into Australia without report	0	0	0	0
Failure to report BNI when requested	0	0	0	0
<b>Total</b>	<b>7</b>	<b>2</b>	<b>14</b>	<b>23</b>

3.18. AFP does not have figures on how many seizures have followed from these detections. Considering the risk of cash in Australia following the number and amounts of foreign-linked cash cases reported by the authorities, this suggests a low detection rate. Australian authorities also reported that an amount of AUD 1.1 billion is declared annually from an average of 30 000 travellers (that is an average of AUD 31 000 per traveller). Travellers who declare are generally not stopped by ACBPS, as there are no restrictions on the amounts of cash that can be moved across the border and as intelligence information would be needed to alert ACBPS to question a traveller. From the data and the on-site discussions it seems that custom officials would generally not proactively question a traveller who declares such large sums of cash.

#### *ii) FIU analysis and dissemination*

3.19. Because many federal partner agencies have direct access to AUSTRAC's database and/or receive a copy of some reports that are submitted to AUSTRAC, dissemination (forwarding) of information (as received from reporting agencies) is less of an issue than it may be in other countries that have "closed buffer" FIUs. Nevertheless, AUSTRAC also proactively and reactively disseminates intelligence products. AUSTRAC ASLOs also produce intelligence reports for partner agencies, both reactively and proactively.

3.20. Reactive dissemination takes place when partner agencies request AUSTRAC to conduct specific analyses. This could be related to a case or to strategic intelligence needs (for example money flows to tax havens for ATO). Since other agencies have access to the AUSTRAC database, they could do this directly themselves; however, AUSTRAC's analytical experience adds value. AUSTRAC intelligence reports are also produced and disseminated proactively (i.e. on AUSTRAC's own initiative). For 2013-2014, AUSTRAC disseminated 752 reports and made 1314 disseminations to partner agencies<sup>1</sup>.

1 Some reports go to more than one agency.

## LEGAL SYSTEM AND OPERATIONAL ISSUES

3.21. AUSTRAC's intelligence reports tend to be based mainly on the reporting information that is available in the AUSTRAC database, and the intelligence reports that AUSTRAC staff shared with the assessment team were all based solely on reported information. These reports seemed to be of a good quality. Examples of the types of intelligence reports that AUSTRAC produces are network analysis reports, transaction trends and patterns reports, and typologies reports. For this, AUSTRAC has two intelligence teams that produce tactical and operational intelligence reports principally from analysing incoming reports (flagging based on red flags), and two other teams: a specialist financial revenue / tax data mining team and a research and development team applying advanced analysis across the entire database.

3.22. The information flow described applies both to ML and TF. AUSTRAC information is generally used for intelligence, but in limited circumstances has been used as evidence (with the exception of SMRs).

3.23. The 'federal authorities underlined the fact that the use of information from the FIU was a routine in almost all investigations with an economic crime component and that they found the information to be both high quality and useful. The ATO uses AUSTRAC information in direct support of their administrative powers, for example to raise assessments.

**3.24. FIU analysis and dissemination supports the operational needs of competent authorities, particularly at the federal level and in relation to predicate offence investigations. AUSTRAC analysis indicates that around 60% of this use relates to predicate crime and the rest to ML/TF investigations.** According to the statistics, AUSTRAC information (including from the 699 intelligence reports and regular database access) was used in 280 investigations in 2013.

**Table 3.3. Use of Financial Intelligence and outcomes 2012-2013**

Partner Agency	Direct agency access searches	AUSTRAC Intelligence assessments disseminated			SMRs disseminated	Significant Investigation Outcomes	Nature of usage and Outcomes
		Total	Pro-active	Requested			
<b>USE (PARTIALLY) RELEVANT FOR ML/TF</b>							
Federal Law Enforcement and Border Security agencies	1 008 851	814	58%	42%	9 717	212 (all cases)	114 (ML cases) 41% Money Laundering, 33% drug, 5% fraud – remaining matters include people smuggling, weapons offences, counterfeit goods and other predicates
State Law Enforcement	174 431	282	47%	53%	2 830	65 (all cases)	
National Security	29 514	18	90%	10%	325	N/A	Terrorism / terrorism financing matters
<b>TAX AND SOCIAL SECURITY RELATED USE</b>							
Australian Taxation Office	510 115	169	58%	42%	44 044	1 428	Tax administration matters leading to AUD 572 million in additional assessments

**Table 3.3. Use of Financial Intelligence and outcomes 2012-2013 (continued)**

Partner Agency	Direct agency access searches	AUSTRAC Intelligence assessments disseminated			SMRs disseminated	Significant Investigation Outcomes	Nature of usage and Outcomes
		Total	Pro-active	Requested			
Department of Human Services - Centrelink & Child Support	302 328	7	29%	71%	1 283	298	Frauds upon the Commonwealth resulting in annualised savings of AUD 4.4 million
<b>OTHER USE</b>							
Regulatory agencies	27 363	34	76%	24%	605	0	Market manipulation / consumer fraud.
Federal and State Corruption agencies	11 327	12	67%	33%	127	2	Corruption
Other agencies	204	5	67%	33%	0	1	State based evasion of tax
<b>TOTAL (all use of AUSTRAC data)</b>	<b>2 063 686</b>	<b>1 341</b>			<b>58 931</b>	<b>2 006</b>	

Note – Some agencies to which financial intelligence is disseminated are not investigative agencies, for example National Security can conduct inquiries and receive financial intelligence from AUSTRAC to enhance the security intelligence picture. Outcomes for National Security investigations are not published on security grounds.

### Box 3.2. Use of financial intelligence

An example of the use of financial intelligence is **Operation Tricord** where financial intelligence assisted in building a comprehensive picture of a sophisticated, transnational ML scheme. The scheme involved multiple companies in Western Australia and Victoria believed to have been set up to launder funds generated through the exploitation of foreign nationals working on farms. By using financial intelligence produced by AUSTRAC, law enforcement strategies were developed to disrupt the alleged organised crime syndicate that had operated over many years. An AUSTRAC Senior Liaison Officer (ASLO) participated in both the investigative and financial teams, providing on-site support to investigators through ongoing searching and analysis of AUSTRAC holdings, and identifying entity linkages and funds flows offshore. The AFP CACT (see IO.8) utilised the intelligence to progress a mutual assistance request to Vietnam to identify syndicate assets held overseas. Following the 18-month investigation, over 45 search warrants were executed in Perth and Melbourne in early May 2014. At least AUD 15.7 million was moved through the accounts of the two ML syndicates, 22 people were charged with 38 offences, with 12 persons arrested for ML offences under subsection 400.3(1) of the CC, laundering in excess of AUD 1 million, detection of numerous firearms and the identification of at least 162 unlawful non-citizens, resulting in charges for harbouring of unlawful non-citizens under the *Migration Act 1958*. Prosecutions and sentencing is pending. This example demonstrates the entire cycle of the effectiveness of Australia's regime, including: suspect reporting by reporting entities; the value of the collection of IFTI reports to track funds movements out of Australia; the proactive and reactive use of financial intelligence; extensive law enforcement coordination and investigation; major

ML arrests; and the use of mutual legal assistance. The ML activity was complex, involving the use of companies, cash money and international wires.

Another example of the use of financial intelligence for TF investigations is **Operation Neath** (this is also described in IO.9, see below) where a group in Australia sent funds destined for use by the Somalia-based terrorist group al-Shabaab. AUSTRAC financial intelligence included several intelligence reports, online requests and alerts, ASLO engagement and analysis, and the dissemination of related assessment to ASIO and AFP. Three suspects were found guilty of conspiring to plan an Australian-based terrorist attack and sentenced to 18 years in jail.

3

*c) Cooperation and exchange of information*

3.25. **AUSTRAC and other competent authorities cooperate and exchange information to a large extent.** This is evident both in the use of cross-agency task forces and ASLOs. Another positive aspect is the degree to which AUSTRAC is able to exchange information and cooperate with foreign partner FIUs, often through the Egmont Secure Web (ESW).

3.26. **The FIU and its partner agencies use secure channels for exchanging information, and protect the confidentiality of information exchanged or used.** This is in accordance with the MOU between AUSTRAC and the partner agencies. International information exchange with FIUs is done by using the ESW, thus also protecting confidentiality in this regard.

*d) Resources - AUSTRAC and law enforcement*

3.27. AUSTRAC's staff numbers have been reduced, from a peak of 370 in 2009 to 327 for the current budget year, and a projected 319 for 2014-2015. AUSTRAC indicated that the peak of staff related to additional resources needed in relation to the recent roll-out of the AML/CTF Act and Rules and its related awareness raising and training, as well as in anticipation of a second tranche of AML/CTF legislation (which was in the end not implemented). The subsequent reduction of resources has not prohibited AUSTRAC from handling an increasing number of reports and creating more output.<sup>2</sup>

3.28. As far as law enforcement bodies are concerned, the use of the overall budgets is within the authority of the commissioners of police. Long term resources are dedicated to combating ML/TF and financial crime through the ACC's *Targeting Criminal Wealth No. 2 Special Investigation*, task forces (such as the *Eligo National Task Force* and *Project Wickenby*) and the multi-agency Terrorist Financing Investigations Unit. The AFP had three permanent Money Laundering Short Term Teams. First established in January 2012, these teams focused solely on ML investigations. One team was merged into the AFP's general organised crime squad, one team was merged with a joint task force on alternative remittance services (Eligo), and the third team is still in place (7 staff in Melbourne). The New South Wales (NSW) Police and NSW Crime Commission also have specialist ML teams.

## **Overall conclusions on Immediate Outcome 6**

3.29. **Australia's use of financial intelligence and other information for ML/TF and associated predicate offence investigations demonstrates to a large extent characteristics of an effective system.**

2 After the on-site, the federal government made AUD 650 million available to fight terrorism. AUD 20 million was said to be earmarked for AUSTRAC, to enhance its TF analysis and tracking capabilities. Although this took place after the cut-off date for the assessment, this should have a positive effect on AUSTRAC's resources.

AUSTRAC and partner agencies collect and use a wide variety of financial intelligence and other information in close cooperation. This information is generally reliable, accurate, and up-to-date. Partner agencies have the expertise to use this information effectively to conduct analysis and financial investigations, identify and trace assets, and develop operational and strategic analysis. This is demonstrated particularly well in joint investigate task forces, and when tracing and seizing assets.

3.30. **A large part of AUSTRAC analysis use relates to predicate crime and not to ML/TF, thus resulting in a relatively low number of ML cases.** Although AUSTRAC information is said to be checked in most AFP predicate crime investigations, that is not the case for the majority of predicate crime investigations which are conducted at the State/Territory level. Both AUSTRAC and law enforcement authorities could raise their focus on ML cases to achieve a larger number of criminal cases in this area.

3.31. **There are also some concerns with regard to the relative low number of money laundering and terrorist financing investigations outside the framework of the task forces related to the abuse of tax or secrecy havens, use of alternative remittance/informal value transfer systems and asset seizure.**

3.32. Although AUSTRAC information is regularly referred to as a catalyst for ML/TF and related predicate investigations, the ability for law enforcement to maintain details of outcomes that are attributed to financial intelligence could be improved.

3.33. **Overall, Australia has achieved a substantial level of effectiveness for IO.6.**

### 3.4 Effectiveness: Immediate Outcome 7 (ML investigation and prosecution)

3.34. **Australia's main policy objective is to disrupt and deter predicate crime, including if necessary through ML investigations/prosecutions. Australia focuses on what it considers to be the main three proceeds-generating predicate risks (drugs, fraud and tax evasion). However, Australia should expand its focus, to ensure that a greater number of cases of ML are being identified and investigated adequately.**

3.35. The assessors recognised that Australian law enforcement agencies are performing well, domestically and internationally, to combat serious and organised crime, including through their disruption and deterrence approach. At the federal level, all matters under investigation by the AFP with an economic crime component are said to be examined from a ML perspective and assessed as to whether a concurrent financial investigation is warranted. It is unclear, however, what such an examination entails in practice (e.g. AUSTRAC data check, or formal decision), and in what proportion of cases financial investigations do commence, as the authorities do not maintain such statistics. In the last three years, for example, the Commonwealth Director of Public Prosecutions (CDPP) received on average 1 700 briefs for narcotics and fraud per year from the AFP, as well as other Federal, State and Territory law enforcement agencies and an average of approximately 90 briefs for ML cases. The high number of briefs for drugs and fraud is consistent with their status as Australia's largest proceeds-generating predicate offences. However, the lower number of ML briefs suggests that more cases of ML from major proceeds-generating offences could be followed through.

3.36. Australian law enforcement agencies view ML investigations as one component, albeit an important component, in a holistic strategy to disrupt organised crime in Australia. Agencies therefore target incidents of crime and suspected offenders in a manner that is designed not to boost arrest and prosecution statistics, but to best disrupt organised criminal activity. In practice, this means that the authorities aim to disrupt ML activity but will not necessarily pursue a ML investigation/prosecution.

3.37. Primary sources to identify ML activity are intelligence, financial flows, human sources and use of coercive powers. AFP works in conjunction with agencies including ACC, AUSTRAC and ATO, as well as State/Territory agencies to investigate predicate and other serious offences. The ACC has significant intelligence gathering capabilities and some investigative capacity, and the results of these activities are passed to AFP for appropriate action. According to ACC records for the year 2013–14, 46% of ACC operational and intelligence resources were dedicated to combating ML and other financial crimes. The information on financial flows

held by AUSTRAC are an asset for AFP in investigating cases, if not for initially identifying criminal activity, then for allowing investigators to build investigations with recourse to the financial information held by AUSTRAC. They cited the IFTI information as particularly useful. According to AFP, recourse to AUSTRAC information is made in most financial cases. ATO also profiles and shares its information with AFP to enhance investigative capacity.

3

3.38. When ML activity is identified, the authorities look to their suite of available measures. This may result in a ML prosecution and/or one or more other appropriate measures, such as the case being handed to ATO to pursue tax remedies; to AFP to pursue criminal action on a predicate offence; or to CACT to pursue confiscation action under POCA. Authorities may also let the activity run to see what further intelligence can be obtained, including by developing human sources .

3.39. Task forces have been established to tackle key enablers of criminal activity, and have begun to have some success in detecting and disrupting key ML risks. Since 2012, the Eligio National Task Force that investigates the use of alternative remittance services by serious and organised crime had led to:

- i. seizure of more than AUD 29 million cash;
- ii. seizure of illicit drugs with a combined estimated street value of more than AUD 614 million;
- iii. restraint of more than AUD 30 million worth of assets;
- iv. disruption of 23 serious and organised criminal groups/networks and the identification of more than 166 targets, operating in more than 20 countries, previously unknown to law enforcement;
- v. arrests of 123 people on 232 charges; and
- vi. 26 convictions, including 7 for ML and 19 for predicate offences.

3.40. Since 2006, Project Wickenby, which investigates arrangements of an international character to avoid or evade taxation and similar offences, has led to 44 convictions, including 3 ML convictions. See IO.6 for more on these task forces.

3.41. At the State/Territory level, police focus is on the investigation of predicate offences, particularly drug offences and outlaw motor cycle gang activity. This is consistent with the risk identified in the NTA. However, most State cases follow through to a ML prosecution only in simple cases where offenders may be caught in possession of cash. Victoria obtains a reasonable level of substantive ML prosecutions and convictions and NSW (which together with Victoria accounts for half the population) generates a relatively large number of cash-possession ML cases. Information available through AUSTRAC and other financial information are used to support investigations into the predicate offence and for asset recovery action. In States and Territories where the number of ML investigations is low, this is mainly due to the complexities involved and the resource-intense nature of the investigations. However, Queensland and other States and Territories should focus much more on ML to achieve the generally satisfactory results that Victoria and to some extent NSW are achieving.

3.42. **The NTA of 2011 identified drugs (particularly methamphetamine or 'ice'), fraud and tax evasion as high-risk areas from a threat perspective. Consistent with this risk assessment, the authorities focus on these predicates, and to a lesser extent on related ML. However, the ML focus on these risks could be reinforced, and the overall ML focus could be broadened to cover other predicate offences such as all forms of corruption (including foreign corruption).** ACC identifies ice and ML as being key risks in the serious and organised crime environment and is currently dedicating most of its resources to these areas, including through Eligio National Task Force and its focus on the remittance sector. Despite the generally good results, several law enforcement entities indicated that actions to date had limited impact on the drugs market and major networks laundering drug proceeds. They also suggested that investigating major drug-related laundering was often frustrated through organised groups using complex corporate structures. Project Wickenby has focused on the tax avoidance/evasion risk. Task Force Galilee focuses on investment fraud, including boiler room activity located off-shore to defraud unsuspecting investors, which

is seen as a serious problem. Whilst this type of criminal activity is being disrupted, the prospect of detection, conviction, and punishment is not dissuading criminals from carrying out these proceeds-generating crimes and ML. Project Wickenby interventions are nevertheless improving taxpayers' willingness to comply with their taxation obligations. See also the boxes with information on task forces in IO.6.

**3.43. Legal issues have arisen in relation to the prosecution of self-laundering offences and ML of foreign predicates is not frequently prosecuted.** In *Nahlous v R* [2010] NSWCCA 58 and *Thorn v R* [2009] NSWCCA 294, the courts have criticised the practice of charging both predicate and ML offences as "double charging" when the criminality of the ML offence is completely encompassed in the predicate offence. Subsequently, the CDPP issued a litigation direction to prosecutors stating that the charging of the predicate offence and a ML offence will not be an abuse of process where it is necessary to charge both offences to reflect the overall criminality in the case. As indicated by the authorities, this issue presents a challenge for prosecutors in Australia in ML cases involving self-laundering.

**3.44.** Foreign predicate offences, including corruption offences, are not frequently prosecuted from the ML perspective – because Australia does not consider that foreign predicate offences are major predicates for ML in Australia. Authorities have referred to the difficulties of obtaining off-shore evidence and have generally found the most successful way to obtain restraint or forfeiture orders is to seek registration of foreign orders. However, federal and State action is not effectively coordinated. For example, while ML of foreign illicit proceeds through real estate is perceived to be a risk for Queensland (Gold Coast), Queensland has no ML convictions for this activity. AFP indicated that it does not focus on this risk, believing this ML activity relates to State level predicates, whereas the Queensland Crime and Corruption Commission stated it does not focus on this risk as it relates to foreign money and is thus a matter for AFP. At the same time, assessors took note of two examples of successful prosecution for foreign predicates (fraud and corruption) by AFP and the registration of two restraint orders from Papua New Guinea in Queensland.

**3.45.** CDPP charges stand-alone and third party ML offences and the majority of CDPP's ML prosecutions now involve these offences. However, it is more challenging to get convictions when ML is prosecuted with the predicate offence, according to CDPP. CDPP data indicates that about 95% of defendants are convicted for the ML offence when they are prosecuted for a stand-alone ML offence, whereas the figure is about 70% when defendants are prosecuted for ML jointly with the predicate offence. The authorities indicated that in many cases the ML offence may be withdrawn by the prosecutor as part of a plea bargain.

**3.46.** The number of prosecutions and convictions of ML offences is difficult to compile due to differences in criminalisation between the federal and State/Territory level, and between States and Territories, and the differences in keeping statistics. Overall, the assessment team considers that Australia has improved in terms of obtaining ML convictions since the last assessment and is achieving reasonable results in the risk and those geographic areas where Australia is focusing on ML. However, the overall results are lower than they could be. The increasing number of ML convictions being obtained is also encouraging (see below).

**3.47.** At the federal level, Australia criminalises ML under Division 400.3 to 400.8 of the CC consistent with the FATF Standards under offence categories based on the value of the property dealt with and the requisite mental elements of knowledge or recklessness. There are also offence provisions based on negligence within these categories, and an offence under 400.9 of dealing with property which is reasonably suspected to be proceeds of crime, which requires a less onerous mental standard than under the Vienna and Palermo Conventions. It is positive that Australia has criminalised certain behaviours beyond what is required in those conventions, but the availability of these lower mental element offences should not distract from pursuing serious level ML.

**3.48.** Consolidated statistics at the federal level for prosecution of ML offences under the offence provisions of Division 400 of the CC are set out in the table below.

**Table 3.4. Federal prosecution of ML under Division 400 of the CC**

Offence	2010-11	2011-12	2012-13	2013-14	Average	%
400.3	19	11	4	7	10	11%
400.4	18	20	13	15	17	17%
400.5	7	3	4	6	5	5%
400.6	19	8	25	26	20	20%
400.7	15	2	8	5	8	8%
400.8	2	4	2	1	2	2%
400.9	16	39	30	52	34	36%
<b>Total</b>	<b>96</b>	<b>87</b>	<b>86</b>	<b>112</b>	<b>95</b>	

3.49. At the State/Territory level prosecutions for foreign predicate ML offences, third party laundering and stand-alone laundering charges are less common than at the federal level. ML charges may also be withdrawn at the prosecution stage in order to obtain a plea and conviction for the predicate offence. The absence of deeming provisions in State/Territory legislation equivalent to the Commonwealth legislation can also make it more difficult for State/Territory authorities to prosecute cases under these provisions. Apart from NSW and especially Victoria, the number of prosecutions for the ML offence equivalent to the Vienna and Palermo standard is very low, and in the case of NSW many of the ML prosecutions are withdrawn to be considered as part of the predicate offence prosecution (however, this will not influence the conviction or total sentence). In Queensland, the Queensland Attorney General's (a Minister) consent is required for a prosecution to proceed and this may also act as an impediment for law enforcement AML action. As with the federal ML offences, the State/Territory offences contain differing mental elements of knowledge, recklessness, negligence, and suspicion.

3.50. An analysis of data on all convictions treated as ML offences or similar at both the federal and State/Territory level is set out in the table below.

**Table 3.5. Convictions equivalent to Vienna/Palermo conventions ("knowledge", "recklessness")\***

	2010-11	2011-12	2012-13	Average
Federal (CDPP)	40	28	38	35
Australian Capital Territory (ACT)	0	1	1	1
New South Wales (NSW)	27	25	23	25
South Australia (SA)	5	5	5	5
Tasmania (TAS)	1	2	0	1
Victoria (VIC)	63	77	100	80
Western Australia (WA)	0	2	0	1
Queensland (QLD)	0	0	0	0
<b>Total – All potential Vienna/Palermo convictions</b>	<b>136</b>	<b>140</b>	<b>167</b>	<b>148</b>
Other convictions (possession of suspected proceeds or negligent dealing in proceeds or receiving of stolen goods offences)				
Federal (CDPP)	14	31	29	25

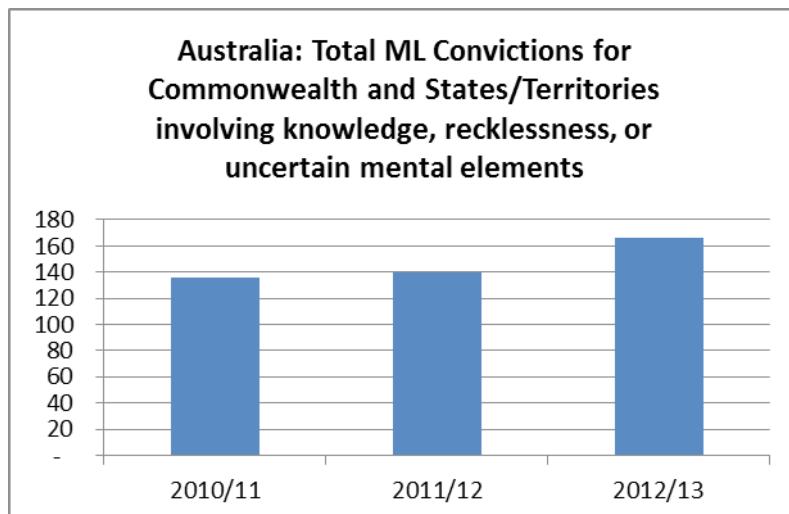
\* The data may slightly overstate the level of convictions equivalent to the Vienna and Palermo standard because they include a few cases where the mental element of the offence is unknown.

**Table 3.5. Convictions equivalent to Vienna/Palermo conventions (“knowledge”, recklessness”)\*  
(continued)**

	2010-11	2011-12	2012-13	Average
Australian Capital Territory (ACT)	0	1	5	2
New South Wales (NSW)	108	112	106	109
South Australia (SA) (no suspicion offence)	0	0	0	0
Queensland (QLD) (receiving offences only)	1 415	1 294	1 444	1 384
Tasmania (TAS)	1	1	0	1
Victoria (VIC)	1 680	1 934	2 242	1 985
Western Australia (WA) (no suspicion offence)	0	0	0	0
<b>Total – Other Convictions</b>	<b>3 218</b>	<b>3 373</b>	<b>3 926</b>	<b>3 506</b>
<b>Grand Total</b>	<b>3 360</b>	<b>3 514</b>	<b>4 099</b>	<b>3 658</b>

\* The data may slightly overstate the level of convictions equivalent to the Vienna and Palermo standard because they include a few cases where the mental element of the offence is unknown.

3.51. As shown above, the bulk of convictions that the authorities consider as ML are for the possession type. The following chart shows the increase over the last three years in total number of convictions for ML offences potentially equivalent to the Vienna and Palermo standards.



3.52. **The authorities have applied a range of sanctions for ML offences to natural persons. However corporations have not been prosecuted for ML offences and it appears that this option is not seriously considered or pursued.** A unique issue arises in relation to prosecution of corporations that are reporting entities due to section 51 of the AML/CTF Act, which has the effect of making it difficult to prosecute them for the ML offence so long as they report the transaction (although they may continue to carry out the transaction – there is no consent mechanism). As far as natural persons are concerned, because at the federal level, 35% of ML cases are prosecuted under 400.9 of the CC or under the negligence provision of the other offences, the sanctions imposed may be at the less severe end of the range, including suspended jail sentences and fines. Overall, data provided indicates that persons are jailed in 58% of the cases involving a ML conviction, with one person receiving a sentence of 14 years (which seems dissuasive). The graded nature of the Division 400 offences with differing mental elements also enables for proportionate sanctions to be applied. Overall, however, many sentences may have been combined with sentences for predicate offences in a number of cases, making it difficult to determine what sanctions are imposed in practical terms for the ML offence.

3.53. Consolidated statistics for sanctions imposed under Division 400 of the CC are set out in the table below.

**Table 3.6. Sanctions imposed under Division 400 of the CC**

	2010-11	2011-12	2012-13	2013-14	Total	%
Jail	40	36	31	42	149	58%
Jail (suspended sentence)	9	16	18	15	58	23%
Fine	1	6	4	6	17	7%
Community service	2	0	8	5	15	6%
Recognisance order	2	0	4	7	13	<b>5%</b>
Other	0	0	1	2	3	<b>1%</b>

3.54. At the State/Territory level, penalties are relatively light, often resulting in fines for possession or handling type charges. Alternatively, the offences may be combined with the overall sanction for the predicate offence.

3.55. **The Australian authorities apply a range of criminal justice measures to disrupt serious criminal activity, including ML offences.** Such measures are applied whether or not it may be possible to secure a ML conviction. As the stated strategy of the authorities is to consider at an early stage how best to disrupt the criminal activity identified, using any measure available from their 'tool kit' or suite of measures, a ML investigation and prosecution will not necessarily be the chosen remedy, even when possible. The focus may instead be action on the predicate offence, asset recovery proceedings and/or other disruptive action. The assessors recognised that Australia's focus on disruption to combat serious and organised crime was having some effect on these issues. However, they were unable to give it much weight in relation to IO7 as the disruption measures are applied whether or not it may be possible to secure a ML prosecution, and a demonstrable effect on reducing ML activities was also not clear.

### Overall conclusions on Immediate Outcome 7

3.56. Overall, Australia demonstrates some characteristics of an effective system for investigating, prosecuting, and sanctioning ML offences and activities. The focus remains on predicate offences, recovery of proceeds of crime, and disruption of criminal activity rather than on the pursuit of convictions for ML offences or the disruption of ML networks, both at the federal and State/Territory levels. However, in the areas of identified risk, Australia is achieving reasonable results and the increase in the number of ML convictions over recent years is heartening. This demonstrates an increased focus on ML compared to the previous FATF/APG assessment. It should be relatively easy to achieve a substantial or even high level of effectiveness by:

- expanding the existing ML approach to other (foreign) predicate offences including corruption,
- focussing more on ML within task forces,
- being able to demonstrate the extent to which potential ML cases are identified and investigated,
- addressing investigative challenges associated with dealing with complex ML cases, including those using corporate structures,
- pursuing ML charges against legal entities, and
- by ensuring that all States and Territories focus on substantive type ML.

3.57. **Australia has achieved a moderate level of effectiveness for IO.7.**

### 3.5 Effectiveness: Immediate Outcome 8 (Confiscation)

3.58. **Confiscation of criminal proceeds, instrumentalities, and property of equivalent value is being pursued as a policy objective in Australia.** Following a general policy review on criminal asset recovery work, the Criminal Assets Confiscation Taskforce (CACT) was established in 2011 and became operational under POCA in January 2012. It has assumed primary responsibility from the CDPP at the federal level for restraint and confiscation of proceeds of crime, except in cases where a conviction is required and no prior restraint order has been obtained. The primary policy objective of CACT is to draw on agency skills to target the criminal economy and take the profit out of crime.

3.59. CACT has been operational under POCA for only two years and aims to take a more proactive approach to litigating proceeds of crime matters and testing the POCA. While it is too early to say whether its efforts are having a marked impact on recovery of proceeds of crime, restraint figures have surged, which is a positive sign. CACT is led by the AFP with around 100 personnel, consisting of forensic accountants, financial investigators, investigators, secondees, and support staff, and supported by over 30 in-house litigation lawyers and litigation assistants in conjunction with the ACC and ATO and the intelligence resources they have at their disposal. As it is not necessary to prove a predicate offence for the purposes of sustaining proceeds of crime action based on ML offences, AFP statistics do not show whether ML cases are based on suspected drug crime or other types of offending. However, based on discussions, most of the focus of the work seems to have been on dealing in proceeds related to drug cases and some fraud activity. Focus on recovery of proceeds of crime arising from, and in connection with, other predicate offences has not been clearly demonstrated, although some recovery action in relation to other predicate offences has taken place. ATO, through Project Wickenby, has targeted recovery of monies from tax crimes. As these recoveries relate to tax administration, they are made in most cases through ATO's taxation powers rather than under POCA.

3.60. All States and Territories have conviction and non-conviction based confiscation schemes. The NSW Crime Commission and the Queensland Crime and Corruption Commission in particular, pursue non-conviction based recovery of criminal proceeds as a policy objective. The authorities in Victoria have also been successful in pursuing significant recoveries as a policy objective, but in other States the policy steer and priority is inconsistent.

3.61. **The competent authorities have increased their efforts to confiscate proceeds of crime since the last FATF assessment, with the amounts being restrained and confiscated increasing at the federal level. Overall, however, the figures remain relatively low in the context of the nature and scale of Australia's ML/TF risks and have only modestly increased since the last assessment.** The total value of amounts recovered at the federal level since 2006-2007 has increased from AUD 12.65 million in 2006-2007 to AUD 65.74 million in 2013-2014. The CACT figures are also showing an upward trend in restraint actions, even though few cases have yet progressed to final confiscation or forfeiture orders.

3.62. CACT takes non-conviction based asset recovery proceedings in most cases allowing for a lower civil standard of proof; however cases can become difficult to pursue when complicated company or overseas structures are used. In addition, under POCA the CACT must provide an undertaking to pay damages to the property holder in all actions it commences to restrain and forfeit property. As such, the CACT is required to consider the potential risk and liability prior to commencing proceedings. This requirement can act as a disincentive to take immediate action in complex matters, especially when successful outcomes may be reliant on overseas evidence not to hand or not forthcoming.

3.63. In line with the authorities' overall objective of disruption, a decision may be made by CACT at the outset to refer the case to ATO to consider whether there has been an avoidance of tax and to use its civil tax recovery powers. The authorities advise that currently around 25 - 30% of cases are referred to the ATO by CACT. ATO has made significant recoveries under Project Wickenby on unpaid tax liabilities, including those related to tax crimes, using its tax recovery powers. While this has been an effective means of recovery, the ATO recoveries are not made under proceeds of crime legislation (POCA). AUD 2.7 million has been recovered under POCA powers in connection with Project Wickenby.

3.64. Unexplained wealth orders are available to target the kingpins of serious and organised crime when they cannot necessarily be linked to criminal offences on available evidence, but to date CACT has not used the

powers due to difficulties with the current legislation and no such orders have been obtained. The procedures allow for a reversal of the onus of proof and require defendants to explain how their wealth was accumulated once it is established the defendant has links to general criminal activity. Amendments to the unexplained wealth regime to improve the investigation and litigation of unexplained wealth matters are currently before the federal Parliament.

3

3.65. CACT has faced challenges in pursuing domestic restraint and confiscation action based on ML involving complex corporate structures and foreign predicate offences where assets are located in Australia. For the latter, the authorities indicated that the challenge is due to the need to obtain foreign evidence and the requirement to give the undertaking as to damages to the property holder if proceedings are commenced. CACT has now begun to work with foreign jurisdictions to register orders obtained abroad under mutual legal assistance procedures against assets identified locally and it has been successful in a few cases to date. CACT aims to continue to process other cases, including cases involving foreign jurisdictional differences, which will require testing before the Australian courts.

3.66. CACT has taken some action to recover proceeds which have been moved outside Australia through requests made under the mutual legal assistance channels. Difficulties have been encountered when funds are located outside Australia, including in investment and boiler room frauds investigated by ASIC. In addition, the authorities do not generally take action under POCA to recover proceeds of crime in fraud cases when there are identified victims, because under POCA, funds recovered are paid into the Confiscated Assets Account and shared with the Australian community to fund anti-crime initiatives. As a result, the authorities do not, as a matter of policy, actively pursue POCA action with a view to restitution of victims, although victims are able to apply to the court during proceeds of crime proceedings to have their interest in property recognised, e.g. through applying for an exclusion or compensation order. Australia does share funds under its sharing program to countries that have provided assistance to Australia in response to mutual legal assistance requests or domestic investigations, and in cases involving restitution of victims abroad.

3.67. As a result of the transfer of the bulk of asset recovery responsibilities, including litigation, to the CACT, the CDPP no longer has specialist litigation resources and personnel for asset recovery work. This is in line with the drop in POCA work now undertaken by the CDPP. As would be expected, CDPP restraint and confiscation figures have declined. CDPP continues with its designated role in cases where a conviction is necessary and no prior restraint order has been obtained.

3.68. At the State and Territory level, comparison of figures for recovery of proceeds of crime is difficult because different jurisdictions take different approaches to data collection. Between 2010-2011 and 2012-2013, Victoria authorities confiscated AUD 54 million in criminal assets (some of which was returned to victims under compensation orders). In the same period, the NSW authorities confiscated assets with a realisable estimated value of around AUD 60.8 million. In NSW and Queensland, the State Crime Commissions pursue non-conviction based confiscation, whilst in other States the DPP takes either criminal or non-conviction based confiscation action. Non-conviction based proceedings are generally not pursued in fraud cases when there is an identified victim, as there is no mechanism to provide restitution to victims and funds are paid into consolidated revenue. The combined recoveries at State/Territory level are about twice the value of recoveries made at the federal level under POCA due to the heavy emphasis on drug related recoveries. Settlement of these cases tends to be more straightforward and less complex than cases undertaken at the federal level by CACT.

3.69. Overall statistics for actual recovery of proceeds, tax liabilities, and instrumentalities of crime are set out in the tables below. A large number of recoveries have been made through ATO but these are recoveries linked to tax evasion under ATO taxation powers, not via POCA recovery powers.

**Table 3.7. Confiscation of proceeds of crime (in AUD millions)**

	2009-10	2010-11	2011-12	2012-13	Average
Confiscated Proceeds					
CACT/CDPP	25.8	13.9	43.1	20.0	25.7
States <sup>1</sup>	56.5	56.7	48.3	61.4	55.7
Cross-border cash confiscations <sup>2</sup>	n/a	n/a	n/a	n/a	n/a
Victim restitution <sup>3</sup>	n/a	n/a	n/a	n/a	n/a
<b>Total Confiscated Proceeds</b>	<b>82.3</b>	<b>70.6</b>	<b>91.4</b>	<b>81.4</b>	<b>81.4</b>

**Notes**

1. Some States report value of orders obtained rather than assets confiscated
2. Australia was unable to provide information on the value of cross-border related confiscations
3. Australia was unable to provide information on the value of compensation orders issued to victims

3.70. Separate from the confiscation of proceeds of crime collections, ATO made the following tax collections (in AUD million) in respect to serious non-compliance audits. These figures include results from Project Wickenby and non-Wickenby activities which relate to the tax implications of organised crime work.

**Table 3.8. Total tax collections: ATO's Serious Non Compliance Audits**

Year	Tax liabilities collected (in AUD millions)
2012-13	91.24
2011-12	119.83
2010-11	109.50
2009-10	81.90

3.71. The Australian authorities regularly make large seizures of drugs due to the size of the domestic drug market and the prevalence of drug offending. The table below sets out the quantum of drugs seized annually:

**Table 3.9. Quantum of drugs seized\***

Year	Amount (in kilograms)
2012-2013	19 628
2011-2012	23 802
2010-2011	9 358
2009-2010	7 851

\* The estimated whole sale value of the seized drugs would have been AUD 438 million (2009-2010); 782 million (2010-2011); 1.01 billion (2011-2012); and 2.67 billion (2012-2013).

3.72. The following table provides information on the values of money recovered as provided to the AFP by the Australian Financial Securities Agency, which operates the Confiscated Assets Account in its capacity as the Official Trustee for the purposes of the POCA. Amounts recovered relate to orders made by the AFP and CDPP<sup>3</sup>.

3 The payments into the Confiscated Assets Account are less costs and fees incurred by the Official Trustee in realising the property.

**Table 3.10. POCA: Amounts recovered into the Confiscated Assets Account from Forfeiture Orders and PPOs\***  
**for the period 2006-07 to 2013-14**

Financial Year	Total amount (in AUD)
2013-14	65 759 185.26
2012-13	20 033 263.34
2011-12	43 095 166.75
2010-11	13 948 991.37
2009-10	25 843 496.07
2008-09	16 669 702.61
2007-08	19 014 501.93
2006-07	12 657 119.95

\* Sections 47, 48, 49, 92, 116 & 134 of the POCA

3.73. No comprehensive information was available to assess the whole system involved in restraint and confiscation of assets, except in relation to the CDPP and CACT. These statistics on applications for restraint and forfeiture orders, together with a comparison against property actually confiscated (i.e. recovered), are set out in the table below.

**Table 3.11. Restraint and confiscation of assets in relation to the CDPP and CACT**

	2009-10	2010-11	2011-12	2012-13	Average
Number of freezes, seizures, & other restraints	44	48	191	228	128
Value of assets frozen, seized, or restrained (AUD millions)	21.1	42.9	116.7	62.5	60.8
Average value (AUD)	480 680	894 717	611 060	274 123	476 142
Number of forfeiture, pecuniary penalty, etc., orders	142	126	144	86	125
Value of forfeiture, pecuniary penalty, etc., orders (AUD millions)	25.4	24.2	75.6	25.3	37.6
Average value (AUD)	179 186	191 912	524 706	293 659	302 084
Value of confiscations (AUD millions)	25.8	13.9	43.1	20.0	25.7
Relative to restraint	122%	32%	37%	32%	42%
Relative to orders	102%	58%	57%	79%	68%

3.74. Funds paid from the Confiscated Assets Account for sharing with foreign governments and entities under sharing arrangements are set out in the table below. The significantly higher figure for 2013-14 relates to a case involving the repatriation of funds to a trustee in bankruptcy overseas for compensation of victims.

**Table 3.12. Funds paid from the Confiscated Assets Account for sharing with foreign governments and entities under sharing arrangements**

Year	Sharing with foreign governments and entities (in AUD)
2013-14	44 600 000
2012-13	0.00
2011-12	0.00
2010-11	0.00
2009-10	4 653 907
2008-9	280 446
2007-8	3 860 000
2006-7	4 015 348

3.75. **Australia is taking some steps to target the cross-border movement of cash and BNIs. However the authorities were unable to provide information about how much of the detected cash is seized or confiscated, and insufficient action is taken to investigate significant declarations.** All persons entering or leaving the country are required to declare whether they are carrying more than AUD 10 000 in currency. In 2012-13, ACBPS detected 308 cases of undeclared cash amounting to about AUD 7.6 million and subsequent seizures are continuing to grow in overall size and value. In 2013-14, there were 430 detections totalling AUD 16 710 909. Around two thirds of these cases involve incoming movements. Fines are issued in cases of undeclared movements over the limit and in serious cases the matters are referred to AFP for further investigation and prosecution. In 2013-14, 167 fines were imposed and 14 individuals were convicted of offences relating to failing to declare cash. Cases of airlines employees transporting significant sums of money have been prosecuted and imprisoned for ML offences and the proceeds seized and confiscated.

3.76. All declarations made at border points and collected by ACBPS are filed with AUSTRAC. If significant sums are declared and an ACBPS officer develops a reasonable suspicion, such as where there is targeted intelligence indicating laundering, they would actively question the traveller. However, it is not clear whether travellers declaring significant sums are questioned in all circumstances. Nor are declarations of significant sums actively reviewed, investigated, or profiled by AUSTRAC when automatically passed on from ACBPS.

3.77. Statistics on border cash detections by ACBPS are set out in the table 3.13 below and demonstrate a recent improvement in the number of detections of undeclared cash.

3.78. **Australia's confiscation efforts are consistent with primary risk identified in the NTA to the extent the majority of assets recovered to date have flowed from the drugs trade and also from tax evasion. Australia is also at significant risk of an inflow of illicit funds from persons in foreign countries who find Australia a suitable place to hold and invest funds, including in real estate.** Cash non-declarations/seizures at border points also indicate illicit funds are entering Australia. The authorities do not appear to be investing serious effort in mitigating this risk, including when foreign predicate offences may be involved.

**Table 3.13. border cash detections by ACBPS**

Border Cash Detections	2011-12	2012-13	2013-14	Average
Number of cash detections				
- incoming	225	230	300	251
- outgoing	54	78	130	87
Total Cash Detections	279	308	430	339
Number of fines imposed	82	107	167	119
Fines as percentage of detections	29%	35%	39%	35%
Total value	AUD 5 478 165	AUD 7 656 212	AUD 16 710 909	AUD 9 948 428
Average Value	AUD 19 635	AUD 24 858	AUD 38 862	AUD 28 397

## Overall conclusions on Immediate Outcome 8

3.79. Overall, Australia demonstrates some characteristics of an effective system for confiscating the proceeds and instrumentalities of crime. The framework for police powers and provisional and confiscation measures is comprehensive and is being put to good use by the CACT, which is showing early signs of promise as the lead agency to pursue confiscation of criminal proceeds as a policy objective in Australia. At the State/Territory level, the focus has remained primarily on recovery of proceeds of drugs offences. The quantum of proceeds confiscated is relatively low in the context of Australia's ML/TF risk and has only increased modestly since the last FATF assessment, which suggests that criminals retain much of their profits.

3.80. **Australia has achieved a moderate level of effectiveness for IO.8.**

## 3.6 Recommendations on legal system and operational issues

3.81. The following recommendations are made in relation to the legal system and operational issues:

### *Financial intelligence (IO.6)*

- The authorities should develop a comprehensive long-term plan for law enforcement to improve the use of AUSTRAC information to increase the number of ML/TF and financial investigations, and to increase the commitment to fight these crimes. In the short term, this should include setting performance indicators.
- The authorities should earmark funds to establish financial crime/ML/TF operational teams within AFP and state police forces, and be committed to keep these funds / operational teams in place for a longer time.
- AUSTRAC should better tailor its information to the needs of its users (outside the context of joint task forces).
- AUSTRAC should (be enabled to) increase the number of sources of information available in its database, for example (but not limited to) criminal conviction records.

### *ML investigations and prosecutions (IO.7)*

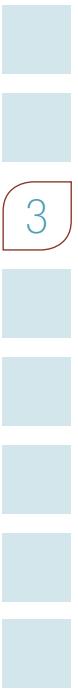
- More emphasis should be placed on the detection, prosecution and punishment of ML offences (not

only the disruption of predicate criminal activity) to dissuade potential criminals from carrying out proceeds generating crimes and ML, both at the federal and even more so at the State/Territory level.

- Authorities should pro-actively monitor the extent to which potential ML cases are identified and investigated and should address investigative challenges associated with dealing with complex ML cases, including those using corporate structures.
- ML cases involving other predicate offences where there is risk, should be proactively pursued, alongside the existing emphasis on drugs and fraud cases, and all States and Territories should focus on substantive type ML offences.
- Self-laundering offences should continue to be charged where appropriate, and more investigations and prosecutions for foreign predicate ML offences, including proceeds of foreign corruption, should be pursued.
- Consideration should be given to imposing ML sanctions on corporations in suitable cases.
- Authorities should consider harmonising State and Territory level ML offence provisions with the federal provisions to improve effectiveness of the State and Territory offences e.g. by inclusion of deeming provisions similar to those in the federal legislation.

### *Confiscation (I0.8)*

- More emphasis should be placed on the confiscation of proceeds of crime reflecting the identified risks from all major revenue generating offences (including fraud and corruption) to increase the volume of confiscation cases to make crime unprofitable, at both the federal and State/Territory level.
- CACT is encouraged to continue its positive action to date to pursue restraint and forfeiture orders, including in difficult cases.
- The authorities should enhance their capabilities to pursue restraint and confiscation action based on ML involving complex corporate structures, foreign predicate offences, and investment frauds where assets are located in and outside Australia.
- State and Territory law enforcement should expand their primary focus beyond recoveries relating to drug offending.
- The authorities should give consideration to allowing restitution of victims of crime under POCA.
- The authorities should take proactive steps to investigate declarations of cross-border movements of significant amounts of cash, which may be an indicator of proceeds of foreign predicate offences being laundered in Australia.



## 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4

### Key Findings

**Australia has undertaken several TF investigations and prosecutions and secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable.** Australia has successfully disrupted two domestic terrorist plots at the time of the on-site visit.<sup>1</sup> Australia also uses these other measures to address the most relevant emerging TF risk – individuals travelling to conflict zones to participate in, or advocate, terrorist activity. Australian authorities identify and investigate different types of TF in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks. On the other hand, **Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions for TF has not been clearly demonstrated.**

**Australia demonstrates a number of characteristics of an effective system for targeted financial sanctions (TFS) both for TF and PF.** A key area of demonstrative effectiveness is in the direct implementation of TFS against persons and entities designated by the UNSC and under Australia's autonomous sanctions regimes. Australia has also domestically listed individuals and entities pursuant to UNSCR 1373 and received, considered, and given effect to third party requests. Australia's legal system and processes for implementing targeted financial sanction provisions related to UNSCRs represent a best practice for other countries, especially the direct legal obligation regarding UN designations.

**However, the effectiveness of the overall framework for targeted financial sanctions both for TF and PF is heavily impacted by the lack of financial supervision of the financial and DNFBP sectors, to ensure compliance with the domestic framework.** Due to the lack of financial supervision or monitoring, the lack of practical examples of implementation issues from the financial sector, and the lack of frozen assets, assessors were unable to establish that the framework is effectively implemented by the financial sector and DNFBPs. A related shortcoming is that AUSTRAC and ASIC do not check their own databases for designated entities.

**NPOs are an area for improved efforts and additional action.** According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a comprehensive sectorial risk assessment (as required by R8), the lack of subsequent outreach in relation to TF to the sector, and the lack of adequate preventive requirements or a supervisory framework that cover all relevant NPOs, leave them vulnerable to misuse by terrorist organisations.

1 Another plot was disrupted soon after the on-site visit.

## 4.1 Background and Context

### *Terrorist financing (criminal justice measures)*

4.1. Terrorist and terrorist financing offences are contained in sections 103.1 (financing of terrorist acts), 102.6 (financing of a terrorist organisation) and 103.2 (financing of an individual terrorist) (all Criminal Code).

### *Targeted financial sanctions for terrorist financing and proliferation financing*

4.2. Targeted financial sanctions for terrorist financing and proliferation financing are contained in the Charter of the United Nations Act 1945 (CoUNA) and its implementing regulations. The programmes are administered by DFAT, in coordination with other relevant agencies.

### *Not for profit organisations*

4.3. Australia has a general charity regulator, but its focus is on voluntary registration (mainly for tax purposes) and not on TF. About 40 000 of the estimated 140 000 NPOs with legal personality, and 20 000 without legal personality, have registered. No TF-related risk assessment has been conducted, no TF-related monitoring and limited TFS-related outreach has taken place.

## 4.2 Technical Compliance (R.5-8)

4.4. See for the full narrative the technical compliance annex:

- **Recommendation 5 (terrorist financing offence) is rated largely compliant.**
- **Recommendation 6 (targeted financial sanctions related to terrorism and terrorist financing) is rated compliant.**
- **Recommendation 7 (targeted financial sanctions related to proliferation) is rated compliant.**
- **Recommendation 8 (non-profit organisations) is rated non-compliant.**

## 4.3 Effectiveness: Immediate Outcome 9 (TF investigation and prosecution)

### *Prosecution/conviction for TF activity consistent with Australia's risk profile*

4.5. Australian authorities demonstrated a generally broad understanding of TF risk (see IO1 above). Risks are largely influenced by international tensions and conflicts, particularly Iraq and Syria. The main domestic risks involve small-scale collection and use of legitimate and illegitimate funds by domestic cells aligned with, or sympathetic to, radicalised Islamic jihadist groups abroad, for the purposes of committing domestic terrorist acts. The most significant emerging risk is the potential for groups as well as other individuals to send money, directly or indirectly, or raise money for, or otherwise support Australians travelling to conflict zones abroad (especially Syria and Iraq) to support foreign terrorist groups and terrorist acts. An on-going risk relates to how these foreign factors continue to pose risks for terrorist activities within Australia.

4.6. Prosecutions are handled by the Commonwealth Director of Public Prosecutions (CDPP), following referral from an investigative agency. The CDPP has designated combat terrorism (CT) prosecutors in each office, and dedicated CT branches in the Sydney, Melbourne, and Canberra Offices to assess briefs of evidence alleging terrorism related offences and to prepare and carry on matters for prosecution. The CDPP designated CT prosecutors in each of its other offices (Brisbane, Perth, Adelaide, Hobart, and Darwin).

4.7. The CDPP also briefs external counsel to provide advice in CT prosecutions, including provision of qualified advice during the investigation stage, and to conduct prosecutions. The CDPP works closely with the AFP to bring the strongest case possible. Cooperation involves the provision of legal advice, the provision of training to AFP CT investigators as required, and joint scenario-based exercises with AFP investigators.

4.8. **Australian authorities have not prosecuted all different types of TF offences.** Australia has prosecuted nine individuals for TF and convicted three. All nine of these prosecutions were for section 102.6(1) CC—making funds available to a terrorist organisation.

4.9. Authorities have prosecuted 41 individuals under Australia's counter-terrorism framework. Twenty-three have been convicted of terrorism offences under the Criminal Code (such as conspiracy to commit or preparation of a terrorist act, or membership of a terrorist organisation); three have been convicted of making an asset available to a proscribed entity under the CotUNA, one has been convicted of an offence under the *Crimes (Internationally Protected Persons) Act 1976*, and one has been convicted under the *Crimes (Foreign Incursions and Recruitment) Act 1978*.

4.10. Most of these terrorism prosecutions have resulted from three counter-terrorism investigations. *Operation Pendennis* (which included TF charges) and *Operation Neath* both involved domestic, "home-grown" cells, sympathetic to radicalised terrorist groups, which aimed to commit terrorist acts on Australian soil in response to Australia's involvement in counter-terrorism efforts abroad. Operation Halophyte involved domestic individuals sending funds to support a foreign terrorist organisation (Liberation Tigers of Tamil Eelam (LTTE)). The cases can be summarised as follows:

- *Operation Pendennis* (2005-2009): involved the prosecution of 13 individuals based in Melbourne, and 9 based in Sydney. The Melbourne cases included charges against six individuals for TF (section 106(1) of the CC—attempting to intentionally make funds available to a terrorist organisation), which resulted in three convictions, as well as convictions for other terrorist offences. The specific terrorist acts the group aimed to commit were not identified. The funding involved was raised from legitimate and illegitimate sources (mainly theft and fraud). Three of the defendants charged with TF were acquitted.
- *Operation Neath* (2009-2010): involved the prosecution of five individuals for terrorism charges, and conviction of three, who plotted to attack the Holsworthy Army barracks. TF charges were not laid in this case.
- *Operation Halophyte* (2007-2009): involved the prosecution of three individuals who were alleged members of, and provided support and/or funds to, LTTE. Charges included section 106(1) of the CC—attempting to intentionally make funds available to a terrorist organisation, i.e. LTTE. These charges were later dropped, given the difficulty to gain evidence relevant to their defence from northern Sri Lanka. However, the individuals were convicted of other terrorist-related offences (i.e., making an asset available to a proscribed entity under Australia's targeted financial sanctions regime).

4.11. As noted above, **the Pendennis case involved convictions for the provision of funds to be used by a terrorist organisation—authorities have not prosecuted other types of TF offences (i.e., collection of funds for TF, the financing of terrorist acts or individual terrorists).**

4.12. Prosecutors have identified potential difficulties in demonstrating a connection with a terrorist act when pursuing an individual, as well as difficulties in proving that an organisation is a terrorist organisation when it is not formally designated under the Criminal Code (which was the case in Operation Halophyte). It is also difficult to pursue TF charges that relate to money supporting terrorists in other countries. The money trail becomes difficult to follow as funds are first transferred to conduit countries -generally countries neighbouring conflict zones making it difficult to prove the final destination of the funds. Prosecutors also face challenges in complex, large-scale investigations involving a large number of people, and indicated that pursuing specific TF charges would add to the burden of prosecutors, without adding much value to the case or sentences (since terrorism offences carry sentences of up to life imprisonment). Australia also focuses on disrupting potential terrorist activity, given the potential high impact of terrorism, before a TF case would have

time to be developed. For these reasons, specific TF charges are not often pursued. The technical deficiencies identified in R.5 have not negatively impacted Australia's investigation and prosecution of TF offences.

### *TF identification and investigation*

4.13. **Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation.** TF is an avenue of enquiry in all terrorism investigations that are conducted. Where evidence supports other more specific offences, TF will be examined as an adjunct to the broader investigation.

4

4.14. In 2010, the AFP established a Terrorism Financing Investigations Unit (TFIU) dedicated to addressing the TF aspects of all matters identified for consideration of criminal investigation. The TFIU is a multi-agency, multi-jurisdictional team with representation from the AFP and State police, AUSTRAC, and input from the Australian Intelligence Community (AIC). It is based on similar successful groups operating in the UK (NTFIU) and the United States (TFOS). The TFIU provides expertise, specialised support, and focused engagement on an Australia-wide basis with internal and external stakeholders on all aspects of TF. The TFIU, based in the AFP's Sydney office, consists of six AFP employees as well as seconded staff from other agencies. All CT investigations which TFIU supports, are done through an investigator nominated as a financial coordinator to the investigation. Seconded members included one staff member from AUSTRAC, one staff member from an AIC agency, and, 2 New South Wales Police officers. Non-seconded staff members also contribute on a regular basis by attending TFIU coordination meetings, and by being available as a direct agency contact point for the TFIU. Both seconded and non-seconded membership fluctuates over time and as needed. The TFIU also has contact points in all Australian capitals to help facilitate a national counter-terrorism approach. The broader CT staffing for the AFP includes approximately 129 (full-time-equivalent) AFP employees complemented by staff from State police and other organisations.

4.15. The AFP has investigated 36 matters which were either TF matters or had a substantive TF component as part of the investigation. The cases included the mentioned prosecutions above and focussed, wholly or in part, on TF aspects which could have led or did lead to charges for TF offences. The investigations were preventative, as proactive steps were taken to ensure that a terrorist act did not occur or that a terrorist, terrorist act or terrorist organisation would not be funded. **In the two cases where TF offences were prosecuted, the investigations identified the financiers.**

4.16. The identification of terrorism cases occurs through a variety of means including:

- information provided by human sources;
- community reporting, including anonymously;
- information coming to the attention during the course of an existing investigation; and
- referral by AIC agencies or by foreign law enforcement or intelligence agencies.

4.17. Once a matter is identified, the full range of investigative powers (see Recommendation 31) supports the investigation process. These powers have been used in Australia's successful terrorism investigations. Investigators can also access relevant analytical software tools through AUSTRAC, or through the authorised disclosure of information which can be analysed using AFP analytical software, to support joint operational and task force investigations. More generally, spreadsheet software and analytical software linked to operational databases provide important means to address the TF components of terrorism investigations.

### *TF investigation integrated with and supporting national counter-terrorism strategies and investigations*

4.18. Counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks, and TF investigation has contributed to this. **TF investigation is integrated with, and used to support, national counter-terrorism strategies, and investigations.** Financial intelligence, in particular AUSTRAC information, has contributed to broader

investigations by identifying other persons of interest and the existence of networks. There is also an AUSTRAC Senior Liaison Officer embedded in the TFIU. This has assisted in opening new lines of enquiry or options for disruption. The TFIU has assisted in identifying:

- the financial activities of a suspected terrorist or terrorist supporter;
- evidence of the means by which a terrorist may conduct his or her financial activity;
- evidence of financial transactions conducted;
- evidence about the time, date and place where financial activity occurs; and
- financial evidence which can be correlated against evidence from other sources, such as surveillance, travel movements or telephone interception, as a means of corroboration.

### *Effective, proportionate, and dissuasive sanctions*

4.19. The sanctions applied against natural persons convicted of TF offences have been effective and proportionate; however, their dissuasiveness is unclear. Three convictions have taken place—all as part of the Pendennis case. The total effective sentences imposed on the accused in relation to all offences were:

- Ahmed Raad: 8 years with a non-parole period of 6 years' imprisonment (including 5 years for TF)
- Aimen Joud: 8 years with a non-parole period of 6 years' imprisonment (including 5 years for TF), and
- Ezzit Raad: 6 years with a non-parole period of 4.5 years' imprisonment (including 4 years for TF)

4.20. One person convicted of terrorism (not TF) charges in the Pendennis case has returned to a conflict zone in the Middle East to support designated terrorist groups (including the Islamic State of Iraq and the Levant (ISIL)) and advocate terrorist activity (mainly through social media). On the other hand, the ideological nature of these individuals and their associations may explain such recidivism, rather than the sanctions previously imposed on them.

### *Other criminal justice and other measures to disrupt TF activities*

4.21. Australia primarily and successfully uses other criminal justice and administrative measures to disrupt TF activities when a prosecution for TF is not practicable. Australia places a strong focus on disrupting terrorist organisations, and terrorist acts before they occur. Thus, investigations may not advance to the stage where a TF charge is practicable. As noted above, there are also practical difficulties in pursuing TF offences.

4.22. The CDPP examines the briefs of evidence provided by the AFP and decides, in line with the Prosecution Policy of the Commonwealth, on the available and appropriate charges to bring. The assessment of the evidence by the CDPP may result in other terrorism offences in the Criminal Code, (e.g. doing an act in preparation for, or planning, terrorist acts or providing support to a terrorist organisation), offences under the CotUNA (e.g. making an asset available to a designated person or entity), or offences under the *Crimes (Foreign Incursions and Recruitment) Act 1978* (e.g. preparations for incursions into foreign states for purpose of engaging in hostile activities) being brought. Administrative action includes ASIO issuing adverse security assessments to DFAT, which can lead to a revocation of a passport.

4.23. These measures are being used to identify and disrupt domestic terrorist activity and the provision of financial support from Australia to offshore extremist groups. This confronts the risk posed by individuals travelling to conflict areas abroad (in particular Syria and Iraq) to become directly involved in designated terrorist groups, and so called “lone-wolves”, who may be sympathetic to but are only indirectly aligned with such groups. The authorities have already convicted one individual under the *Crimes (Foreign Incursions and Recruitment) Act 1978*, and had begun prosecutions of three more at the time of the on-site visit. Since 1 July 2013, the federal government has also cancelled more than 70 passports on national security grounds.

## Overall conclusions on Immediate Outcome 9:

4.24. Australia exhibits most characteristics of an effective system for investigating, prosecuting, and sanctioning those involved in terrorist financing. It is positive to note that Australia has undertaken several TF investigations and prosecutions, and also secured three convictions for the TF offence. Australia also successfully uses other criminal justice and administrative measures to disrupt terrorist and TF activities when a prosecution for TF is not practicable. Australia had successfully disrupted two domestic terrorist plots (Pendennis and Neath) at the time of the on-site visit.<sup>2</sup> Australia also uses these other measures to address the most relevant emerging TF risk – individuals travelling to conflict zones to participate in or advocate terrorist activity. Australian authorities identify and investigate different types of TF offences in each counter-terrorism investigation, and counter-terrorism strategies have successfully enabled Australia to identify and designate terrorists, terrorist organisations, and terrorist support networks. Australian authorities have not prosecuted all the different types of TF offences, such as the collection of funds for TF, or the financing of terrorist acts or individual terrorists, and the dissuasiveness of sanctions applied has not been clearly demonstrated.

4.25. **Australia is therefore rated as having a substantial level of effectiveness for IO.9.**

## 4.4 Effectiveness: Immediate Outcome 10 (TF preventive measures and financial sanctions)

### *Targeted financial sanctions for TF*

4.26. **Australia is actively using the TFS framework and demonstrates some characteristics of an effective system for TFS.** With UNSCR 1267/1989 and UNSCR 1988 designations, the legal obligation to freeze assets is automatic upon designation at the UN; no additional action by Australian authorities is needed to give legal effect to a designation. Nevertheless, when there is a change in the listing at the UN, the next business day DFAT amends its Consolidated List to reflect changes in the UNSCR 1267 designations and the updated Consolidated List is published on the DFAT website and circulated for information to subscribers via email. **The automatic asset freeze obligation is a best practice for other countries on how UN designations can be implemented without delay.**

4.27. Australia had co-sponsored or acted as co-designator for a number of designations at the UN. Australia's decision to co-sponsor proposals or co-designate, includes consideration of whether the proposed designation has links to Australia or is otherwise in Australia's national interest. At the time of the on-site visit, Australia also took into account the necessity of ensuring its impartiality as chair of the UNSCR 1267/1989 and 1988 Committees when considering possible co-sponsorship or co-designation.

4.28. Australia is also using its framework to domestically list individuals and entities pursuant to UNSCR 1373 and has listed 89 persons and entities (at the time of the on-site). At the domestic level, targets for listing can be proposed to DFAT by any agency, including AFP, AGD, ASIO and other intelligence agencies. DFAT then works with intelligence agencies and law enforcement to determine if the proposed designee meets the legal test for designation. Authorities can use both open source and classified information in the creation of a statement of reasons (SOR), but the preference is to rely as little as possible on classified information in composing the SOR. After consideration by the Ambassador for Counterterrorism (a DFAT official), the SOR and a recommendation for listing, is submitted to the Minister for Foreign Affairs, who makes a final determination. After listing, a designee may contact DFAT for a copy of the unclassified SOR.

2 Another plot was disrupted soon after the on-site visit. AUSTRAC also took action in November 2014 to cancel the registration of remittance dealer (Bisotel Rieh Pty Ltd) due to concerns that its continued registration may involve a TF risk. This followed a period of engagement and notification of action by AUSTRAC.

4.29. Third party requests from foreign jurisdictions are considered under the same process. Australia receives requests either directly through DFAT or via its embassies or High Commissions abroad. DFAT begins consideration of such requests within one business day. Australia has received numerous requests from foreign jurisdictions since the establishment of the regime and has given effect to both formal and informal requests. DFAT noted that most of its domestic designations were a result of either formal requests or informal discussions with like-minded countries. Where Australia does not believe that the information provided meets the legal threshold for designation (for example due to differences in designation criteria or because the request is politically motivated), authorities still continue to monitor the individuals and entities for information to substantiate a designation. Australia has never formally rejected a request. From November 2013 to June 2014, Australia received only 3 formal third party requests. At the time of the on-site visit, authorities were advancing one for domestic designation.

4.30. Australia has made no unilateral requests to other countries for consideration of the names it has designated.<sup>3</sup> Australia explained that many of the designees it believes would have warranted a third-party request were subsequently designated at the UN or were subject to a third-party request by a like-minded country with Australia's active or in-principle support, often after informal discussions between Australia and a group of like-minded countries.

4.31. All designations made pursuant to Australia's implementation of UNSCR 1373 must be reviewed every three years. The review process is similar to the process for the initial listing and is to determine that the designee continues to satisfy the criteria for listing. DFAT also invites, via a media release and posting on its website, public submissions for the review regarding listees and anyone can make a submission. The Minister for Foreign Affairs must make a formal determination to renew the listing or the listing expires. As a result of the review process, four listings were permitted to expire in 2013.

4.32. Listees may apply to the Minister for revocation of the designation. Since 2002, DFAT has received three de-listing requests related to TF TFS. Two requests were filed by the same entity and were rejected in 2003 and 2004; the third request, which was filed in January 2014, was still pending at the time of the onsite visit.

4.33. As part of its outreach efforts, DFAT administers an Online Sanctions Administration System (OSAS) through which members of the public can enquire if an activity is subject to prohibitions under the sanctions regime and can apply for a sanctions permit (license). Across the TFS regimes, the average time to consider a request for a sanctions permit is approximately 15 days. DFAT also offers LinkMatchLite software to assist asset holders to consider the probability that a provided name is a match with a name on the Consolidated List. Under section 41 of the *Charter of the United Nations (Dealing with Assets) Regulation 2008*, asset holders may contact the AFP for assistance to determine whether or not an asset is owned or controlled by a listee (the process has been agreed by DFAT, the AFP, the Australian Bankers Association and major banks, and as set out on the website of DFAT). Based on the information available to the AFP, it provides an indication as to whether a name match to the Consolidated List is 'likely', 'unlikely' or 'unknown'. Under its TF sanctions regime Australia has frozen property related to only one entity listed pursuant to 1373; in 2002 AUD 2 000 was frozen in multiple bank accounts for the listed entity. There was also a false positive in 2002, where funds were initially frozen and then released. DFAT also conducts sanctions-related outreach to businesses, universities, and individuals and holds national outreach tours twice a year and speaks at relevant seminars and conferences. The March 2014 DFAT outreach events had over 100 attendees from across ten sectors, including banks, law firms, mining and dual use industries.

4.34. DFAT has primary responsibility for compliance with sanction requirements and it does issue production orders to enforce the sanctions framework. However, this is a reactive process, as DFAT's production orders are usually in response to a suspected violation. DFAT also undertakes outreach to educate society on the requirements. However, DFAT does not monitor or supervise the financial sector for compliance with the requirements of the FATF Recommendations (which would be difficult given that DFAT is not a supervisory

<sup>3</sup> After the on-site, Australia made requests to other jurisdictions following designations in Australia under UNSCR 1373.

entity) and as expected of a supervisory authority. In addition, no financial institutions are supervised or monitored for compliance with the TFS requirements (as in financial supervision) by any other competent supervisory authority. This is a major shortcoming in the supervisory regime, as reflected under IO.3, but is relevant for IO.10 to measure effective implementation. The assessment team also confirmed that AUSTRAC does not check its own databases for matches with DFATs lists on an ongoing basis. AUSTRAC staff indicated that the vast number of false positives this would generate, would make this a challenging or impossible task. However, there is an internal SMR analysis rule that allows for checking with possible list hits, and reporting agencies can indicate on an SMR that there is a possible list hit. In addition, when discussing company registration with ASIC, ASIC stated that it does not automatically check the DFAT lists when registering a company, its directors or its shareholders. Not checking government databases against government issued lists effectively limits the same government ability to detect compliance breaches.

4.35. Assessors also sought to establish effective implementation of the requirements during interviews with the private sector, or through the statistics. All financial institutions were aware of their obligations to freeze (often referred to as the “UN, OFAC and DFAT lists”) and confirmed that they were not supervised for compliance with their sanctions obligations. A few were aware that they should contact AFP if there was a question about whether they had a match with the Consolidated List, but most were unable to share feedback on the remaining practical issues that inevitably would have to come up during implementation (e.g. how to deal with similar names i.e. false positives issues; what assets needed to be frozen) and that would establish that the private sector effectively implements the requirements. Moreover, as indicated above, despite the large number of domestic designations (89 at the time of the on-site visit), only in one case were assets detected (approximately AUD 2 000 in 2002), and one false positive in 2002. The list of designated entities contains names that are common in Australia. As a result, it could be reasonably expected that similar names would have caused false positives, which would have allowed financial institutions to gather experience with dealing with false positives, demonstrating that the system was being effectively implemented.

4.36. A possible explanation for this lack of evidence of implementation may be that it seems that the sanctions framework to implement UNSCR 1373 is not used to target entities in Australia or against Australian citizens (at the time of the on-site), which indeed limits the likelihood of detecting funds and other assets of designated entities in Australia. This is in line with another related shortcoming, which is that the legal provisions are not applied systematically by the authorities. Specifically, some of the persons that had previously been convicted in Australia for terrorism or terrorist financing completed their sentences and then left Australia to openly take part in terrorist acts abroad. At the time of their travel, the groups that these Australians joined (Jabhat al-Nusra or JN and Islamic State of Iraq and the Levant or ISIL) were already designated by the federal government under UNSCR 1373 (JN) and under UNSCR 1267 (ISIL and JN) in 2013. Nevertheless, at the time of the on-site, these persons (especially those that had previously been convicted) had not been referred to the UN (under UNSCR 1267) for designation, or designated domestically (under UNSCR 1373). It should, however, be noted that two of these individuals were considered by the federal government for designation. Designation of these two persons took place on 13 November 2014, which was only after the on-site. The Australian authorities believe that their regular interaction with financial entities regarding possible designated entities before an institution entered into a customer relationship also limits the number of possible false positives.

4.37. **The Australian legal framework for the implementation of TFS is a good example for other countries, especially the immediate legal obligation to freeze assets as soon as an entity is listed by the UN, and the numerous designations made under the domestic regime are to be commended as best practices for other countries. However, effective implementation of the framework is difficult to confirm in the absence of freezing statistics, financial supervision, supervisory experience, and feedback on practical implementation by the private sector.**

### *Non-Profit Organisations (NPOs)*

4.38. The NRA cites charities and NPOs as one of the key channels that can be used to raise funds for TF in or from Australia. It notes that organisations can be exploited in a number of ways, including disguising international funds transfers to high-risk regions, co-mingling of humanitarian aid and funds raised to finance terrorism, and diversion or siphoning of legitimate funds by or to terrorist groups after the funds arrive in the destination country.

4.39. Despite the general risks identified by the authorities in the NRA, Australia has not undertaken a risk review of the NPO sector to identify the features and types of NPOs that are particularly at risk of being misused for TF. Subsequently, there is no TF-related outreach to, or TF-related monitoring of, the part of the sector that would be at risk and that account for a significant share of the sector's activities.

4.40. Australia's general NPO regulator, the Australia Charities and Not-for-profits Commission (ACNC) was established in 2012 to administer the framework for the voluntary registration and regulation of charities. Only charities are permitted to register with the ACNC. About 40 000 of the 140 000 NPOs with legal personality and 20 000 without legal personality have registered, and mainly to take advantage of tax incentives. The ACNC has the ability to conduct reviews of registered charities, which focus on whether the organisation has a charitable purpose and the funds are used solely for that purpose. While the ACNC actively works to improve transparency, it has no specific TF mandate and it has not conducted outreach to the NPO sector regarding TF risks.

4.41. **Outreach efforts to the NPO sector are minimal, and not targeted.** In 2009 the AGD issued a brochure "Safeguarding Your Organisation against Terrorism: A Guidance for Non-profit Organisations". This non-binding guidance sets out best practice principles for NPOs, including on undertaking risk assessments, applying due diligence procedures to beneficiaries and third parties, being aware of legal obligations, and ensuring internal processes of transparency and accountability. In 2013 the AGD issued a fact sheet about the ongoing violence in Syria; the document focuses primarily on the Australian sanctions obligations and the best way to donate funds for humanitarian support. Both documents focused mainly on DFAT-lists requirements.

### *Terrorist asset seizure and confiscation (criminal justice measures)*

4.42. Two TF cases have been referred to CACT since its establishment to recover TF related assets. No seizures or confiscations resulted from these referrals. These outcomes do not seem commensurate with the overall TF risk.

## Overall conclusions on Immediate Outcome 10

4.43. Australia demonstrates some characteristics of an effective system in this area. Terrorists and terrorist organisations are being identified in an effort to deprive them of the resources and means to finance terrorist activities.

4.44. An area of strong technical compliance is the legal framework for TFS against persons and entities designated by the UNSC (UNSCR 1267) and under Australia's sanctions law (for UNSCR 1373). Australia has co-sponsored designation proposals to the UNSCR 1267/1989 Committee and adopted very effective measures to ensure the proper implementation of UN designations without delay. Australia has also domestically listed individuals and entities pursuant to UNSCR 1373 (including most recently two Australians fighting overseas for terrorist entities) and received, considered and given effect to third party requests. Australia actively works to publicly identify terrorists and terrorist organisations.

4.45. Furthermore, the TFS regime is administered robustly. Australia has procedures for:

- i. identifying targets for listing,
- ii. a regular review of listings, and
- iii. the consideration of de-listing requests and sanctions permits.
- iv. The authorities make a concerted effort to sensitize the public to Australian sanctions laws and to assist potential asset holders in the implementation of their obligations.

4.46. However, the private sector is not supervised for compliance with TFS requirements and was unable to demonstrate that the legal framework is effectively implemented. Effective implementation is difficult to establish in the absence of freezing statistics, financial supervision, supervisory experience, and feedback on

practical implementation by the private sector. Designating Australians previously convicted for terrorism or terrorist financing, who openly join designated terrorist organisations, could improve the system's effectiveness.<sup>4</sup>

4.47. NPOs are an area for improved efforts and specific action. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a targeted TF review and subsequent targeted TF-related outreach and TF-related monitoring of NPOs leaves NPOs and Australia vulnerable to misuse by terrorist organisations. Since 2010, no effort has been directed at NPOs to sensitise them to the potential risk of misuse for TF. While the ACNC actively works to improve transparency, it has no specific TF mandate and it has not conducted outreach to the NPO sector regarding TF risks.

4.48. **Australia has been rated for a moderate level of effectiveness for IO.10.**

### 4.5 Effectiveness: Immediate Outcome 11 (PF financial sanctions)

#### *Targeted financial sanctions related to proliferation financing*

4.49. Australia's legal system and processes for implementing UNSCRs 1718 and 1737 (as required by Recommendation 7 and assessed in this IO) are identical to those for implementing UNSCR 1267 (as required by Recommendation 6 and assessed in IO.10). The same key findings apply: a sound legal system and process exist. However, the assessors were unable to ascertain effective implementation of the requirements due to the absence of a supervisory or other compliance testing framework, the absence of implementation feedback from the financial sector, and the absence of freezing actions (including for false positives).

4.50. In addition, Australia has a proliferation-related autonomous sanctions regime, as described in the paragraphs below. This capability, and the process Australia undergoes to identify proliferation-financing targets, contributes to the overall effectiveness in preventing persons and entities involved in the proliferation of WMDs from raising, moving, and using funds.

#### *Domestic cooperation to implement obligations to combat the financing of proliferation*

4.51. DFAT takes the lead on domestic coordination regarding operational threats, cases, and international cooperation in relation to proliferation financing. DFAT discusses operational issues with domestic partners, and reaches out to the businesses that are involved. Part of this work relates to the authority of DFAT to grant licences that relate to UNSCR 1718 and 1737.

4.52. With respect to UNSCR 1718 and 1737, DFAT considers applications for sanctions permits for trade in goods and services as well as for financial transactions, and has implemented a unified system that facilitates a holistic approach to any proposed activity. Consideration of applications for sanctions permits for trade in goods and services includes seeking information about related financial transactions to ensure DFAT bases decisions about proposed activities on full information.

4.53. In considering sanctions permit applications, DFAT coordinates principally with Defence (including the Defence Export Control Office, DECO), the Australian Customs and Border Protection Agency (ACBPS) and the Australian Intelligence Community, and other agencies as appropriate. DFAT's Sanctions Section's contacts with relevant agencies appear well developed, which facilitates early identification of possible cases of proliferation financing concern and a coordinated whole-of-government response. The monthly inter-agency Non-Proliferation Coordination Group, co-chaired by DFAT's Arms Control and Counter-Proliferation Branch and attended by the Sanctions Section, is the primary mechanism for raising and discussing issues of concern, whether these are individual cases or emerging trends. All relevant agencies, including ACBPS,

<sup>4</sup> At the time of the on-site, two of these individuals were under consideration by the government for designation. Designation of these two persons subsequently took place on 13 November 2014, after the onsite.

DECO, and AUSTRAC attend these meetings. The Sanctions Section is also in direct daily contact with ACBPS and DECO, and has established standard operating procedures in agreement with these agencies to facilitate coordination of sanctions permit applications.

4.54. As reflected under IO. 10, all financial institutions were aware of their obligations to freeze (often referred to as the “UN, OFAC and DFAT lists”) and confirmed that they were not supervised for compliance with their sanctions obligations. However, there was strong evidence that the financial institutions were actively seeking to comply with TFS obligations due to the possible reputational risks and legal penalties flowing from contravening Australian sanction laws as well as concerns connected to supervisory action that had taken place in other jurisdictions for non-compliance with IO.11 / PF-related TFS obligations. DFAT is the competent authority for processing informal inquiries and formal applications relating to sanctions permits. Since 2010, DFAT has received only one application in relation to targeted financial sanctions under UNSC Iran or DPRK sanctions, which was refused. DFAT has received 276 inquiries and 873 applications in relation to trade in goods and services under UNSC and Australian autonomous DPRK and Iran sanctions. Of the 873 applications, 404 were granted, 36 denied, 326 withdrawn, and 107 never required a permit. In considering inquiries and applications, DFAT checks its own sanctions lists and the AUSTRAC database, and may also reach out to the intelligence services and – as required – to the UN. DFAT also coordinates with universities to ensure that export controlled knowledge is not acquired by sanctioned countries.

## Overall conclusions on Immediate Outcome 11

4.55. Australia demonstrates to a large extent the characteristics of an effective system in this area. The issues listed under IO.10 and that relate to UNSCR 1267 also apply to IO.11.

4.56. Even though IO.11 suffers from the same issues as IO.10, IO.10 has additional shortcomings in relation to NPOs that do not apply to IO.11. In addition, the overall domestic cooperation in relation to country sanction programmes for Iran and DPRK seems sound, which may have a positive effect on the targeted financial sanctions implementation that are related to these country programmes. This domestic cooperation benefit does not apply in the case of IO.10 / UNSCR 1267, as it is not a country programme.

4.57. **Australia has been rated for a substantial level of effectiveness for IO.11.**

## 4.6 Recommendations on Terrorist Financing and Financing of Proliferation

### *Investigating and prosecuting terrorist financing (IO.9)*

- Australia should give consideration, where appropriate, to actively prosecuting different types of TF offences.

### *Targeted financial sanctions on TF (IO.10) and financing of proliferation (IO.11)*

- Australia should ensure financial institutions are actively supervised for implementation of DFAT lists, ideally through a legislative amendment to the statute identifying and authorising the agency responsible for supervision. Specifically, supervision should include a focus on those issues that other countries’ supervisors have detected in relation to non-compliance with targeted financial sanctions requirements by global financial institutions, such as the facilitation of sanctions evasion by financial institutions (IO.10 and IO.11) (see also IO.3).
- Australia should ensure that government entities implement and/or supervise the targeted financial sanctions requirements of DFAT. This includes monitoring AUSTRAC’s and ASIC’s databases for possible matches (IO.10 and IO.11).
- Australia should take comprehensive measures to ensure that DNFBPs can also be supervised or monitored for compliance with targeted financial sanctions requirements (IO.10 and IO.11).

## TERRORIST FINANCING AND FINANCING OF PROLIFERATION

- Australia should continue using its preventive designation powers against identified (self-declared) members of designated terrorist groups, or propose the names of these persons for designation to the UN (IO.10).
- Australia should implement a targeted approach in relation to preventing NPOs from TF abuse. As a first step, Australia needs to undertake a thorough review of the TF risks that NPOs are facing (beyond the issues already covered in the NRA) and the potential vulnerabilities of the sector to terrorist activities. Australia should then apply the required measures to those NPOs that are at risk and that account for a significant portion of the financial resources under control of the NPO sector, and a significant share of the sector's international activities (IO.10).

4

## 5. PREVENTIVE MEASURES

### Key Findings

5

**Reporting entities' understanding of their ML/TF risks and the effective implementation of preventive measures varies across and within sectors.** The major reporting entities – including the big four domestic banks which dominate the financial sector – have a good understanding of their Australian AML/CTF risks and obligations, which do not all comply with FATF Standards.

**Australia's requirements on CDD, beneficial ownership, and the requirements for PEPs were enhanced on 1 June 2014.** Most of the reporting entities interviewed by the assessment team advised that they are not yet able to apply the improved requirements; they have a transition period until 31 December 2015. Therefore, those reporting entities that are applying the pre-June 1 measures are not adequately identifying beneficial owners or applying CDD to PEPs.

**DNFBP sectors, other than casinos and bullion dealers, including those assessed as high risk in the NTA, are not subject to AML/CTF regulation, and have demonstrated a poor understanding of their ML/TF risks.** Australia should establish comprehensive AML/CTF obligations for all DNFBPs as a matter of priority.

## 5.1 Background and Context

### (a) Financial Sector and DNFBPs

5.1. Australia's financial sector is the 12th largest in the world, and is dominated by banks. Total banking sector assets amount to over 200% of GDP (over AUD 321.1 billion). Australia's banking sector is the third largest in the Asia-Pacific region, following Japan and China, and is highly concentrated, with the four largest banks accounting for 78% of the total banking assets. The Australian banking system comprises a mix of domestic and foreign players, with 48 of the 68 licensed banks being subsidiaries or branches of foreign banks.

**Table 5.1. Type of Financial Institutions Authorised to Conduct Financial Activities and Operations**

Type of financial institution	No. of entities
Banks	68
Australian owned banks	20
Foreign Subsidiary Banks	8
Branches of Foreign Banks	40
Building Societies	9
Credit Unions	85
Specialised credit card institutions	2
Other authorised deposit-taking institutions	4
Finance companies – Australian Credit Licensees	5 856
Authorised Credit Representatives	28 201
Lease Finance Companies – Credit Licensees Providing Consumer Leases	4 102 With 19 330 authorised representatives
Money Remittance Companies	6 230
Australia Financial Securities Licensees	5 093
Financial Markets	18
Clearing and Settlement Facilities	6
Market Dealers	136 market participants
Securities Dealers	800
Friendly Societies	12
Superannuation Funds and Trustees	200 superannuation fund trustees 53 Pooled Superannuation trusts 2 979 small APRA funds 62 Single-member authorised deposit funds 528 701 self-managed superannuation funds
Funds Managers	
Managed Investment Schemes (trustees)	784 494 responsible entities for MIS
Registered Managed Investment Schemes	4 152
Foreign Financial Service Providers	614

**Table 5.1. Type of Financial Institutions Authorised to Conduct Financial Activities and Operations (continued)**

Type of financial institution	No. of entities
Custodial Service Providers	718
Investment Banks	26
Hedge Fund Managers	250
Retail Over-the-Counter (OTC) Derivative Providers	43
Life insurers / Life Insurance Brokers/ Life Insurance Agents	28
Foreign exchange contracts – Australian Financial Services License holders	1 079
AFS Authorised Representatives	7 853
Money and currency exchange providers – bureaux de change	108

5.2. Australia is one of the major centres of capital market activity in the Asia Pacific region. Annual turnover across Australia's financial markets was AUD 135 trillion in the year to June 2013. Australia's total stock market capitalisation is more than USD 1.3 trillion, making it the 10th largest market in the world and the 4th largest in the Asia Pacific region. Australia's foreign exchange market is ranked 8th in the world by turnover, with the AUD/USD the fourth most actively traded currency pair in the world by turnover.

5.3. Australia has a large number of remittance providers which provide an important service to Australia's significant multicultural society. MVTS are offered by remitters, which fall into three types: remittance network providers (RNPs); agents or affiliates of the RNP; and independent remittance providers. Over 6 000 reporting entities registered with AUSTRAC operate in the remittance sector in one of these three categories. More than 5 500 of these entities are agents or affiliates of RNPs and the value of transactions flowing through the remittance sector is relatively concentrated. The top five networks account for 90% of all MVTS. The top 14 remitters account for 83% of the value of funds transferred in and out of Australia through the remittance channel. Outside of these networks, there are approximately 650 independent remitters registered with AUSTRAC. In terms of value, international funds transfers through remitters accounted for 1.7% or AUD 66 billion of over AUD 3.9 trillion aggregate international funds transfers in 2013. The banking sector accounts for more than 95% of the total cross-border funds transfers.

5.4. The NTA highlights banks, the gaming sector, and remitters as the main channels for ML (and also for TF through the remitters). Specifically, the NTA appears to have been a substantial driver for the creation of the Eligio National Task Force in December 2012. As noted earlier, the four largest banks are domestic banks and account for 78% of total banking assets and 66% of the international funds transfers by value. AUSTRAC has a dedicated team called Major Reporters, which regulates the 19 most significant reporting entity groups (REGs) comprising mainly the major Australian and foreign banks. In considering the risk and context of the financial sector, assessors gave greater material importance to the domestic banks and remitters.

5.5. Most of the DNFBPs operate in Australia. As highlighted under IO.1, the real estate sector has been identified by authorities as a high ML/TF risk, and professional facilitators (lawyers, accountants, trust and company service providers – especially from lower tier firms) were almost universally considered a major risk for ML. The real estate sector in Australia was also identified as an attractive avenue for investments, including by organised crime groups looking to launder illicit monies. As a result, the assessors viewed these sectors as materially important in determining effectiveness.

**Table 5.2. DNFBPs: Type and number of entities**

Type of Entity	Number of entities
Casinos	12
Lawyers	The Law Council acts on behalf of approx. 56 000 legal practitioners
Notaries	Approx. 260
Accountants	Institute of Public Accountants – over 25 000 members in 50 countries Certified Practicing Accountants Australia – over 150 000 in 121 countries Institute of Chartered Accountants Australia – over 73 000 members globally
Precious Metals & Stones Dealers	82 Bullion Dealers Jewellers Association of Australia - 1 100 outlets
Trust and Company Service Providers	Approx. 300 company formation agents.
Real Estate Agents	35 019

### (b) Preventive Measures

5.6. Australia's AML/CTF regime has undergone significant reform since the last assessment in 2005. The most important reform was the enactment of the AML/CTF Act in 2006, which expanded the scope and coverage of Australia's AML/CTF regime. Businesses with AML/CTF obligations increased from approximately 3 000 under the previous AML/CTF regime to about 15 000 under the AML/CTF Act. The AML/CTF Act focuses on the services to be regulated – called “designated services” in the Act – rather than the nature of the entity that provides the service. In broad terms, the AML/CTF Act applies to the services provided by financial institutions, gambling service providers, bullion dealers and remittance dealers. Entities that provide these designated services are known as reporting entities and are supervised by AUSTRAC for compliance with the Act. Beyond bullion dealers and gambling services, including casinos, other DNFBPs (i.e. real estate agents, dealers in precious stones, lawyers, notaries, other legal professionals and accountants, and trust and company service providers) are only covered when they provide one of the designated services – i.e. essentially acting in the capacity of a financial institution under the FATF Recommendations. None of the services designated relates to real estate agents, dealers in precious stones or trust and company service providers activities.

5.7. The AML/CTF Act requires REs to establish an AML/CTF programme, which is divided into two parts – Part A and Part B. The primary purpose of Part A of the standard AML/CTF programme is to identify, mitigate and manage ML/TF risks that a reporting entity faces and includes AML/CTF risk awareness training for employees, employee due diligence program, oversight by boards and senior management, and procedures for independent review of programme. The primary purpose of Part B is to set out the reporting entity's applicable customer identification procedures (ACIP), including beneficial ownership, ongoing customer due diligence and enhanced due diligence. A standard programme applies to a particular RE; joint programmes apply to each reporting entity that belongs to a particular DBG .

5.8. The AML/CTF Act is supplemented by the *AML/CTF Rules Instrument 2007* (AML/CTF Rules), issued by AUSTRAC's CEO pursuant to section 229 of the AML/CTF Act. The AML/CTF Rules expand on the requirements and provide greater specificity with respect to some of the obligations in the AML/CTF Act. For example, the AML/CTF Rules set out the requirements on reporting entities' risk assessments, and include provisions on their adoption of a risk-based approach.

5.9. The AML/CTF Rules were updated on 15 May 2014 via the *AML/CTF Rules Amendment Instrument 2014 (No.3)* (Rules Amendment). The Rules Amendment updated a number of the preventive measure requirements, including those related to customer identification, beneficial ownership, and the provisions of Part A of the AML/CTF program. The Rules Amendment commenced on 1 June 2014 but REs have until 1 January 2016 to fully implement the requirements before certain sanctions will be applied.

(c) *Risk-Based Exemptions or extensions of preventive measures*

5.10. Casinos and bullion dealers are the only categories of DNFBPs subjected to AML/CTF requirements, including the requirement to establish AML/CTF programmes to mitigate ML/TF risks. Other DNFBP sectors such as lawyers, accountants, real estate agents, and trust and company service providers are not subject to such obligations, which is in direct contrast to their assessment as a high threat in the NTA and the risk-based approach. On the regulated sectors, Australia sets the threshold for CDD requirements to be applied to customers of casinos at AUD 10 000 (USD 9 300 / EUR 6 900), which exceeds the USD / EUR 3 000 threshold in the FATF Recommendations. Persons licensed to operate gaming machines are also not subject to most of the AML/CTF obligations under the Australian regime if they operate no more than 15 such machines, although there are State and Territory-level restrictions on winnings paid in cash.

5.11. AUSTRAC has the powers to grant exemptions to specified persons from all or parts of the AML/CTF Act. In practice, it has granted full or unconditional exemptions to various applicants, including those operating in private banking, prepaid cards or investment funds. According to the AUSTRAC Exemption Policy, exemptions are considered based on a number of factors, including – but not limited to – the risk profile of the applicant, the designated service, issues of competitive neutrality, and the level of regulatory burden to which the applicant is being subjected. While AUSTRAC considers these exemptions on a case-by-case basis, the assessment team was not convinced that the exemptions were sufficiently justified as low risk.

## 5.2 Technical Compliance (R.9-23)

5.12. See for the full narrative the technical compliance annex:

- **Recommendation 9 (financial institution secrecy laws) is rated compliant.**
- **Recommendation 10 (customer due diligence) is rated partially compliant.**
- **Recommendation 11 (record-keeping) is rated largely compliant.**
- **Recommendation 12 (politically exposed persons) is rated largely compliant.**
- **Recommendation 13 (correspondent banking) is rated non-compliant.**
- **Recommendation 14 (money or value transfer services) is rated largely compliant.**
- **Recommendation 15 (new technologies) is rated largely compliant.**
- **Recommendation 16 (wire transfers) is rated partially compliant.**
- **Recommendation 17 (reliance on third parties) is rated partially compliant.**
- **Recommendation 18 (internal controls and foreign branches and subsidiaries) is rated partially compliant.**
- **Recommendation 19 (higher risk countries) is rated partially compliant.**
- **Recommendation 20 (reporting of suspicious transactions) is rated compliant.**
- **Recommendation 21 (tipping-off and confidentiality) is rated compliant.**
- **Recommendation 22 (DNFBPs – customer due diligence) is rated non-compliant.**
- **Recommendation 23 (DNFBPs – other measures) is rated non-compliant.**

### 5.3 Effectiveness: Immediate Outcome 4 (Preventive Measures)

5.13. The AML/CTF Act requires reporting entities to perform regular risk assessments. This entails assessing the risk of the reporting entity being involved in or facilitating ML or TF, and determining what the reporting entity will need to do to identify, mitigate, and manage those risks. The AML/CTF Rules specify that in its risk assessment a reporting entity must consider its customer types, the types of designated services it provides, the methods by which it delivers designated services and the foreign jurisdictions with which it deals.

5.14. **Financial institutions' and DNFBPs' understanding of ML/TF risks and measures to mitigate them varies across sectors.** Financial sector representatives demonstrated a better understanding of their ML/TF risks and were better at identifying steps to mitigate and manage those risks. Most DNFBPs that are not subject to prudential or AML/CTF regulation or supervision did not demonstrate an adequate understanding of their ML/TF risks.

5.15. **The understanding of risks and measures also vary across reporting entities within the respective sectors, depending on the scale and complexity of their operations.** Across the board, larger reporting entities demonstrated a better understanding and ability to mitigate their identified ML/TF risks.

5.16. **Across sectors it was reported to the assessment team that smaller reporting entities found it challenging to understand and meet all the AML/CTF requirements.** AUSTRAC has undertaken a large number of outreach strategies to communicate with small to medium reporting entities, including compliance guides for small bookmakers, independent remitters and clubs and hotels and outreach to industry associations. Nevertheless, the small to medium reporting entities have a lower level of understanding of their obligations and risks. To a large extent this is as a result of the inherent characteristics of smaller entities that do not have the capacity to maintain the wide range of compliance resources and capabilities employed by larger entities. Both large and small reporting entities interviewed suggested that insufficient regulatory and enforcement presence was a contributing factor. The larger reporting entities enjoy close working relationships with AUSTRAC and the law enforcement agencies, which enhances their ability to understand the authorities' views on risk. The same opportunity is not as available to the smaller reporting entities, which rely on the NTA and the published AUSTRAC guidance and typologies for insight into how the authorities assess risk. While reporting entities indicated that the guidance and typologies were generally useful, they all noted that these materials could be clearer and more up-to-date.

5.17. **DNFBP sectors that are not subject to the AML/CTF regime generally demonstrate a poor understanding of ML/TF risks.** Most were unaware of the NTA or its findings that many of the unregulated DNFBPs are a high risk for ML. Those that were aware of the NTA disagreed with its conclusions, citing the lack of clear evidence in typologies reports or criminal prosecutions to justify the assessment. Nearly all of these sectors asserted that the ML/TF risks in their respective sectors are low, as they handle no or minimal cash transactions. They also claimed that the current professional standards for their sectors sufficiently protect the sector from abuse by criminals.

5.18. **Banks – Banks operating in Australia generally have a sufficient understanding of the ML/FT risks of their clients, and have a framework in place to mitigate them.** In addition, large banks demonstrated a better understanding of their AML/CTF obligations and had the resources to effectively implement them. This was significantly more challenging for small to medium sized banks due to more limited resources and capacity, as well as the complexity of the requirements laid out in the AML/CTF Act and the AML/CTF Rules.

5.19. **Domestic banks did not have measures that fully meet FATF Standards on CDD, beneficial owners and politically-exposed persons.** This appeared to be due to Australian-based banks limiting the scope of their ML/TF assessment to the scope of the requirements as outlined in AML/CTF Act and Rules. International banks whose home jurisdictions comply with these relevant Standards generally considered a wider array of factors when reviewing the ML/TF risks of their bank and its business lines.

5.20. **Money and Value Transfer Services – Within the remittance sector, the ability to adequately assess risk varies widely.** Large RNPs with global operations seem to adequately identify and mitigate the

risk associated with their product lines and their customers (the five largest RNPs in Australia account for 90% of affiliates). For example, large RNPs will have varying thresholds for enhanced due diligence based on transaction corridor, or customer type based on internally determined risk profiles. Such approaches are less likely in smaller RNPs and independent remitters, but they make up only a limited part of the sector.

5.21. In 2011, regulatory changes were implemented to strengthen the remittance registration process. The criteria applied to registration changed and the AUSTRAC CEO was given the capacity to refuse, cancel, suspend or impose conditions on registration. RNPs were included in the registration process and the compliance obligations of agents/affiliates shifted to the RNP. This included requiring RNPs to undertake due diligence on their affiliate (including requiring RNPs to obtain criminal records checks of all key personnel within their affiliates), providing the agent/affiliate with a compliance program, monitoring agent compliance, training agents, and conducting transaction monitoring of their entire network.

5.22. The 2011 regulatory changes improved the ability of AUSTRAC to monitor the remittance sector and improved implementation of obligations. However, representatives from the sector reported to the assessment team that **implementation of obligations in line with the FATF Standards continues to vary greatly within the sector**. A number of larger remitters and RNPs implement obligations in line with the FATF Standards. Smaller remitters – which account for a small part of the sector – lack capacity to implement Australia's complex regulatory requirements and do not implement preventive measures in line with the FATF Standards.

5.23. In line with Australia's AML/CTF Rules, money remitters are implementing the Australian obligations for wire transfers and the filing of IFTIs, but the existing Rules are not in line with the requirements of Recommendation 16. Smaller remitters were universally identified by the authorities and the private sector as less compliant with Australian AML/CTF obligations and highly vulnerable to ML.

5.24. To improve compliance throughout the remittance sector, sector participants are considering the creation of a professional association of remitters. In addition to furthering compliance, an association would further establish professional standards and would act as an advocate for the sector.<sup>1</sup>

5.25. *Casinos* – The casino sector has been identified by the NTA and AUSTRAC as high risk and is therefore supervised more intensively, especially over the last two years. One of the **larger casinos in Australia demonstrated a good understanding of its AML/CTF obligations** and reported having more stringent AML/CTF measures than what the law required in some aspects. For instance, they set lower cash thresholds for CDD triggers, or have wider scope of due diligence. This is driven in part by their desire to better manage business and reputation risks in their activities, and/or to ensure the chances of success in renewing or holding on to their licences. Given the relatively small number of casino operators and AUSTRAC's supervisory focus on this sector, the discrepancy among casino operators in implementing AML/CTF measures that are commensurate with their scale and ML/TF risks is unlikely to be as large as in some other sectors.

5.26. *Bullion dealers* – Bullion dealers are regulated by AUSTRAC and are required to comply with AML/CTF obligations. Consistent with feedback from most private sector representatives, the larger bullion dealers attract regular scrutiny from AUSTRAC, and are likely to demonstrate better understanding of their AML/CTF obligations and have adequate AML/CTF safeguards as a result. Insufficient information was provided for the assessors to establish whether smaller bullion dealers implement AML/CTF measures commensurate with their activities and ML/TF risks. The characteristics of small bullion dealers are consistent with other small reporting entities – the understanding of obligations and compliance levels are expected to be lower than it is for the larger players.

5.27. *Other DNFBPs* (lawyers, accountants, real estate agents, trust and company service providers, dealers in precious stones) – These DNFBPs are not subject to AML/CTF requirements or supervision and, with limited exceptions, demonstrated a low understanding of their respective ML/TF risks.

<sup>1</sup> In October 2014, the Australian Remittance and Currency Providers Association Limited was established with 50 members from RNPs and independent remitters.

## PREVENTIVE MEASURES

5.28. Some sectors, such as the legal and accounting profession, are of the view that they are subject to stringent professional standards that are sufficient to manage any potential ML/TF risks and/or allow them to adequately know their customers. However, the sector representatives were unable to demonstrate to or convince the assessors how existing professional standards were sufficient to mitigate ML/TF risks over and above their personal business interests, or had enabled them to be an effective contributor in combating system-wide ML/TF risks. These sectors do not see themselves as having a gatekeeping role to prevent ML/TF, and felt this is the responsibility of the financial sector, on the basis that most funds are expected to flow through the financial system.

5.29. Other sectors like the business incorporators (i.e. trust and company service providers) reported having a fairly good understanding of their customers, given the nature and simplicity of the services that they provide.

5.30. On the whole, however, there is no conclusive evidence that these non-regulated DNFBPs are rejecting customers due to suspected ML/TF activities. They also do not have obligations to report suspicious matters to AUSTRAC, and do not do so in practice.

### *Requirements on CDD and PEPs*

5.31. **Financial institutions' and DNFBPs' existing measures on customer due diligence and identification of beneficial owners and PEPs are not in line with FATF Standards.** As mentioned above, the Rules Amendment commenced on 1 June 2014. The implementation period is outlined on the AUSTRAC website and is accompanied by policy principles issued by the Minister for Justice. The policy principles indicate that certain enforcement action – being an application for a civil penalty order or an injunction, the issuing of a remedial direction, or the imposition of a requirement to undertake an external compliance audit – will not be taken by the AUSTRAC CEO during the period of the policy principles for breaches of the additional CDD requirements, provided the reporting entities demonstrate that they have taken “reasonable steps” to comply by 1 January 2016. What constitutes “reasonable steps” is also set out in the policy principles and includes requiring reporting entities to have adopted a board approved transition plan to comply setting out how it will reach compliance with the new obligations. The transition plan was required to have been adopted by 1 November 2014. Also, where reporting entities are able to comply with the provisions through their existing operations, they must do so to demonstrate that they have taken reasonable steps. In addition, high-risk customers on-boarded by a reporting entity after 1 June 2014, but prior to the full implementation of the new obligations, are required to be retrospectively identified at the level required by the new obligations.

5.32. Based on interviews with reporting entities, assessors determined that at the time of the onsite a majority of reporting entities were not able to fully implement the requirements in the Rules Amendment; most continue to operate under the pre-June 1, 2014 requirements. While all the reporting entities endeavour to be in compliance as soon as possible, Australia-based reporting entities generally responded that they were unlikely to be able to comply with the new requirements ahead of 1 January 2016. Most sector representatives indicated that enforcement action would be taken against them if they took until that time to implement them. See also the preamble to Section 5 of the TC Annex. A number of international reporting entities noted that they were already implementing a number of the requirements based on their foreign obligations, and expected to be in compliance with the Rules relatively quickly.

5.33. The Rules Amendment expands on the CDD requirements with respect to the identification of the beneficial owner and the PEPs requirements, which are more in line with the FATF standard on Recommendations 10 and 12. However, even under the updated rules, several deficiencies remain as outlined in Recommendation 10.

### *Record Keeping*

5.34. **The larger reporting entities appear to have adequate record keeping measures in place, while some smaller entities have weaker record keeping procedures.** In demonstrating that reporting entities in general had effective record keeping measures in place, AUSTRAC provided information on a range of sectors. Of 68 on-site and off-site assessments conducted on major reporters since 2009, record-keeping deficiencies did not seem to be a key weakness across the major reporters. Only 16 requirements

were issued relating to record keeping requirements. The number of recommendations issued by AUSTRAC to reporting entities to remediate record-keeping requirements in 2013/14 is also relatively low compared to other obligations, such as identification procedures and reporting obligations. These suggest that the major reporters do not have major difficulties with meeting record keeping requirements. Private sector representatives reported anecdotal feedback on limited capacity of smaller players to cope with obligations in the AML/CTF Act in general. Law enforcement's experience was that, with the exception of many smaller remitters, most reporting entities kept fairly good records.

5.35. On average across all industry sectors, 90% of reporting entities that lodged compliance reports to AUSTRAC to report their compliance with AML/CTF obligations in 2012 reported that they retain records of all customer identification information. While this proportion has improved over time, this suggests that some reporting entities (most likely the smaller ones) may not be meeting basic record keeping obligations fully.

5

## Other Measures

### *Correspondent banking*

5.36. Financial institution representatives did not highlight any major challenges or difficulties in instituting measures for correspondent banking under the AML/CTF Act and AML/CTF Rules. AUSTRAC identified very few breaches of correspondent banking obligations in 2013/14. Based on AUSTRAC's understanding, financial institutions would adopt a risk-based approach to determine the extent of due diligence that is required with respect to correspondent banking. Interviews with the sector indicate that Australian rules on correspondent banking are being implemented. It should however be noted that the AML/CTF Act correspondent banking requirements are not in line with the FATF Standard; as a result the measures implemented by reporting entities may not meet the FATF standard, even if they meet Australia's requirements.

### *New technologies*

5.37. Sector representatives whom the assessors interviewed did not report particular difficulties in applying AML/CTF measures for new technologies. Before introducing a new designated service, delivery method or technology, larger reporting entities would typically conduct a product risk assessment that included ML/TF risk, and determine the controls needed to mitigate these risks.

### *Wire transfer rules*

5.38. Sector representatives indicated that the information accompanying cross-border wire transfers seems to comply with Australian requirements. However, the Australian requirements are not in line with the FATF Standard. In some cases, especially with respect to large, international financial institutions, the information accompanying a wire transfer exceeds the Australian requirements and may be in line with the FATF Standards. Representatives for banks and remitters were aware of the Australian requirements regarding the filing of international funds transfer instructions (IFTI) reports with AUSTRAC.

### *Targeted financial sanctions (TFS)*

5.39. As noted under IO.10, reporting entities were generally aware of their obligations with respect to the DFAT sanctions lists. Under section 41 of the *Charter of the United Nations (Dealing with Assets) Regulation 2008* using a process agreed to by DFAT, the AFP, the Australian Bankers' Association and major banks, reporting entities should contact AFP if there was a question about whether they had a match with the Consolidated List. Only a few reporting entities were aware that the AFP is the point of contact. However, it was universally reported by both the public and private sector that DFAT is responsible for enforcement of TFS and that reporting entities were not being monitored for compliance with TFS obligations.

5.40. AUSTRAC's role in relation to TFS is limited to its FIU activities – DFAT is a partner agency of AUSTRAC for these purposes. From a regulatory perspective, AUSTRAC would only have a role in monitoring the compliance with TFS obligations to the extent that an entity failed to lodge an SMR where it has formed a suspicion relevant to a breach of the laws related to TFS. In some limited instances during its regulatory

## PREVENTIVE MEASURES

engagements, AUSTRAC has identified possible breaches of sanctions during its compliance assessments. In two instances, reporting entities were involved in sending transactions to sanctioned Iranian banks. Warning letters were issued by AUSTRAC in relation to these matters. Of the two instances, one entity ceased trading and closed accounts, and the second entity ceased the relationship with the Iranian bank. No further action was taken (by AUSTRAC). AUSTRAC has also taken sanctions matters into account in determining registration decisions related to particular remitters.

### *Higher risk countries*

5.41. Larger reporting entities that employ risk models usually use multiple data sources to assess jurisdiction risks, to a large extent based on their experience with foreign regulators. Based on AUSTRAC's understanding, the FATF International Cooperation Review Group list of jurisdictions carries a significant weighting in such assessments. The outcomes of these risk assessments are used to guide their business and customer on-boarding decisions. Smaller entities with less sophisticated measures are likely to rely only on DFAT's list and guidance to identify higher risk countries.

### *Suspicious Transaction Reporting Obligations and Tipping Off*

5.42. **Reporting obligations are generally well understood by FIs and DNFBPs and they are filing SMRs.** As AUSTRAC is both the FIU and the AML/CTF regulator, reporting of SMRs and other reporting obligations such as IFTIs and TTRs (i.e. quality of the reporting) is often the focus of its engagement with financial institutions and DNFBPs. In this regard, the quality and volume appears to meet AUSTRAC's expectations. Overall, the assessors felt that reporting entities were effectively implementing the SMR requirements.

5.43. **On the other hand, the number of recommendations that AUSTRAC issued to reporting entities to remediate reporting obligations is the second highest among all obligations in 2013-14.** This may be a result of AUSTRAC's focus on reporting obligations and the IFTI obligation. Based on feedback gathered, the timeliness of SMR reporting varies according to reporting entities. It is also influenced by the complexity of the transactions and when a suspicion is formed. Some reporting entities, particularly the major financial institutions, will contact AUSTRAC and provide notice of an impending SMR that they consider a priority. Some financial institutions and remitters will reportedly contact law enforcement agencies before submitting an SMR to ensure that they are capturing and reporting adequate information. Private sector representatives also reported having good communication channels with AUSTRAC and other law enforcement agencies, and sharing of transaction details or records on an ad hoc basis to facilitate their investigations.

5.44. Universally, the private sector highlighted the need for information and more timely feedback from AUSTRAC and law enforcement agencies to improve their transaction monitoring systems for detecting ML and TF. Reporting entities specifically noted challenges in detecting TF in the absence of specific information, and putting in place effective measures to prevent them.

5.45. With respect to the quality of reporting, AUSTRAC considers that most medium to large reporting entities provide sufficient information and context for the SMRs submitted. Missing information usually relates to insufficient detail on the subject of the report, but does not appear to have significant adverse impact on the relevance or value of the SMRs. Overall, the reports received by AUSTRAC – including SMRs, TTRs and IFTIs – form a fundamental pillar of financial intelligence (see also IO.6).

5.46. Reporting entities are aware of the prohibitions against tipping off and have included the provisions in their internal policies, controls and trainings. A number of the large, international REs noted that the scope of the tipping off provisions have required them to have exemptions from the global AML/CTF programmes, as notifying the parent or home office of the institutions about SMRs would violate the provisions.

### *Internal AML/CTF Controls*

5.47. Reporting entities are aware of their requirement to have AML/CTF programmes – as outlined earlier under this IO – to ensure compliance with their obligations under the AML/CTF Act. They are also

aware of their obligation to submit compliance reports to AUSTRAC annually. REs reported having screening procedures when hiring new employees, ongoing training programmes and independent audit functions.

5.48. Reporting entities that are headquartered outside Australia and subject to AML/CTF regulation and supervision elsewhere generally reported having benefitted from comparing and contrasting guidance and requirements imposed by their home or other host jurisdictions, and adapting sound or best practices and applying them to their Australian operations. As a result, a number of these entities are implementing internal controls in line with FATF Standards, even when the Australian requirements do not meet the standard.

5.49. Reporting entities headquartered in Australia with cross-border operations include their overseas branches in their AML/CTF programmes. However, they reported that they have not extended their internal controls to their foreign subsidiaries, on the basis that they are separate legal entities from the Australian parent and because it is not a requirement under the Australian regulatory regime. It also appears that they have not adopted the more stringent of Australian or host jurisdiction rules in their group-wide AML/CTF framework on areas where host country requirements are stricter or more in line with FATF Standards.

5.50. Due to confidentiality provisions in Australia laws, reporting entities are not permitted to share their SMR information and details with their overseas operations unless they are branch operations. This relates to both Australian headquartered as well as foreign entities operating in Australia. Private sector representatives reported to the assessors that this restriction has impeded the efficiency and effectiveness of their group-wide AML/CTF controls. However, assessors noted that Australia's tipping off provision is in line with the FATF Standard. Authorities also note that reporting entities often share information with other parts of the REG about matters triggering alerts without sharing specific information that an SMR has been filed.

## Overall conclusions on Immediate Outcome 4

5.51. Australia exhibits some characteristics of an effective system for applying preventive measures in financial institutions and DNFBPs. In general, the major reporting entities and other high risk reporting entities subject to more regular supervisory engagement appear to have a reasonable understanding of ML/TF risks and preventive measures that comply with the Australian AML/CTF regime. Reporting entities have demonstrated that they are aware of their requirement to have AML/CTF programmes and reported having implemented the necessary internal AML/CTF controls. However, a number of aspects of the AML/CTF regime – including those that relate to internal controls, wire transfers, correspondent banking, etc. – do not meet FATF Standards. As a result, reporting entities' implementation of AML/CTF measures will not meet the FATF Standards if its internal controls are developed solely to meet the Australian requirements. In addition, while the requirements have been revised with respect to CDD and PEPs, none of the reporting entities reported they were able to fully implement these requirements at the time of the onsite. As a result, at the time of the onsite visit, reporting entities were working to transition from the pre-June 1 AML/CTF Rules, which were not in line with the FATF Standards. At the same time, a lot of reliance is placed on the banking and financial sector as gatekeepers due to the absence of AML/CTF regulation and requirement on key high-risk DNFBPs such as lawyers, accountants, real estate agents and trust and company service providers. As a result of these factors, the effectiveness of the preventive measures in the financial system as a whole and DNFBPs is called into question to some extent.

5.52. **The overall rating is therefore a moderate level of effectiveness for Immediate Outcome 4.**

## 5.4 Recommendations on Preventive Measures

5.53. The following recommendations are made on preventive measures (IO.4):

- Ensure that lawyers, accountants, real estate agents, precious stones dealers, and trust and company service providers understand their ML/TF risks, and implement effective AML/CTF obligations and risk mitigating measures in line with the FATF Standards. Among others, persons and entities in these sectors should be able to demonstrate that they are effectively refusing businesses on ML/TF grounds or when CDD is incomplete, in addition to their own business or reputation considerations.

## PREVENTIVE MEASURES

In addition, they should be required to report suspected proceeds of crime and funds in support of terrorism to competent authorities in a swift manner. Last but not least, the effectiveness of the controls and measures that they put in place should be subject to sufficient monitoring and supervision to ensure compliance.

- Ensure that reporting entities implement preventive measures in line with the FATF Standards.
- Ensure that reporting entities implement as early as possible before 1 January 2016 the obligations on enhanced CDD, beneficial owner, and politically exposed persons introduced on 1 June 2014.
- Monitor and ensure that reporting entities headquartered in Australia with cross-border operations to ensure that their overseas branches and subsidiaries have effective AML/CTF programs and risk mitigation measures in place as required under the AML/CTF Act.
- Improve the feedback and guidance to reporting entities on reporting quality and volumes of SMRs and reinforce this feedback loop into their ML/TF risk identification and the effectiveness of their AML/CTF programmes.

## 6. SUPERVISION

### Key Findings

Licensing, registration and other controls implemented by Australia to a large extent adequately prevent criminals and their associates from entering the financial sector. However, there are some questions about the effectiveness of these measures for remitters.

AUSTRAC has an insufficient understanding of the ML/TF risks of the individual reporting entities within reporting entity groups, which raises questions on the adequacy of how it selects individual reporting entities for compliance assessments.

**AUSTRAC is good at promoting compliance, but does not focus sufficiently on effective supervision and enforcement of individual reporting entities' compliance with AML/CTF obligations within the various sectors.** AUSTRAC allocates its limited supervisory resources to the reporting groups and/or entities it considers higher risk.

**The majority of deficiencies identified by AUSTRAC through its compliance activities are voluntarily remediated by reporting entities based on recommendations and requirements issued by AUSTRAC after an assessment. AUSTRAC does not take sufficient enforcement action to ensure compliance by industry.**

**AUSTRAC does not supervise subsidiaries of Australian reporting entities located abroad nor maintain relationships with supervisory authorities where those subsidiaries operate, besides New Zealand.**

## 6.1 Background and Context

6.1. Financial institutions are required to be licensed or registered with the APRA and/or the Australian Securities and Investment Commission (ASIC). Casinos are licensed through State or Territory legislation and are supervised by the relevant State or Territory casino control authorities or gaming departments. Pubs and clubs are licensed at the State and Territory level. Remittance service providers, currency exchange businesses (*bureaux de change*), licenced gaming operators and bullion dealers are required to register (enrol) with AUSTRAC. Other DNFBPs, like lawyers, precious stones dealers, real estate agents, accountants and trust and company service providers are not subject to AML/CTF requirements and are therefore not regulated or supervised for AML/CTF purposes.

6.2. AUSTRAC is responsible for monitoring the AML/CTF compliance of financial institutions and those DNFBPs that provide a 'designated service' under the AML/CTF Act. All providers of a designated service must enrol with AUSTRAC, and be entered on the Reporting Entities Role. This requirement provides AUSTRAC with visibility over the scope of the regulated population and assists AUSTRAC in exercising its supervisory function. The Compliance Branch of AUSTRAC is responsible for supervision. There are approximately 40 employees directly contributing to supervision in the branch. AUSTRAC has 13 657 reporting entities under supervision. Staff are located in AUSTRAC's offices in Sydney, Melbourne and Brisbane. While the Brisbane office is about to be closed, the positions in this office have been maintained and moved to other offices.

## 6.2 Technical Compliance (R.26-28, R.34, R.35)

6.3. See for the full narrative the technical compliance annex:

- **Recommendation 26 (regulation and supervision of financial institutions) is rated partially compliant.**
- **Recommendation 27 (powers of supervisors) is rated partially compliant.**
- **Recommendation 28 (regulation and supervision of DNFBPs) is rated non-compliant.**
- **Recommendation 34 (guidance and feedback) is rated largely compliant.**
- **Recommendation 35 (sanctions) is rated partially compliant.**

## 6.3 Effectiveness: Immediate Outcome 3 (Supervision)

### *Licensing, registration and enrolment*

6.4. Licensing, registration and other controls implemented by Australia to a large extent adequately prevent criminals and their associates from entering the financial sector. However, there are some questions about the effectiveness of these measures for remitters. Australia has a system of self-certification for fitness and propriety by financial institutions. This process may not be in line with the standards. Regarding their respective regulated financial sectors, APRA and ASIC perform a certain level of supervision of the adequacy of the assessment by the financial institutions of the fitness and propriety of all 'responsible persons' or 'responsible managers'. Full background verifications are conducted on owners and controllers before issuing a licence. This assessment must be done prior to initial appointment and afterwards repeated on an annual basis. ASIC conducts probity checks with its overseas counterparts whereas the prudential regulator APRA does not have a direct role in such checks. APRA seeks comments and information on a basis of need where it is relevant rather than as a matter of course. Both APRA and ASIC are designated agencies under the AML/CTF Act and can directly access AUSTRAC's systems for information

relevant to their supervisory and enforcement responsibilities. APRA and ASIC also engage with AUSTRAC Compliance Branch on matters of mutual interest.

6.5. AUSTRAC's approval process for registering as a RNP, affiliate or agent, or independent remittance dealer, provides AUSTRAC with the capacity to remove entities that pose an unacceptable risk of ML or TF from the system. AUSTRAC does not systematically sample criminal records checks at the time of registration. Applicants provide AUSTRAC with information relevant to the suitability of 'key personnel' such as criminal history and beneficial owner arrangements. Typically, AUSTRAC only reviews whether the criminal history check has been performed when an entity is known to be of concern to partner agencies. AUSTRAC may also conduct sample testing of criminal history checks performed by the remitter during examination. In addition, from time to time, AUSTRAC compares the key personnel of remitters on its register against criminal targeting lists of its partner agencies. An increasing number of actions have been undertaken by AUSTRAC including giving an infringement notice to a large multi-national remittance provider for providing services to unregistered affiliates. Given that remitters are considered to present high ML/TF risks, this process could be enhanced through more systematic validation of criminal history and beneficial owner arrangements.

6.6. Licensing and due diligence checks on casino operators, key persons, and employees are governed and performed by State and Territory laws and regulators. The two major casinos are in New South Wales and Victoria. The Independent Liquor and Gaming Authority (ILGA), the casino regulator in New South Wales, conducts extensive due diligence to assess the suitability of the applicant and their associates to own and run a casino. These checks are also performed once every five years during the licence renewal process. The ILGA conducts police checks on many key personnel who work in casinos as required under the *Casino Control Act 1992*. In Victoria, similar periodic licence renewal due diligence is performed by the state casino regulator. The assessors understand that not all States and Territories have similarly strict laws for licensing, regular licence renewals and probity checks. This is a concern given the ML risk profile of casinos and the involvement of some in high profile ML cases.

### *Risk identification*

6.7. AUSTRAC regulates entities at a group level as DBGs or REGs. Those reporting entities that are owned and controlled by a parent reporting entity within normal corporate group structures form a REG, e.g. one major bank has over 120 individual REs within its corporate structure. This includes every subsidiary in the group. As previously noted, the four largest banks in Australia are domestic and they dominate the financial sector; therefore they have been identified to be of high ML/TF risk and impact. In addition, given their heightened risk, remitters are also considered to be of greater materiality than other aspects of the financial sector. Under its risk-based approach<sup>1</sup> AUSTRAC identifies and maintains an understanding of the ML and TF risks of these REGs and the individual reporting entities stemming from the results of the NTA regarding ML/TF channels and risks, compliance assessment outcomes; engagement with peak industry associations and bodies; specific interest by and engagement with partner agencies; analysis of reported transactions; and strategic research and analysis of different crime types, including methods and vulnerabilities.

6.8. AUSTRAC focuses on those corporate groups in sectors identified in the NTA as having a higher exposure and vulnerability to ML/TF. As mentioned before, these sectors are: domestic banks, foreign and investment banks, cash in transit operators (armoured car and cash delivery services), remitters, currency exchange businesses (bureaux de change) and casinos. While the authorities recognize the need to update the NTA, these sectors continue to remain particularly vulnerable. More recently, AUSTRAC has used information from its internal intelligence function and from partner agencies to focus to a large extent on the remittance sector, identified as high risk based on recent high profile examples of criminal exploitation and infiltration of the sector.

6.9. Important factors in identifying ML/TF risk at the REG and reporting entity level are volume and value of transaction reports (SMRs and IFTIs) as an indicator of the volume of funds flowing through an entity, and the size of an entity as a proxy measure of the number and type of customers, products, distribution

1 Based on AUSTRAC's *Compliance & Enforcement Tactical Plan 2013-2014*.

channels and geographic reach. However, it has not been made sufficiently clear that AUSTRAC, when risk profiling REGs or individual reporting entities, collects and uses sufficient information necessary to adequately determine the level of inherent risk of the REG and individual reporting entities, beyond the information from transaction reports. International standards on the risk-based approach require, for example, an insight into the level of inherent risk of entities under supervision, including the nature and complexity of products and services, business model, financial and accounting information, delivering channels, customer profiles, geographic location, countries of operation, etc. The assessors were of the view that AUSTRAC's approach was not sufficiently nuanced to account for variance and risk between the reporting entities within a single REG and within and between sectors.

6.10. After selecting a REG and/or reporting entity for review, when AUSTRAC is planning for (on-site) assessments, it does take into account the detailed characteristics of the REG and/or reporting entity under review. AUSTRAC also has regard to its considerable data holdings and any information held by the FIU to inform the scope of the assessment. At this stage AUSTRAC requests and receives documentation from the entity or group of entities for detailed consideration prior to the review. Where particular issues are identified through a review of these materials, the scope of the assessment may be changed or expanded. Where customer identification records are to be sampled as part of the assessment, AUSTRAC focusses on assessing higher risk customer types as part of the assessment.

**Table 6.1. Reporting entities in high-risk corporate groups**

Alternative remittance dealers (including affiliates)	4 960
Betting agencies	4
Bookmakers	4
Cash in transit operators	6
Casinos	12
Credit unions & building societies	3
Custodians	93
Domestic banks	44
Financial services intermediaries	58
Foreign & investment banks	54
Foreign exchange providers	15
Insurance product issuers	19
Non-AML regulated entities	6
Non-bank lenders & financiers	229
Non-bank wealth creation groups	3
Provider of purchased payment facilities	1
Precious metal trader	1
Pubs & clubs	38
Stock brokers	106
Superannuation fund trustees	45
Trustees of managed investment schemes	123
<b>Grand Total</b>	<b>5 837</b>

6.11. In 2013/14, AUSTRAC identified 230 high risk REGs, representing 5 837 Res or 43% of the total population of 13 657 reporting entities in Australia – including all affiliates of registered remittance network

providers. There are high-risk REGs in low-risk sectors because of relative risk factors. An incident relating to ML/TF may result in a reporting entity or REG that is not currently in the high-risk category for supervisory engagement being elevated into the high-risk group where, for example, an entity is identified by law enforcement. While REs from low-risk sectors that are large in comparison to their specific industry peers targeted for engagement by AUSTRAC, smaller reporting entities from these sectors which pose a higher ML/TF risk due to other factors (like high-risk activities, geographical presence, concentration of high-risk clients, risks resulting from company culture and behaviour etc.) may see limited direct compliance engagement.

6.12. After determining ML/TF risk, AUSTRAC determines the level and type of engagement with a REG based on its compliance risk. This is based on the knowledge that most corporate groups have a centralised AML/CTF compliance function. Compliance risk is defined as the risk that an REG is non-compliant with its obligations under the AML/CTF Act. It is used to determine the level and type of engagement with an REG.

6.13. At the time of the on-site AUSTRAC advised the assessors that it had developed, but not implemented, a **comprehensive tool to identify and track compliance risk as the residual risk<sup>2</sup>**. A compliance risk score sheet was being used that produces an indicator of compliance (which is the score) of the reporting entity or REG, based on a self-assessment by each reporting entity or REG's compliance officer. Previous direct compliance engagements, information from the enrolment / remitter registration processes, and behaviour monitoring relative to industry peers are taken into account in determining compliance risk at the REG level. In addition, AUSTRAC has developed data mining techniques that scan its reporting database to identify reporting entities that display outlier behaviours compared to their industry peers. For example, this can be in the form of material change in reporting patterns or unusual reporting patterns.

6.14. To a certain extent, further threats and vulnerabilities are also considered through campaign-based activities, which are based largely on reports filed with AUSTRAC. Occasionally, campaign-based work can involve follow up on information received from partner agencies and/or through the media. Examples provided include the remittance sector, which is a known high risk sector, and the gaming sector.

### *Mitigating risks through supervision or monitoring compliance*

6.15. With a view to mitigating the risks, AUSTRAC and other Australian regulators adopt a graduated approach to supervision. In AUSTRAC's case this extends from low intensity (media articles, guidance, forums and presentations); through to moderate intensity (behavioural reviews, letter campaigns, desk reviews) and high intensity (onsite inspection, enforcement consideration, remedial direction, enforceable undertakings and civil penalties). This wide range of measures should allow AUSTRAC to implement tailored responses depending on the type of reporting entities and their inherent factors, such as their relative importance, their size, and the ML/TF risk they face, etc. In addition, AUSTRAC's supervisory approach has been modified over time to take into account the stage of development of the Australian AML/CTF regime. Immediately after the implementation of AML/CTF regulation in Australia, AUSTRAC was primarily focused on engaging large proportions of the reporting population to educate them on their obligations and nurturing a compliance attitude following the implementation of the AML/CTF Act. Over time, this has developed into a more detailed assessment of reporting entities' compliance with the substantive obligations of the AML/CTF Act. From July 2007 to June 2010 AUSTRAC undertook a combined total of 944 onsite inspections and desk reviews. As a result, over 3 362 requirements have been issued to reporting entities to remedy breaches of AML/CTF obligations and 2 149 recommendations to improve systems, processes and practices. From July 2010 to June 2014, AUSTRAC has since continued to escalate monitoring activities and, through campaigns aimed at different sectors, has issued a further 3 163 remediation requirements for breaches of obligations and 1 605 recommendations to seek best practices from 1 152 on-site inspections and desk reviews. **AUSTRAC succeeds to a fair extent in promoting compliance with the AML/CTF requirements among the sectors it has engaged.**

6.16. **The focus of supervision is targeting high risk entities for enhanced supervisory activity and to test the effectiveness of REGs / reporting entities' systems and controls in practice.** AUSTRAC focuses

2 As of the face-to-face meeting, the tool had been fully implemented.

## SUPERVISION

its supervisory resources on the 230 high risk REGs and reporting entities within these groups are subject to periodic on-site reviews under AUSTRAC's risk-based supervision approach. Transactions through high-risk REGs represent over 99% of the reported monetary value flowing in and out of Australia. A combined total of 317 reviews (59 on-site assessments or 258 desk reviews) to verify reporting entities' AML/CTF effectiveness were conducted by AUSTRAC in 2012-13, of which fewer than 20% (in total 60; 32 on-site and 28 desk) were high-risk REGs / reporting entities. In 2013-14, the total number of reviews decreased to 165 reviews (62 on-site inspections and 103 desk-reviews) – but 99% were in high risk REGs/ reporting entities - following a shift in AUSTRAC's compliance approach to better calibrate ML risks. Between 2010 and 2014, 118 on-site inspections were conducted in high-risk groups as well as 163 desk-reviews. These numbers include thematic assessments. AUSTRAC periodically reviews multiple REGs against a particular AML/CTF obligation, for example, KYC, ongoing CDD and enhanced CDD. AUSTRAC may commence a thematic assessment based on the results of any compliance activity with a view to identifying and remedying any systemic breach of the AML/CTF Act or Rules.

6

6.17. As shown in the table below (*Detailed Supervisory actions and outcomes for 2012-14*), 34 assessments have been performed in 2012/2013 on the banking sector, aimed at 12 groups, consisting of 303 individual REs and a further 20 individual reporting entities outside of a DBG. AUSTRAC considers that it assessed compliance in all 303 reporting entities on the basis of 15 onsite audits and 19 desk reviews. AUSTRAC's Standard Operating Procedures relating to the assessment of reporting entities' AML/CTF program require supervisors to, in respect of each designated service, identify the risk reasonably faced by the reporting entity that provision of the service might (inadvertently or otherwise) involve or facilitate ML or TF (ML/TF risk) by reference to customer types, the type of designated service that is being provided, the methods by which the designated service is being delivered, and the foreign jurisdictions being dealt with. If the reporting entity forms part of a DBG, the supervisors should separately identify the ML/TF risk reasonably faced by each reporting entity in the group by reference to the designated services that each provides. Assessors question whether the way such assessment work is being done is sufficiently robust to assess compliance by the 303 individual reporting entities.

6.18. AUSTRAC is clearly able to assess the effectiveness of mitigation for those individual reporting entities of the group directly engaged during the assessment. However, assessors are not convinced that AUSTRAC holds sufficient information about the ML/TF risk profile of all reporting entities within REGs to be able to design each REG's assessment work-plan such that the targeting and sampling used produces reliable results about compliance across the group. The assessors also consider that AUSTRAC's recent focus on assessing compliance by remitters means that the number of banks targeted for the assessments is too low relative to that sector's risk profile. **This makes it insufficiently clear for the assessment team to conclude that AUSTRAC's supervisory response is adequately adapted to the ML/TF risks.** During the interviews with the private sector, representatives from the sector mentioned several times that they were under the impression that assessments undertaken since 2010 are still aimed primarily at assisting AUSTRAC in understanding the activities, entities, and REGs.

**Table 6.2. AUSTRAC AML/CTF compliance assessments of entities in High-Risk Groups between 2010-11 and 2014-15**

On-site inspections – High-risk Groups / High-risk entities	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Hotels or clubs (gaming)		2	4	17		23
Domestic banks	5	5	6	6		22
Foreign and investment banks	2	1	6	9	1	19
Remittance service providers	3		6	4	1	14
Currency exchange dealers	1	3		5		9
Casinos		2	3	3		8

**Table 6.2. AUSTRAC AML/CTF compliance assessments of entities in High-Risk Groups between 2010-11 and 2014-15 (continued)**

On-site inspections - High-risk Groups / High-risk entities	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Stockbrokers			2	4		6
Corporate bookmakers			1	4		5
Specialist credit providers		1	2	1		4
Bookmakers				2		2
Funds managers				2		2
Bullion dealers				1		1
Superannuation funds				1		1
Cash in transit operators				1		1
Precious metal traders			1			1
Insurers				1		1
Credit unions / building societies			1			1
<b>Grand total</b>	<b>11</b>	<b>14</b>	<b>32</b>	<b>61</b>	<b>2</b>	<b>118</b>
Desk reviews – High-risk Groups / High-risk entities	2010-11	2011-12	2012-13	2013-14	2014-15	Total
Foreign and investment banks		5	8	12		25
Specialist credit providers	1		3	16	1	21
Domestic banks		11	5	3	1	20
Funds managers		2	4	11		17
Financial planners		1		13		14
Stockbrokers		2	1	10		13
Hotels or clubs (gaming)			1	12		13
Superannuation funds		3	1	7		11
Credit unions / building societies	1	4		2		7
Currency exchange dealers			2	3		5
Remittance service providers			1	4		5
Custodians				5		5
Cash in transit operators		3	1			4
Small bookmakers				2		2
Insurers			1		1	2
Casinos					1	1
Bullion dealers				1		1
Precious metal traders				1		1
<b>Grand total</b>	<b>2</b>	<b>31</b>	<b>28</b>	<b>102</b>	<b>4</b>	<b>163</b>

**Table 6.3. Detailed Supervisory actions and outcomes for 2012-14**

Year	Industry sector	N° of Assessments	Breakdown of reporting entities assessed			
			N° of DBGs (entities within DBG)	N° of individual entities	Desk review	Onsite audit
2012-13	Banks	34	12 (303)	20	19	15
	Gambling	194	3 (17)	191	176	18
	Remitters	13	0	13	2	11
	NBFS	76	10 (42)	66	61	15
<b>TOTALS</b>		<b>317</b>	<b>25 (632)</b>	<b>290</b>	<b>258</b>	<b>59</b>
2013-14	Banks	32	14 (159)	17	17	15
	Gambling	41	8 (47)	48	15	26
	Remitters	8	1 (3)	2	4	4
	NBFS	87	19 (88)	55	70	17
<b>TOTALS</b>		<b>168</b>	<b>42 (297)</b>	<b>122</b>	<b>106</b>	<b>62</b>

*NBFS: Non-bank financial services (securities, life insurance, etc.)*

6.19. AUSTRAC uses the annual compliance reports (ACR) tool, which reporting entities are required to submit under the AML/CTF Act, as an important tool for providing information on potential compliance or implementation issues and thematic assessments. It is comprised of an online questionnaire with fixed choice responses across 22 key question areas. Following the results of this exercise, further thematic analysis may be conducted in relation to the entities to assess the need for further escalation. AUSTRAC identified several problems regarding the current ACR; the usefulness has decreased over time as the ACR was designed in a time when AUSTRAC was more focused on implementing AML/CTF programs rather than ML/TF risk and ongoing compliance. As a result, the ACR now provide limited visibility over the maturity and effectiveness of reporting entities' AML/CTF programs. AUSTRAC is in the process of reviewing the format of the reports.

6.20. The duration of the overall reporting entity's on-site assessment process (from pre on-site preparation to post on-site follow-up) lasts from several weeks to several months. The actual on-site components are short (in general 1-2 days at most for nearly all financial institutions, which follows a much longer off-site preparation). In line with the risk-based approach, medium and low risk reporting entities are not part of the aforementioned cycle, but can be involved in assessments through campaign based work (for example, the clubs and pubs in 2013-14 and through ACRs based on self-assessment disclosure) or can be targeted for an assessment based on other factors.

6.21. As noted under IO.10, there is no systematic monitoring of compliance with the international and autonomous sanctions regimes. During its reviews, AUSTRAC periodically uncovers issues of non-compliance, and primarily refer the matters to DFAT which has responsibility for the sanctions regimes.

### *Remedial actions and sanctions*

6.22. AUSTRAC's enforcement strategy is based on its *Compliance & Enforcement Tactical Plan 2013-14* and focusses on 'fixing the problem' before sanctioning. **In most cases, deficiencies identified by AUSTRAC through its compliance activities are remediated by reporting entities according to the recommendations and requirements issued by AUSTRAC after an assessment.**

6.23. **When AUSTRAC determines that it is necessary to use its formal enforcement powers under the AML/CTF Act,** the sanctioning instrument used most often is the Enforceable Undertaking (EU). An EU is a written undertaking that is enforceable in a court and is used where there has been a contravention of the

AML/CTF Act, the regulations or the AML/CTF Rules. The EU is mutually agreed by the reporting entity and the AUSTRAC CEO. The AUSTRAC CEO may accept an undertaking that a person will comply with the AML/CTF requirements, take specified action, refrain from taking specified action, and/or take specified action towards not contravening, or being likely to contravene the requirements in the future. Copies of each EU are published on AUSTRAC's website.

**6.24. AUSTRAC issues around five enforcement actions each year which is assessed as low compared to the total number of reporting entities and not commensurate with the severity of findings and control deficiencies that it found in the reporting entities through its supervisory processes.** EUs have been used 14 times since 2008. Eleven cases were based on AUSTRAC's own compliance assessment, one on a voluntary breach reporting, one on referral from APRA, and one on referral from AUSTRAC's intelligence function. Sectors involved were the banking sector (two EUs), remitters (five EUs) and hotels with gaming activities (seven within one REG). AUSTRAC has only applied financial sanctions in one case, related to the failure of a remittance provider to register its affiliates. No financial sanctions have ever been applied for non-compliance with AML/CTF obligations relating to preventive measures. The number of enforcement actions and the subjects of these actions do not convincingly demonstrate that reporting entities are subject to effective and proportionate sanctions. Reporting entities met by the team confirmed the absence of a deterrent effect of measures taken by AUSTRAC. Remediation work for large entities is dissuasive to the concerned reporting entity (considering the volume and cost of remediation work, as remediation actions are reviewed by external third parties, such as consultancy firms). Remediation actions are not made public by AUSTRAC.

**Table 6.4. Summary of AUSTRAC enforcement actions from 2008-09 - 2013-14**

Enforcement action	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14
Infringement notices (section 184)	-	-	-	-	-	1
Enforceable undertakings (section 197)	1	3	7 (one RE Group)	1	1	1
Remedial direction (section 191)	-	1	1	1	-	-
Notices to appoint an authorised external auditor (section 162)	-	7 (one RE Group)	-	1	-	-
<b>Total</b>	<b>1</b>	<b>11</b>	<b>8</b>	<b>3</b>	<b>1</b>	<b>2</b>

**6.25.** Within the remittance sector, AUSTRAC has refused, cancelled, suspended or placed conditions on the registration of a number of remitters as a means of reducing the ML/TF risk posed by the sector. The AUSTRAC CEO has refused the registration of 7 applicants; imposed conditions on 17 registrations; suspended the registration of 2 persons; and cancelled the registration of 8 persons. In addition, as a result of AUSTRAC's enquiries, 9 persons have voluntarily removed themselves from the register and 5 persons have withdrawn their applications to be registered.

#### *Demonstrating effect on compliance*

**6.26. AUSTRAC was unable to convince assessors that its supervisory activities had a demonstrable effect on compliance by individual reporting entities that were not subject to onsite or offsite engagement.** While AUSTRAC's outreach activities promote an awareness of AML/CTF obligations, assessors were not satisfied that its approach to on- and off-site supervision and enforcement action had a demonstrable effect on compliance by reporting entities. This was particularly notable among REs that AUSTRAC had limited direct engagement with or had not inspected. Since the compliance risk tool (as a tracking mechanism) was not yet implemented at the time of the onsite, AUSTRAC has advised the team that it **does not have full insight into the effect of its supervisory activities on compliance by sectors, reporting entities or REGs**. At this stage, effectiveness can be shown based on the results of EUs; the cover ratio regarding reviews of high risk groups (approximately 40% per year); the outcome of ACRs (self-assessment disclosure) regarding individual REGs and/or individual reporting entities; and the volume of SMR reports and other types of reporting provided by the REGs to AUSTRAC. The ACRs through self-disclosure are however – as mentioned

before - past their expiry date and AUSTRAC is reviewing their use and content with the aim of gaining a better insight in risk identification and classification by reporting entities. The assessors were of the view that the majority of these metrics on the adequacy of reporting entities' controls and AML/CTF compliance are based on attestations from the reporting entities, with insufficient work done to independently verify these assertions.

### *Promoting a clear understanding of AML/CTF obligations and ML/TF risks*

6.27. Promoting awareness of AML/CTF obligations is a key priority for AUSTRAC. This is reflected by the fact that one of the statutory functions of the AUSTRAC CEO is 'to advise and assist the reporting entities in relation to their obligations under this Act, the AML/CTF Rules and regulations'. **In its function as regulator and supervisor, AUSTRAC engages with the sector through consultation and explanation of the AML/CTF obligations through several mechanisms**, including through the development and dissemination of information and guidance materials (including e-learning), regular industry forums and consultation processes, and the AUSTRAC Help Desk. The main guidance issued is the AUSTRAC Compliance Guide. **Remittance businesses have been provided with broad information on AML/CTF obligations, including registration requirements. Their application in practice seems however to be challenging**, especially as it relates to smaller, unaffiliated remitters. This challenge is not unique to Australia.

6.28. **Materials and other information on ML/TF risks are limited and somewhat outdated.** The private sector indicated that there's a need for AUSTRAC to further develop its understanding of ML/TF risks regarding several sectors (including the banking sector) and regarding activities of individual reporting entities in order to better promote a clear understanding of ML/TF risks, not only of AML/CTF obligations. Reporting entities unanimously desire to obtain more feedback on reported SMRs to guide them in their further work in identifying relevant ML/TF risks in Australia, and stated that the feedback provided was too general and outdated to be useful.

6.29. At the time of the onsite, reporting entities had mixed views about the usefulness of AUSTRAC's guidance. While many found it helpful, they expressed reservations about its complexity and timeliness of its updates. AUSTRAC addressed these issues shortly after the onsite by redesigning its website and issuing the Compliance Guide which provides comprehensive guidance on reporting entities' AML/CTF obligations.

### **Overall conclusion on Immediate Outcome 3**

6.30. AUSTRAC relies heavily on varying forms of reporting (i.e. SMRs and IFTIs) and unverified self-reporting of compliance to determine reporting entity risks; other risk factors should be considered and AUSTRAC supervisory practice should extend to more individual reporting entities. AUSTRAC's approach does not seem sufficiently nuanced to adequately account for the risks of individual reporting entities in a REG. More generally, AUSTRAC's graduated approach to supervision does not seem to be adequate to ensure compliance. No monetary penalties for violations of the AML/CTF preventive measure obligations have ever been pronounced. Rather, AUSTRAC had applied sanctions to a limited extent in the form of enforceable undertaking, which amounts to – among other things – a formal agreement that the reporting entities will comply with AML/CTF requirements. The assessors concluded that the use of sanctions for non-compliance has had minimal impact on ensuring compliance among reporting entities not directly affected by the sanction. The private sector shared similar views about the depth, breadth, and effectiveness of the supervisory regime. In addition, there is no appropriate supervision or regulation of most higher-risk DNFBPs because they are not subject to AML/CTF requirements. Overall, the authorities were unable to demonstrate improving AML/CTF compliance by REs or that they are successfully discouraging criminal abuse of the financial and DNFBP sectors.

6.31. **The overall rating is therefore a moderate level of effectiveness for Immediate Outcome 3.**

## 6.4 Recommendations on Supervision

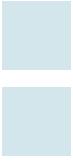
6.32. The following recommendations are made to Australia on supervision (I0.3):

- Keep the inherent risk picture of domestic markets and sector(s) up to date.
- Incorporate more (inherent) risk factors besides data analysis from filed reports into identifying and assessing the risk of reporting entities.
- Focus more on the assessment of the effectiveness of the application of the controls at the individual reporting entity level, instead of on the assessment of the design of (parts of) the AML/CTF programmes on a group level.
- Australia should take comprehensive measures to ensure financial institutions are actively supervised for implementation of DFAT lists. As the AML/CTF regulator, this supervision may appropriately align with responsibilities of AUSTRAC, although additional compliance staff would be required. DFAT and AUSTRAC should work closely together in promoting compliance with sanctions regimes (both obligations and risks).
- AUSTRAC should consider opportunities to further utilise its formal enforcement powers to promote further compliance by reporting entities through judicious use of its enforcing authority. Australia should make the corresponding changes to its legal framework for AUSTRAC, where necessary, to enable this. In relation to remitters, the regulatory oversight of self-certification should be reinforced or enhanced.
- Enhance the utility and timeliness of feedback provided to reporting entities on the SMR reporting to enable them to better understand the real ML/TF risks of their activities;
- AUSTRAC's supervision should extend to subsidiaries of Australian reporting entities located abroad and establish supervisor relationships with the supervisory authorities in the countries where these entities operate.
- Extend the supervision of the DNFBPs for AML/CTF compliance beyond casinos and bullion dealers to include services offered by other DNFBPs – real estate agents, other precious metals and stones dealers, lawyers, notaries, other independent legal professionals and accountants, and trust and company service providers.

## SUPERVISION



6



## 7. LEGAL PERSONS AND ARRANGEMENTS

7

### Key Findings

**Australia has not conducted a formal risk assessment on TF risks associated with legal persons and arrangements.** The majority of legal persons are registered with ASIC (federal) while others with State or Territory authorities. While the information seems to be largely available to competent authorities and to the public, very limited verification is conducted on the registration information. **Hence, there is no certainty that information maintained on legal persons is accurate or up-to-date.** The same conclusion applies to the Australian Business Register maintained by the ATO.

**In most cases, registration is carried out by a third party (i.e. lawyers, accountants or trust and company service providers) not subject to AML/CTF obligations.**

**Trustees are not required to maintain adequate, accurate and current information on the settlor, trustee, protector, beneficiaries, etc. of a trust.** Nor are they explicitly required to disclose their status.

**Information on the beneficial owner of legal persons and legal arrangements is not maintained and accessible to competent authorities in a timely manner.**

**Some information on shareholders is available** (on first rank shareholders only, but does not extend to the beneficial owner as defined by the FATF), which may themselves be other legal persons. Public company share registries are required to collect information on whether shares are held beneficially or not. Information on proprietary companies is collected through the Australian Business Register. Law enforcement agencies advised that access to companies' registers was not timely due to obstacles posed by lawyers.

**Some measures have been taken to mitigate the risks posed by nominee shareholders and directors but they are insufficient to address other risks.**

## 7.1 Background and Context

### (a) Overview of legal persons

7.1. The types of legal persons that can be established or created in Australia are: proprietary companies; public non-listed companies; public listed companies; incorporated and limited partnerships; incorporated associations; and cooperatives.

7.2. Australia reports that in 2012-13 there were more than 2 million registrations with ASIC, including 1 990 551 proprietary companies; 21 690 public companies; and 3 324 foreign companies. Incorporated and limited partnerships, incorporated associations and cooperatives are registered at State or Territory level. The number of registrations by jurisdiction are listed below.

**Table 7.1. Number of legal person registrations by jurisdiction**

State / Territory	Incorporated Associations – New	Incorporated Associations – Total	Registered Cooperatives – New	Registered Cooperatives - Total	Limited Partnerships – New	Limited Partnerships – Total
New South Wales	Data not available	<b>36 037</b> (as at 30 June 2013)	121 (as at 30 June 2013)	<b>617</b> (as at 30 June 2013)	Data not available	Data not available
Victoria	<b>1 695</b> (2013-14)	<b>39 883</b> (2013-14)	Data not available	Data not available	<b>29</b> (2013-14)	<b>271</b> (2013-14)
Queensland	<b>1 081</b> (2012-13)	<b>23 631</b> (as at 30 June 2013)	<b>4</b> (2012-13)	<b>182</b> (as at 30 June 2013)	Data not available	Data not available
Australian Capital Territory	<b>93</b> (2013-14)	Data not available	Data not available	Data not available	Data not available	Data not available
Tasmania	<b>165</b> (2012-13)	<b>3 591</b> (as at 30 June 2013)	Data not available	<b>27</b> (as at 30 June 2013)	Data not available	<b>122</b> (as at 30 June 2013)
South Australia	<b>380</b> (2012-13)	<b>19 770</b> (as at 30 June 2013)	<b>0</b> (2012-13)	<b>56</b> (as at 30 June 2013)	Data not available	Data not available
Northern Territory	<b>20</b> (2012-13; includes unincorporated associations)	<b>535</b> (2012-13; includes unincorporated associations)	Data not available	Data not available	Data not available	Data not available
Western Australia	Data not available	Data not available	Data not available	Data not available	Data not available	Data not available

7.3. The New South Wales (NSW) Department of Fair Trading registers incorporated and limited partnerships, incorporated associations and cooperatives. There are approximately 36 037 associations; 149 limited partnerships, 121 incorporated partnerships and 617 cooperatives registered in NSW. Some information on the number of entities registered in other States and Territories was also provided. NSW is expected to have the largest number of entities registered in each category of legal persons registered

7.4. As described below and in the TC Annex, proprietary companies, public non-listed companies, public listed companies, incorporated limited partnerships, and incorporated associations must register with ASIC. Incorporated and limited partnerships, incorporated associations and cooperatives are at State or Territory level. ASIC and the relevant State or Territory authorities maintain a number of registers that relate to legal

persons. They are available to competent authorities and to the public (possibly subject to the payment of a fee) and allow for several types of searches.

7.5. In addition to these registers, the ATO maintains a register of the businesses (i.e. any type of legal persons and arrangements) holding an Australian Business Number (ABN). Holding an ABN is compulsory for businesses that are required to register for the goods and services tax (GST). Australia also advised that there is a significant incentive for businesses which are not required to have an ABN to register for one, as other businesses are required to withhold 46.5% of the value of the invoice when paying charges to businesses without an ABN.

7.6. Some specific sectors, such as the non-profit and alternative remittance sectors, are subject to additional regulation which applies to all entities operating within these sectors, regardless of the type of legal persons and arrangements.

### *(b) Overview of legal arrangements*

7.7. Trust law in Australia is governed primarily by common law at the State and Territory level. States and Territories also have statutes which impose additional obligations on trustees and a trust's constituent elements. The federal *Corporations Act 2001* (Corporations Act) applies in addition to trust law when a trustee is a corporate entity; and if the trust receives income, it is subject to federal tax laws and must lodge an annual tax return with the ATO. In doing so, information about trustees and in some cases beneficiaries is disclosed and recorded by the ATO.

7.8. Australia does not have a central registry of trusts although the Australian Business Register (ABR), hosted by the ATO, records information for a significant number of trusts. Some information on trusts holding a tax file number is recorded by the ATO but is limited to trusts registered with the ATO. As of 30 September 2014, approximately 802 700 trusts lodged a tax return for the 2011–12 income year and over 768 000 trusts lodged tax returns for the 2012/13 income year. The ABR indicated that the number of trusts registered as of 30 June 2013 was over 991 000 trusts. There is no estimate of the total number of trusts existing in Australia.

### *(c) International context for legal persons and arrangements*

7.9. Australia's political and economic stability is attractive to foreign investment. Australia requires that at least one corporate director resides in Australia.

7.10. In 2009, Project Mercury investigated risks or vulnerabilities arising from the lack of transparency in the ownership of Australian securities. The primary focus was offshore ownership and Custodial Service Provider (CSP) and nominee company arrangements. It found that:

- Approximately 40% of the ASX (Australia Securities Exchange) market was owned by foreign entities, and
- Approximately 47% of the ASX market was held by CSPs and nominee companies.

7.11. These characteristics of the ownership of ASX securities were not in themselves cause for concern, provided effective controls and measures for accessing information are in place. Indeed, foreign investment is essential to the Australian economy. Further, CSPs and nominee companies play an important role for investors in helping them to maintain a level of public anonymity, as well as providing flexibility in their investment options.

## 7.2 Technical Compliance (R.24, R.25)

7.12. See for the full narrative the technical compliance annex:

- **Recommendation 24 (transparency and beneficial ownership of legal persons) is rated partially compliant.**
- **Recommendation 25 (transparency and beneficial ownership of legal arrangements) is rated non-compliant.**

## 7.3 Effectiveness: Immediate Outcome 5 (Legal Persons and Arrangements)

### *Risk and transparency of legal persons and legal arrangements*

7.13. Australia has assessed the threat of ML through corporate vehicles and other legal persons in the NTA and, in the context of organised crime, in the sanitised version of the ACC's biennial OCTA (Organised Crime Threat Assessment in Australia). The NTA made a distinction between corporate entities that can be used to conceal crime wealth and ownership, and public companies where shares can be purchased using proceeds of crime. The first scenario was given a high threat rating; the second a medium threat rating. The two threat/risk levels over the next three years was assessed as being stable, although there will be an increasing use of legal persons and arrangements by organised crime and an increased use of foreign legal entity structures. During the on-site visit to Australia, the different stakeholders advised that they shared the conclusions of the NTA with respect to legal persons and arrangements. The sanitised version of the NRA on TF risk does not formally assess the risk of TF through legal persons. Nevertheless, Australia does have some understanding of TF risks associated with legal persons as a result of the NTA in which TF, as a predicate crime to ML, was examined. This understanding flows into the NRA where TF through legal persons is referenced by case examples and red flag indicators, although not formally rated with a risk rating.

7.14. Prior to the NTA, in 2009 Project Mercury (a sub-project of Project Wickenby) investigated the risks and vulnerabilities arising from the lack of transparency in the ownership of Australian securities. The primary focus was on the following: (1) offshore ownership, (2) custodial service providers and (3) nominee company arrangements. However, no specific assessment of the ML and TF risks associated with numbered companies, shelf companies, foreign owned domestic companies and companies incorporated in high risk jurisdictions subsequently registered in Australia has been undertaken.

7.15. Following the assessment of ML risks associated with legal persons and legal arrangements in the NTA, some improvements to the ABR were made to address the general identified risk requiring the collection of information on associates and trustees for new registrations from December 2013. In addition, as a result of Project Mercury, some typologies and case studies following on from that project supported general CDD enhancements in recent 2014 measures.

7.16. Apart from the general information in the NTA, no other risks specific to the trusts were raised by the Australian authorities. However, it was acknowledged that the authorities have encountered difficulties, in particular, to access information on foreign trusts established in jurisdictions such as the Cook Islands, Jersey, and Panama, and other off-shore trust jurisdictions. They further advised that the difficulties encountered with certain jurisdictions are limited thanks to a good cooperation with key partners. It is however planned to improve the ABN register held by the ATO and to computerise the register held by the NSW Department of Fair Trading.

### *Nominee shareholders and nominee directors*

7.17. As described in the TC Annex, nominee shareholders may hold shares for the benefit of another natural or legal person. Under the Corporations Act, nominee shareholders are required to advise the company that shares are held "non-beneficially" which must be recorded in the company register. Failure to comply with this requirement is an offence under the Corporations Act (section 1311(1); and Schedule 3) (i.e. a fine

of 5 penalty units or AUD 850). If the offence is committed by a body corporate, the fine may be increased by up to 5 times the maximum amount. Further sanctions apply if the shareholder fails to comply with their obligations in relation to any beneficial tracing notice issued to it. Australia has partially addressed issues with nominee shareholders using ASIC powers to trace beneficial owners of shares, but only for publicly listed entities.

7.18. The appointment of nominee directors ("alternate directors") must be notified to ASIC within 28 days. Failure to notify such a nomination is sanctioned by a fine (approx. AUD 10 000) and/or one year imprisonment. While the sanction is appropriate to the risk of nominee directors being appointed to conceal control of corporate entities, no fines under this provision have ever been applied.

### *Basic information*

7.19. ASIC holds a number of on-line registers, including:

1. the company register, containing approximately 2 million registrations at the time of the on-site visit;
2. the national business register;
3. the register for AFSL holders; and
4. the register for liquidators and company auditors.

7.20. When registering, companies are required to provide certain information, including the company details (name, type, address of the registered office, etc.), the names and addresses of the directors and secretaries and the share structure. Although rarely seen, bearer share warrants may nevertheless be issued by Australian companies incorporated under the Corporations Act, but there are no measures in place to identify the holder of the beneficial owner of those instruments.

7.21. The company register contains the following information:

- name of the company;
- unique identification number (ABN, Australian Company Number [ACN], Australian Registered Business Number [ARBN], or Australian Registered Scheme Number (ARSN));
- type of company;
- date of registration;
- date of the next annual review;
- address of registered office, and
- the list of documents lodged with ASIC.

7.22. This information is available to competent authorities. Basic information is accessible to the public online. Other information, such as current or historical extracts, roles and relationship extracts or copies of certain documents lodged with ASIC, is available to competent authorities as well as to the public for a small fee.

7.23. While ASIC does checks to ensure substantial compliance with lodgement obligations, it conducts only limited accuracy of information checks. Examples are (1) checks against Australia Post Files to ensure addresses are valid physical addresses if required, and (2) checks of new officeholder names against bankruptcy records held by the Australian Financial Security Authority. No key information verification, including checks on criminal records or terrorist lists, is conducted. ASIC advised that if the registration

## LEGAL PERSONS AND ARRANGEMENTS

contains suspicious elements or raises suspicion, more verification would be undertaken but that such a situation is very rare.

7.24. Companies are required to notify ASIC within specified timeframes (generally 28 days or less) about a change of registered office, principal place of business, its member register, its share structure, directors or secretaries, including in their personal details. Failure to notify is sanctioned by a fine of 60 penalty units (AUD 10 200) and/or one year imprisonment.

7.25. ASIC also conducts an annual review of each of the companies registered. The review occurs at the anniversary date of the registration. Companies are required to review and as necessary update their information and to provide a solvency declaration. Along with the annual review, companies also have to pay the annual review fee, which helps to identify companies that have changed address or that have ceased their activities. However, ASIC advised that it does not have the resources for proactive searches and verifications. ASIC may also require a company at any time to respond to a return of particulars (section 348A of the Corporations Act) if there is a suspicion that recorded information is incorrect.

7

7.26. ASIC advised that 80 to 95% of the companies registered were registered online by a third party. These third parties can be lawyers or accountants, but a large majority of the companies are registered by trust and company service providers specialising in companies' registration. In addition to registration, trust and company service providers also set up trust and self-managed funds. They justified the high level of reliance on third parties for companies' registration by the fact that they are specialised in this activity and are aware of any obstacle in the registration process. Moreover, most trust and company service providers have direct access to ASIC and ASIC's registers, which ensures a timely registration. Trust and company service providers met during the onsite also advised that the large majority of their clients are not the companies themselves, but lawyers and accountants acting on the behalf of their clients. Once registered, companies can still rely on trust and company service providers to fulfil the companies' obligations vis-à-vis ASIC. This includes the notification of any changes affecting the company or the response to the annual review and the payment of the annual fee. These elements (the fact that companies' registration businesses do not know who their clients are and provide services after the registration) raise concerns as to the veracity and accuracy of the information recorded in ASIC registers and potential misuse of companies for ML/TF purposes. Neither trust and company service providers nor lawyers or accountants are subject to AML/CTF obligations.

7.27. Registers are maintained by State and Territory authorities in relation to the creation of incorporated and limited partnerships, incorporated associations and cooperatives. From discussions that the assessment team had with the New South Wales (NSW) Department of Fair Trading, it appears that the obligations on partnerships, associations and cooperatives are similar to those of companies registered by ASIC, including with respect to the notification of changes affecting them. Certain basic information is available to competent authorities and to the public for a small fee. It should be noted that access to the registries is currently being improved through a computerisation project. As with ASIC, the NSW Department of Fair Trading takes the registration information it receives on face value and does not conduct any specific accuracy verification. Accordingly information in State and Territory registers may not be accurate or up-to-date.

7.28. Apart from the registers held for the different types of legal persons, the ATO also maintains the ABR, which gathers information on the natural persons, legal persons and arrangements that have an ABN. In total there are over 7.5 million ABN holders registered in the ABR.

7.29. The ABR contains information on individuals, companies, government agencies, partnerships, trusts and superannuation funds. The ABR contains information on the ABN holder; however in case of companies, there is no comparison / cross-verification with the data held by ASIC on a specific company. There is, however, verification of company number and company name, but no cross-referencing of director or secretary information. ABN holders are required to notify the ATO of any relevant change; in case of failure to notify changes within the set period, sanctions similar to those mentioned above for failure to notify ASIC apply. In 2013-14, 3.8 million updates were made to the ABR. The ATO advised that only a few companies are picked up every year for a review of their information. The ABR is available to competent authorities and to the public. Numerous searches are made every year; however only limited information on the ABN, state of operation, legal name and business name, and date of registration, is available to the public. The ATO advised

that it has a project to improve the ABR and implement expanded automated processes, including for the verification of the information provided.

7.30. With respect to legal arrangements, there is no obligation for trustees to maintain basic information on the trust. Australia relies on the obligation to identify customers that are legal arrangements, which apply to reporting entities to get basic information on legal arrangements. As described under IO.4 and in the TC Annex, this obligation is overall in line with the FATF Standards. While the measures were introduced on 1 June 2014, entities have a transition period until 31 December 2015. Moreover, this mechanism will only be available for trusts with relationships with financial institutions, because trust and company service providers, lawyers, and accountants who create the trusts do not have AML/CTF obligations.

### *Beneficial ownership information*

7.31. Under section 169 of the Corporations Act, companies are required to hold a register of members (shareholders) containing each member's name and address, date on which the member was issued shares, the number and class of shares held, and date of issuance. This information relates to legal, not beneficial, ownership. However, for publicly listed entities, the register must also include information disclosed in the context of the ASIC's power to trace beneficial ownership of shares (Corporations Act, Part 6C.2). Under this article, ASIC may direct a member of a publicly listed company, a person having a relevant interest or having given instructions about voting shares, to disclose the detail of his/her interest in the shares, information about the acquisition or disposal of the shares, the exercise of the voting rights or any other matters relating to the shares. Any information received by the company in this context must be recorded. There are no equivalent powers in relation to non-list companies. Law enforcement agencies met in Australia recognised that companies' registers are a good source of information on beneficial ownership, but also expressed frustration about how long it can take to trace such information, exacerbated if structures are complex and involve foreign shareholders, the use of front persons or trusts that mask the ultimate beneficial owner, or both.

7.32. For listed companies, section 672DA of the Corporations Act provides that "relevant interests" in shares (securities) must be disclosed; "relevant interest" is defined in section 608 as meaning, amongst other things, an interest "however remote" and can include beneficial interests as contemplated by the meaning of beneficial owner in the Glossary to the FATF Methodology.

7.33. ASIC registers contain information on the share structure, including for companies limited by shares the number and class of shares each member and for unlimited companies, information on the issue of shares, as well as membership details. The ATO registers also contain information on 20 key shareholders (regardless of whether they are natural or legal persons) as well as on the trustee, the settlor and the beneficiaries of a trust. The ABR holds information on the 20 key shareholders of private companies, registered from December 2013 and trustees and beneficiaries for closely held trusts registered from December 2013. The ABR is governed by the *A New Tax System (Australian Business Number) Act 1999*. These measures mitigate to some extent the ML and TF risks identified in the NTA.

7.34. With respect to beneficial ownership, law enforcement advised that the best source of information is reporting entities. This entails that law enforcement knows which reporting entity has a business relationship with the legal person or arrangement at stake, and that the legal person or arrangement has established a business relationship with a reporting entity. As mentioned above, reporting entities are since 1 June 2014 required to identify the beneficial owner of their clients and to take reasonable measures to verify their identity consistent with Recommendation 10. However, entities have a transition period until 31 December. The quality of the information held by reporting entities is therefore questionable. Furthermore, reporting entities met during the onsite visit to Australia advised that they currently fulfil their obligation with respect to beneficial owners through the consultation of public registers, such as ASIC registers. In addition, as mentioned, TCSPs, lawyers, and accountants are not reporting entities.

7.35. Special measures for listed companies: ASIC or a listed company may issue a tracing notice in relation to holdings in the listed company (section 672A of Corporations Act). In practice, there are a number of businesses that issue beneficial tracing notices on behalf of listed companies and it is common for this to occur. In most instances, ASIC will not be involved as the listed company will do this work and the responses

from these notices must be publicly available (section 672DA of Corporations Act). Third parties can also request ASIC to issue a tracing notice. Disclosure in response to a tracing notice must be made within two days, and failing to respond to a tracing notice is a strict liability offence with penalty up to 25 penalty units (AUD 4 250) and/or six months imprisonment. ASIC is infrequently approached by companies seeking ASIC involvement where there has been a failure to comply with a beneficial tracing notice sent by a listed company or responsible entity of a listed management investment scheme. There are also obligations under tax law for declaring trustee status in tax returns.

### *Information exchange and international cooperation*

7.36. The numerous registers held by the different authorities involved in the registration of legal persons and the tax authorities are accessible to law enforcement authorities. At national level, ASIC can share information pursuant to MOUs or via information forums or committees with a large number of federal law enforcement agencies and competent authorities, including the AGD, the ACC, the AFP, the two financial supervisory bodies, and AUSTRAC. At the State and Territory level, ASIC can exchange information to assist the federal, State or Territory governments to perform a function or exercise a power (section 127 of the ASIC Act). In 2012/2013, over 60 million searches were made, as well as more than 4 million paid searches.

7.37. ASIC can exchange information with 102 foreign counterparts under the International Organisation of Securities Commissions (IOSCO) Multilateral Memoranda of Understanding (MMOU) Concerning Consultation and Cooperation and the Exchange of Information (enforcement). ASIC can exchange information with 64 foreign counterparts under an additional 80 bilateral MOUs covering supervision and enforcement. ASIC's MOUs and the MMOU allow for the exchange of information recorded in ASIC's registers. ASIC can exchange information recorded in ASIC registers with foreign counterparts and other agencies, including law enforcement agencies, whether or not there is an MOU. This includes publicly available information. If the information is not publicly available on ASIC's registers but is held by ASIC in relation to its registry function, ASIC can release the information pursuant to section 127(4) of the ASIC Act and, if an MOU exists, pursuant to the terms of the MOU.

7.38. The ABR is widely accessible to federal agencies and State and Territory Governments. Over 370 million searches were made in the ABR in 2012-2013. In addition, ASIC has provided information on the number of additional requests made by law enforcement authorities for information not in the public registers. Also in 2013-2014, the ATO received 2 610 requests from a range of law enforcement agencies, including 10 requests for ABR information.

## **Overall conclusions on Immediate Outcome 5**

7.39. Legal persons and legal arrangements were identified as presenting medium to high risks for ML in the NTA, and the use of complex corporate structures in ML schemes was frequently cited by law enforcement spoken to by the assessment team. There is good information on the creation and types of legal persons in the country available publicly, but less information about legal arrangements. The ATO has made some improvements to the ABR that involve collecting information on associates and trustees for new registrations from December 2013. The authorities seem to appreciate the extent to which legal persons can be, or are being misused for ML, and had some awareness in relation to TF. However, they could do more to identify, assess and understand the vulnerabilities both for ML and TF, as past assessment efforts seem to have focused more on underlying predicate crime. While Australia has implemented some measures to address the specific risk identified in the NTA to legal persons and legal arrangements, other measures need to be taken, including imposing AML/CTF obligations on those who create and register them to strengthen the collection and availability of beneficial ownership information. Concerning beneficial owners of legal persons and legal arrangements, the existing measures and mechanisms are not sufficient to ensure that accurate and up-to-date information on beneficial owners is available in a timely manner. It is not clear that information held on legal persons and legal arrangements is accurate and up-to-date. The authorities did not provide evidence that they apply effective sanctions against persons who do not comply with their information requirements. Overall, legal persons and arrangements remain very attractive for criminals to misuse for ML and TF.

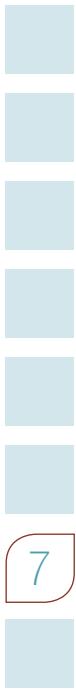
7.40. **Australia has a moderate level of effectiveness for IO.5**

## 7.4 Recommendations on Legal Persons and Arrangements

7.41. In relation to IO.5, Australia should:

- Conduct a formal assessment of the TF risks to which legal persons are exposed, and subsequently take adequate mitigating measures.
- Conduct ML and TF risk assessments for differing legal persons (numbered companies, public companies, foreign companies, etc.) to identify where the risks are, to address those specific issues.
- Ensure that minimal information on the creation of legal arrangements, including those that are not registered with ATO, is publicly available.
- Ensure that information on legal persons recorded in ASIC, State or Territory, and ATO registers is accurate and up-to-date.
- Take measures to mitigate the ML/TF risk posed by bearer share warrants.
- Ensure that competent authorities have timely access to a company's register.
- Ensure that information on the beneficial owner of legal persons and legal arrangements is maintained and accessible to competent authorities in a timely manner.
- Require reporting entities to implement as early as possible before 1 January 2016 their obligations on beneficial ownership, introduced on 1 June 2014.
- Apply proportionate and dissuasive sanctions for failure to advise a company that shares are held non-beneficially and take further measures against nominee directors.

## LEGAL PERSONS AND ARRANGEMENTS



## 8. INTERNATIONAL COOPERATION

### Key Findings

**Australia cooperates well with other countries in mutual legal assistance (MLA) matters**, receiving an average of 300-400 MLA requests per annum which are processed in a timely manner in accordance with the case prioritisation framework.

**Some problems have been identified by Australia concerning other countries meeting the requirements of the *Foreign Evidence Act 1994*.** These problems translate into delays encountered in receiving information on requests made, but these issues are mitigated to some extent by direct cooperation with the ACA and AFP for assistance. Nevertheless, delays can exist as a result of the stringent requirements of the Act.

**Australia cooperates well in extradition, both making and receiving requests in ML and TF related matters, and informal cooperation is generally good across agencies.** Australia cooperates well in providing available beneficial ownership information for legal persons and trusts in relation to foreign requests, keeping in mind that what is not (required to be) available in Australia cannot be shared. But the ability to provide beneficial ownership information for legal persons and trusts in relation to foreign requests is limited.

**Australia maintains comprehensive statistics in relation to MLA and extradition matters**, including in relation to ML and TF, although there are some limitations in relation to categorisation of ML offences within the case management framework.

## 8.1 Background and Context

8.1. Proceeds of crime in Australia are generated by a range of criminality. Internationally, Australia is prone to receive proceeds of crime generated from abroad, particularly from countries in the region and sometimes involving foreign corrupt persons, who send funds to Australia which has a safer banking sector and is attractive for foreign investment. The real estate sector in particular may be attractive for foreign investment.

8.2. Australia has ratified the Vienna, Palermo, CTF, and Merida Conventions and has a strong framework for international cooperation. The main instruments used are bilateral treaties for MLA and extradition, the *Mutual Assistance in Criminal Matters Act 1987*, the *Extradition Act 1988*, and corresponding regulations. The Australian Central Authority in the federal Attorney-General Department is Australia's central authority for MLA and extradition.

## 8.2 Technical Compliance (R.36-40)

8.3. See for the full narrative the technical compliance annex:

- **Recommendation 36 (international instruments) is rated largely compliant.**
- **Recommendation 37 (mutual legal assistance) is rated compliant.**
- **Recommendation 38 (mutual legal assistance: freezing and confiscation) is rated compliant.**
- **Recommendation 39 (extradition) is rated compliant.**
- **Recommendation 40 (other forms of international cooperation) is rated compliant.**

## 8.3 Effectiveness: Immediate Outcome 2 (International Cooperation)

8.4. Australia observed in its NTA for money laundering that there is almost always an international dimension to ML offences in Australia. Similar comments were made in the NRA for TF. Highest risk countries are not listed in the de-classified versions of those risk assessments, but authorities indicated during the mutual evaluation that some countries in the Middle East, south-east Asia and north Asia are of primary concern.

### *MLA and Extradition*

8.5. The Australian Central Authority (ACA) for MLA and extradition is within the federal Attorney General's Department (AGD). The ACA currently has 19 full time officers (11 in MLA and 8 in Extradition) who work within a case management and prioritisation framework for incoming and outgoing requests. Case prioritisation for MLA is based on factors such as court dates, crime type, national security issues, whether organised crime is an issue, and the overall seriousness of the offence involved in the request. Requests from high risk countries are managed within this set of factors but not given a higher level of priority.

8.6. Australia can provide MLA to another country on the basis of reciprocity; membership in a multi-lateral convention/treaty to which Australia is also a member; or a bilateral treaty (29 currently exist). Bilateral treaties are negotiated where the other state to the treaty requires such an instrument or where the volume of requests exchanged between Australia and the other state calls for a framework instrument to guide the processing of mutual requests (e.g. with the US).

8.7. In the 10 years between 2004-05 and 2013-14, Australia received 3 370 MLA requests; 163 related to ML and 1 477 (1/3 of all requests) related to ML predicate crimes.

**Table 8.1. MLA Requests: ML and Associated Predicate Offences**

FY	New Requests Made	ML	ML Predicates	Finalised	Refused
2004-05	205	8	41	191	0
2005-06	228	9	52	159	0
2006-07	239	5	106	242	0
2007-08	290	9	163	385	0
2008-09	340	12	173	338	0
2009-10	380	13	205	373	1
2010-11	427	15	200	438	0
2011-12	387	28	179	391	1
2012-13	398	38	198	385	1
2013-14	321	26	160	345	0
<b>TOTAL</b>	<b>3 370</b>	<b>163</b>	<b>1 477</b>	<b>3 011</b>	<b>3</b>

8

8.8. Australia is unable, due to the case management system, to break down these statistics further, to show how many of the ML-related requests involved self-laundering, third party laundering, or foreign predicate crimes. None of the three refusals in this time period were in relation to ML cases. Over the same period, Australia received 28 terrorism-related MLA requests and 10 TF-related requests, none of which were refused.

**Table 8.2. MLA Requests: Terrorism and Terrorist Financing**

FY	New Requests Made	Terrorism	Terrorist Financing	Finalised	Refused
2004-05	151	0	1	126	0
2005-06	167	0	1	94	0
2006-07	220	2	0	176	0
2007-08	225	6	3	298	0
2008-09	184	4	0	186	0
2009-10	182	2	1	192	0
2010-11	203	11	2	175	0
2011-12	263	1	0	225	0
2012-13	292	0	2	259	0
2013-14	353	2	0	303	0
<b>TOTAL</b>	<b>2 240</b>	<b>28</b>	<b>10</b>	<b>2 034</b>	<b>0</b>

8.9. Over the same 10-year period, Australia received 281 requests to obtain or enforce proceeds orders, but is only able to provide information in relation to those requests made between 2010 and 2014. During that period, Australia received 46 MLA requests for restraint or forfeiture action, all of which involved ML and associated predicate crimes. Of the 46 requests, nine restraint actions were taken and one forfeiture action, totalling approximately AUD 34.6 million in assets for both types of actions. At the time of the on-site visit, a further restraint request totalling AUD 3.7 million was under consideration. Bearing in mind that Australia is at some risk of receiving proceeds of crime from foreign predicate offences, including corruption offences, the

## INTERNATIONAL COOPERATION

authorities should continue to enhance efforts on effective restraint and forfeiture action pursuant to foreign requests received.

8.10. For expediency, MLA requests may be made directly to the ACA via email, post and fax, and not strictly through diplomatic channels. The time necessary to complete MLA requests is dependent on a number of factors, including whether the request involves coercive or non-coercive measures; whether the request is detailed or accurate enough to comply with the request; and whether witnesses from whom statements are requested can be located. The AFP's International Liaison Officers Network assists countries in making requests to Australia where required in order to ensure that requests to the ACA are not delayed. Authorities indicated that requests requiring a search warrant (bank records) may take two to three months, whereas non-coercive assistance (voluntary witness statements) may take one to two months. Feedback from 20 countries prior to the mutual evaluation shows that Australia's cooperation is good both in terms of the time taken to process incoming requests and the quality of the information provided by authorities.

8.11. Likewise, Australia pursues assistance from other countries in order to enforce criminal law in Australia. Since 2004 Australia has sought MLA in 201 instances from other countries relating to ML; 1 074 instances in relation to associated ML predicate crimes; and 90 MLA requests in relation to terrorism, including nine requests (one investigation) in relation to TF. In one case (Project Hyssop) involving an Australian-based narcotics syndicate, assistance was sought from other countries involving MLA and information exchanges through Egmont. This resulted in restraint action overseas totalling AUD 15 million in relation to narcotics trafficking and ML.

8.12. Australia has not always received the information sought in a form admissible within Australian courts in accordance with the *Foreign Evidence Act 1994*. The requirements of that Act are onerous for other countries to meet (agreed by Australia) and there will likely be delays in providing the information requested when meeting them. While these issues are mitigated to some extent by direct cooperation and assistance from ACA and AFP, delays can exist as a result of stringent requirements of the Act. Serious consideration should be given to easing the admissibility requirements.<sup>1</sup>

8.13. With respect to extradition, Australia cooperates bilaterally on the basis of several regimes including bilateral treaties; the London Scheme for Commonwealth countries; multilateral conventions/treaties; and whether a country has been designated as an extradition country under Australian regulations. A simplified and speedy system of "backed warrants" exists with New Zealand. Requests under this scheme are managed on a police to police basis. The CDPP appears in extradition proceedings on behalf of New Zealand, including reviews and appeals. According to the CDPP, challenges to surrender do not happen often. The CDPP is also involved in outgoing requests where extradition is sought of persons charged with federal offences.

8.14. Between 2004 and 2014, 228 extradition requests were received. In that ten-year period, 95 requests were granted, six of which related to ML and TF. In the same period Australia made 171 extradition requests. 113 requests were granted in that period.

**Table 8.3. Extradition Requests Received from Other Countries**

	2004-05	2005-06	2006-07	2007-08	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14
Requests received	15	21	22	12	17	30	23	22	23	43
Requests granted	12	11	8	9	10	6	5	10	11	13
Requests refused	1	2	0	1	2	1	0	1	2	2

1 The FEA was amended following the on-site visit to address these issues including more streamlined procedures to admit in evidence material obtained through MLA or agency-to-agency channels

8.15. As with MLA, Australia's cooperation in extradition has been good with positive feedback from other countries. In one instance, a country complained of delays by Australia in an extradition matter indicating Australia's bureaucratic requirements, but this is not reflective of the general feedback received from the 19 other countries that provided feedback.

### *Other Forms of International Cooperation*

8.16. AUSTRAC: There are no legal barriers for AUSTRAC to cooperate with other supervisory bodies. However, AUSTRAC indicated that it had never received a request from any foreign AML/CTF regulator/supervisor, neither directly or indirectly (through APRA). AUSTRAC has never submitted a request to a foreign AML/CTF regulator/supervisor. AUSTRAC stressed that the absence of international cooperation in the regulatory area may be caused by the fact that AUSTRAC is the FIU and the AML/CTF regulator/supervisor, something which is unique according to AUSTRAC. It is noteworthy that AUSTRAC has taken the initiative to set up regulatory overseas contacts with the FIUs of Canada and New Zealand.

8.17. ASIC: Under the ASIC Act, ASIC can share any information that is in its possession and can exchange information directly with foreign law enforcement agencies, including Interpol. ASIC may seek further information from regulated entities based on a foreign request when the request is in support of a civil or administrative regulatory matter. If a request is solely related to criminal matters, it needs to come to ASIC via AGD and the MLA channel. To date, almost all information exchanges resulting from foreign requests have related only to direct or basic beneficial ownership in addition to other readily available information such as information on directors and senior managers, corporate status or licensing information of entities registered with ASIC. ASIC has been able to respond to these requests quickly. When requests are made for more extensive beneficial information beyond what is readily available to ASIC (i.e. basic information), law enforcement authorities use their powers to secure that information if it relates to information held in Australia. However, if foreign requests relate to public companies, beneficial ownership tracing notices may be issued by ASIC. ASIC can share and exchange ML/TF-related information. While an MOU is not necessary for ASIC to share information, ASIC nevertheless has 76 bilateral and multilateral MOUs with foreign counterparts. ASIC has no AML/CTF-related responsibilities and exchanges of information with foreign FIUs are made via AUSTRAC. When ASIC's enforcement branch becomes aware of AUSTRAC-related information that might be of interest to a foreign counterpart, the enforcement branch refers the matter to ASIC's international cooperation branch, who works with AUSTRAC to determine the best way to convey that information to the foreign agency; this may involve telling a foreign counterpart to request information from Australia via the FIU.

8.18. APRA: APRA's international cooperation is limited to the exchange of information related to prudential supervision. While MOUs are not required to exchange information with foreign counterparts, APRA has approximately 25 MOUs with counterparts with whom they are likely to share information on a regular basis. APRA reported that they have not had many requests to exchange information. APRA noted that it would reject requests that were not related to prudential supervision. APRA did not have a formal policy for how to respond to AML/CTF requests; authorities stated that if it received a request related to AML/CTF it would either refer the matter directly to AUSTRAC or it would deny the request and recommend the counterpart contact AUSTRAC.

8.19. AFP: The AFP's International Liaison Officer Network consists of 99 liaison officers in 29 countries attached to Australian embassies and high commissions often supported by a number of MOUs – which are not necessarily required for police-to-police cooperation. The Network is the first point of contact for law enforcement enquiries to be raised with Australian law enforcement domestically. It operates with foreign counterparts to exchange information on asset recovery matters, often having knowledge of assets in jurisdictions where they are located well before an MLA request is made. The AFP is also the designated INTERPOL National Central Bureau (NCB) for Australia and facilitates international enquiries to and from relevant Australian and foreign law enforcement, government, and regulatory agencies. Australia has provided case material to illustrate the effectiveness of the Network.

8.20. ACBPS: The ACBPS has a network of 50 MOUs with relevant foreign counterparts. As with the AFP, MOUs are not required to cooperate and exchange information with other customs and border protection services. ACBPS can share information with other law enforcement agencies, such as the AFP, but not with

intelligence agencies, except through the relevant agency in Australia (e.g. AUSTRAC). Recently, the ACBPS established a Trade Enforcement Unit to target trade-based ML in Australia and is in the process of establishing international connections to exchange information relevant to trade-based ML. Currently, this new unit is involved in a major trade-based ML investigation with the United States.

8.21. ATO: The ATO has a number of instruments which permit international cooperation in the exchange of information with foreign counterparts, including double tax agreements, multi-lateral tax conventions and MOUs. The ATO belongs to the Joint International Tax Shelter Information Centre, which is designed to facilitate the sharing of information amongst partner agencies, including intelligence and individuals of interest (in particular financial intermediaries). However, the ATO can only share information with other tax administrations, including information held relating to trusts that are meeting the strict legal requirements of confidentiality obligations. The ATO is not able to share information with other non-revenue agencies, unless other agencies are involved in investigating a criminal offence.

### Overall conclusions on Immediate Outcome 2

8.22. The Immediate Outcome is achieved to a very large extent. Australia uses robust systems for MLA, as demonstrated by their statistics, although there are some limitations in relation to the categorisation of ML offences within the case management framework. Informal cooperation is generally good across agencies. Although diagonal cooperation does not appear to be permitted with ASIC and APRA, this is not a significant issue. Australia cooperates well in providing available beneficial ownership information for legal persons and trusts in relation to foreign requests, keeping in mind that what is not (required to be) available in Australia cannot be shared.

8.23. **Australia has achieved a high level of effectiveness for IO.2.**

### 8.4 Recommendations on International Cooperation

8.24. In relation to IO.2, Australia should (noting that the Foreign Evidence Act 1994 was amended post on-site):

- Establish mechanisms to ensure that if a foreign request is made for beneficial ownership information beyond basic information in relation to legal persons and arrangements, it can provide that information.

## **TECHNICAL COMPLIANCE ANNEX**

### **1. INTRODUCTION**

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations of Australia. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2005. This report is available at:

[www.fatf-gafi.org/countries/a-c/australia/documents/mutualevaluationofaustralia.html](http://www.fatf-gafi.org/countries/a-c/australia/documents/mutualevaluationofaustralia.html).



## 2. NATIONAL AML/CFT POLICIES AND COORDINATION

### Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

a2.1. This is a new Recommendation and assessing against it requires full analysis against all of the criteria.

#### *Risk assessment*

a2.2. **Criterion 1.1** – Australia uses many processes to identify and assesses its ML/TF risks that generally result in a reasonable portrayal of most of those risks. The written ML risk assessment conducted focuses on most major risks but likely fails to identify all potential ML risks, or provide a sufficient basis for proper analysis to assess the risks due to its somewhat limited scope and information base (elaborated below), but this is supplemented by other ongoing risk analysis. Australia has generally identified and assessed its TF risks. Australia has produced two national reports on its ML/TF risks, which are supplemented by an Organised Crime Threat Assessment (OCTA) (produced by the ACC every two years) that contains information about aspects of the predicate crime environment arising from organised criminal activity, but not other forms of criminal activity<sup>1</sup>. In addition, Australian authorities use dynamic processes for ongoing analysis of risk built around strong inter-agency cooperation and joint task forces. These processes include informal regular discussions as well as intelligence assessments and other studies into specific areas of risk. The two national reports, produced by AUSTRAC, in collaboration with law enforcement and national security agencies, were:

- The 2011 NTA assesses ML threats by examining measures, the intelligence picture, drivers and enablers, and gaps.<sup>2</sup> It also assesses high-risk countries that influence Australia's ML environment. While providing a baseline upon which future assessments can build, its scope is somewhat limited as it focuses primarily on the channels identified as vulnerable to laundering proceeds in the private sector (akin to the approach in the FATF Money Laundering and Terrorist Financing Global Threat Assessment 2010) rather than broader AML/CTF regime vulnerabilities, thus potentially failing to identify some risks (e.g. customer risk, foreign predicate risk, risks due to weaknesses in the authorities' AML/CTF efforts). Some of these vulnerabilities may have been examined through a threat matrix that assessed deterrence and detection elements of the framework, related mainly to the AML/CTF preventive measures but not to other measures. It is primarily a qualitative assessment based on law enforcement and financial intelligence experts' input<sup>3</sup>, taking into account mainly classified information that was not made available to the assessors. The NTA draws links between crime types, criminal groups, ML channels and dominant typologies, informed by the OCTA and other strategic criminal intelligence. There is a modest discussion on the predicate crime threat environment concentrating on organised and serious crime which may not assess or examine all of the predicate crimes for their ML risk as fully as may have been expected<sup>4</sup>. The NTA

1 The OCTA focuses on offences that involve two or more offenders, substantial planning and organisation and the use of sophisticated methods and techniques, which is committed in conjunction with other serious offences punishable by imprisonment for a period of three years or more.

2 Note that it was produced prior to FATF adopting R.1 or publishing any guidance on assessing ML/TF risk.

3 The main agencies making input were: AUSTRAC, AGD, ACC, AFP, ACBPS, ATO and the New South Wales Crime Commission. Other federal, State and Territory agencies were consulted, provided information, or both (e.g. ASIC, the Queensland Crime and Corruption Commission, and the Victoria Police). Information from international law enforcement partners and FIUs was also used.

4 For example, it downplays the ML risk posed by domestic cannabis markets identified in: Australian Institute of Criminology (AIC) Counting the costs of crime in Australia a 2005 update (published 2008); Australian Bureau of Statistics The Non-Observed Economy and Australia's GDP, 2012. This is due to the OCTA assessment of the predicate

A2

also relied on analysis of information reported to AUSTRAC, which may not be representative of actual ML behaviour in Australia. To address an absence of data on the number or value of ML cases, the assessment drew on a sample of 174 sanitised predicate crime and ML cases contained in AUSTRAC's annual typologies report. The authorities involved in the NTA considered that these cases broadly represented the main areas of ML activity, although they recognised the limitations of this approach and that it does not reflect levels of activity across the breadth of sectors exploited for ML. These cases contain some information about the value being laundered but other intelligence and analysis of AUSTRAC data was used to fill this gap. The NTA also does not address the harm or consequences of the identified risks; the NTA notes that, apart from fuelling criminal enterprises, reliable evidence of ML consequences is limited in Australia. Thus, overall, while the NTA identifies and assesses most of the main risks, the assessors question whether the scope, inputs, and focus limit the analysis in relation to some other ML risk areas.

- The 2014 NRA focuses on TF risks (within Australia and from foreign countries) which impact on Australia's domestic environment. It assesses the risk associated with the methods and financial channels used to raise or transfer funds for TF. High-risk countries which influence TF in Australia are also examined. It was coordinated by AUSTRAC, finalised in April 2014, and prepared with input from intelligence held across law enforcement and national security agencies.<sup>5</sup> In addition, AUSTRAC developed a 'forensic' profile of financial activity from the reports in AUSTRAC's data holdings since 2006 related to TF matters. The methodology used, which drew on the NTA and modified it to take into account the FATF guidance on conducting ML/TF risk assessment was superior to that used for the NTA such that it more likely identifies and assesses the TF risks in Australia.

a2.3. **Criterion 1.2** – Australia's 2010/11 National Organised Crime Response Plan (NOCRP) identified that ML risks would be assessed and that AUSTRAC, as lead agency for AML/CTF, would be responsible. AUSTRAC, in consultation with the AFP and ASIO, was also chosen to take the lead for coordinating actions to assess TF risks.

a2.4. **Criterion 1.3** – While the NRA is new and therefore up to date, the NTA is less so. For example, it did not identify or assess new and emerging risks that have been reflected in the latest FATF standard, and contains some outdated information about Australia's predicate crime environment. The authorities have indicated that they plan to update the NTA and NRA at five yearly intervals. In between these updates AUSTRAC has been producing thematic criminal and financial intelligence assessments to respond to the areas identified as requiring further work in the NTA (e.g. on: PEPs, corruption and foreign bribery; digital and virtual currencies; legal practitioners, and real estate agents). These reports have been provided to partner agencies to help them understand evolving risks (e.g. TBML is now seen as a greater risk than it was assessed in the NTA). However, while useful, these reports do not normally assess the level of risk or reassess existing levels of risk, nor do they derive from a methodology like those in the NTA or NRA. In addition, the authorities maintain that other reports, such as the two-yearly OCTAs, intelligence analysis produced by national criminal task forces, and national security statements also provide regular information about ML/TF risks. However, these other reports do not focus primarily on ML/TF and most do not formally identify and assess ML/TF risks.<sup>6</sup>

---

crime environment, on which the NTA was based, including an assessment of the harms posed by the different crimes, meaning that the large volume of domestic proceeds generated from cannabis was given less attention. Australia may want to reconsider this approach given that the assessment is meant to focus on ML not predicate crime.

5 Input came from: the AFP-led Terrorism Financing Investigations Unit (TFIU), AGD, ACNC, ACC, ACBPS, Australian Intelligence Community agencies, DFAT and Department of Prime Minister and Cabinet. The TFIU coordinated input on the assessment from State and Territory law enforcement agencies through Australia's network of joint counter-terrorism teams.

6 Recent OCTAs have included some assessment of certain emerging ML risks.

a2.5. **Criterion 1.4** – The authorities shared the classified NTA with all partner agencies and have published a summary version for use by self-regulatory bodies, financial institutions, and DNFBPs. However, the summary version of the NTA reads in many parts like a generic ML typologies report and it does not share information on a key result of the risk assessment - high risk countries, nor does it draw attention to the relative importance of transnational ML risks. The classified version of the NRA has been shared with partner agencies but no mechanism had been used to provide information on the NRA results to the private sector at the time of the onsite.<sup>7</sup>

### *Risk mitigation*

a2.6. **Criterion 1.5** – The AML/CFT regime is calibrated around mitigating risks from organised and serious crimes with the regulatory focus on banks, the gaming sector, and remitters – seen as the main channels for ML (and also TF for the latter). The AML IDC agrees and sets annual risk-based priorities to guide the work and resource allocation of its member agencies on AML/CFT matters. Each agency must initiate changes to its resource allocation through its Minister and ultimately Parliament. Most AML/CFT agency budgets have been reduced recently as part of broader government-wide budget reductions since the Global Financial Crisis despite the NTA identifying high risk areas requiring attention and the OCTA identifying ML as a key risk enabling organised and serious crime. Despite this tighter budgetary backdrop, additional funding has been given to agencies (e.g. AUSTRAC received additional funding for new intelligence systems in 2010 and AUSTRAC for a remitter register in 2011) on the basis of understanding risks.<sup>8</sup> There are also some examples of reallocating existing resource to address risks (the ACC established a remittance task force in December 2012 that participating agencies funded by reallocating resources, and the NSW Police and NSW Crime Commission established dedicated dedicated ML teams). While these examples of moving resources to address identified risks involve interagency consultation, there does not appear to be any whole of government approach to resource allocation to AML/CFT matters on the basis of risk. A large concern is that no legislative or regulatory measures have been promulgated to mitigate the high risks identified with certain DNFBPs (accountants, lawyers, trust and company service providers and real estate agents), other businesses (e.g. high-value goods and cash intensive businesses) all of which are outside of the scope of the AML/CFT regime or related to preventing the abuse of legal entity structures. This indicates that the AML/CFT legal and regulatory framework could be better harmonised with the identified risks.

a2.7. **Criterion 1.6** – The regulatory framework does not require reporting entities to fully implement all requirements of the relevant FATF Recommendations (see section of report on preventive measures). However, the basis for these exemptions is not solely on the basis of low risk. The legislative requirements (sections 248 and 212 of the AML/CFT Act) and published policy provide that the basis is also concerned with avoiding excessive regulatory burden and other considerations. While the authorities have rejected some exemption applications because risks were too high, they have not provided convincing evidence that those granted were on the basis of demonstrated low ML and TF risk and some exemptions appear to be granted solely on the basis of excessive regulatory burden.<sup>9</sup> Moreover there are other examples where the FATF Recommendations are not fully applied that are not clearly based on low ML/TF risk. There is an exemption for the gaming industry in relation to transactions under AUD 10 000 and the exemption from most of the AML/CFT obligations applicable to any person licensed to operate no more than 15 gaming machines (Chapter 52 of the AML/CFT Rules) run counter to the NTA assessment that the gaming sector

7 A sanitised version of the NRA was published on 11 September 2014, following the on-site.

8 After the on-site, the federal government also made AUD 650 million available to fight terrorism, including AUD 20 million for AUSTRAC to enhance its TF analysis and tracking capabilities.

9 AUSTRAC states that it will consider exemptions where “*the burden imposed on business is likely to be greater than is warranted by the risk*” (see [www.austrac.gov.au/exemption\\_policy.html](http://www.austrac.gov.au/exemption_policy.html)). Moreover, the AML/CFT Act section 212(3)(c), requires that the AUSTRAC CEO must have regard to, amongst other things, “*the desirability of ensuring that regulatory considerations are addressed in a way that does not impose unnecessary financial and administrative burdens on reporting entities*”. Collectively these demonstrate that considerations other than demonstrated low risk are taken into account when granting exemptions.

A2

## NATIONAL AML/CFT POLICIES AND COORDINATION

presents a high threat (including potentially in relation to transactions below AUD 2 000), and the exemption applies regardless of the number of transactions or amounts gambled. Similarly, the thresholds set for stored value cards, which are based on a risk assessment, combined with the absence of an explicit requirement in relation to structuring, do not seem in line with the NTA assessment, which identified these means of payment as providing criminal opportunities to move funds, including cross-border, and do not seem to factor in TF risk. Casinos and bullion dealers are the only two categories of DNFBPs subject to AML/CTF obligations under the current Australian regulation despite the high level of ML threat that professionals such as lawyers, accountants, trust and company service providers, etc. represent.<sup>10</sup> The NTA assessment also identified high value goods as high risk; only bullion dealers are covered by the AML/CTF Act. Moreover, there are no review mechanisms in place to ensure that the circumstances justifying the exemptions are still met.

a2.8. **Criterion 1.7 –** Australia identified in its NTA seven areas as presenting high ML risks (the banking system, money transfer businesses and alternative remittance services, the gaming sector, high-value goods, professionals, legal entity structures, cash intensive businesses) and one presenting potentially high ML risks (electronic payment systems and new payment methods). Yet, while the AML/CTF regime is reasonably well calibrated to focus on the risks in banking, remittance, and gaming sectors, the authorities have not demonstrated that it addresses all of the remaining identified high risks. More specifically, there is no requirement on reporting entities to take enhanced measures in respect of transactions or customers associated with higher risks identified by the authorities, nor any requirement that those higher risks be incorporated into the risk assessments conducted by FIs and DNFBPs. Chapter 15 of the AML/CTF Rules only requires regulated entities to apply enhanced due diligence measures to risks that they identify themselves and not those identified by the country – e.g. in the NTA or NRA. Also, the wording of the rules leaves open the possibility that reporting entities may not apply enhanced or specific measures for higher risk activities identified in the FATF Recommendations. Some of the measures prescribed are not enhanced measures, but instead regular due diligence measures (see criterion 10.17).

a2.9. **Criterion 1.8 –** The authorisation for reporting entities to take explicit simplified measures in the AML/CTF Act is limited to certain CDD measures under the AML/CTF program requirements, and requires the existence of appropriate risk-based systems and controls based on a proper assessment of risk in accordance with the AML/CTF program requirements (e.g. see Paragraphs 4.3.8 and 4.4.8 of the AML/CTF Rules in relation to simplified verification requirements for companies and trusts). In addition, there is a broad discretion about how and in what circumstances those obligations need to be discharged (e.g. Paragraph 8.1.3 of the AML/CTF Rules “*some requirements... may be complied with by a reporting entity putting in place appropriate risk-based systems and controls*”). There are also safe harbour provisions setting out what amounts to “simplified” CDD procedures for both “low” or “medium” risk customers. Rule 4.1.3 lists customer type, service provided, delivery channel, and foreign jurisdiction as mandatory areas to consider when identifying ML/TF risk. Nonetheless, the discretion left with reporting entities (whether to determine customer risk levels and thus access the “safe harbour” provisions, or the extent of the measures that they put in place, which could, in practice, be simplified compared to the full requirements of the FATF standard), is not premised on any requirement that it be based on low risk only or be consistent with the country’s assessment of the ML/TF risks. In fact, reporting entities are not required anywhere in the Rules to consider the risks already identified by the jurisdiction.

a2.10. **Criterion 1.9 –** AUSTRAC applies a risk-based approach to the supervision of financial groups, in particular those *core principles institutions* and those operating within a DBG or providing services as a remittance network provider. While bullion dealers and casinos are supervised by AUSTRAC, other DNFBPs, (most of which are identified as high risk in the NTA) are not subject to AML/CTF obligations, and therefore not monitored by competent authorities or self-regulatory bodies. AUSTRAC supervises entities subject to AML/CTF obligations on a risk sensitive basis which includes assessment for those classified as high risk of their policies, practices, systems and controls in place to address their ML/TF risks. Thus, a large number of FIs and DNFBPs are supervised on a lesser basis or not at all in relation to their obligations under Recommendation 1.

10 See NTA.

a2.11. **Criterion 1.10** – Reporting entities (except financial advisers and planners) are required under sections 84-86 and 165 of the AML/CTF Act and Parts 8.1 and 9.1 of the AML/CTF Rules to produce a written program to identify, mitigate, and manage their ML/TF risks. This includes having regard to the nature, size and complexity of its business and the type of ML/TF risk that it might reasonably face. There is an implicit requirement to provide risk information to the authorities, because a copy of the program must be provided to AUSTRAC to help rectify any situation of non-compliance. Financial advisers and planners need only have a program that details customer identification procedures and do not need to otherwise assess ML/TF risks. However, many DNFBPs identified in the NTA as presenting a high threat are not reporting entities and thus not subject to this obligation (e.g. accountants, lawyers, trust and company service providers, dealers in precious metals and stones, and real estate agents).<sup>11</sup>

a2.12. **Criterion 1.11** – The programs mentioned above must be approved by the Boards or senior management of reporting entities (Parts 8.4 and 9.4 of the AML/CTF Rules) and require ongoing monitoring and updating in response to changes in ML/TF risks (Paragraphs 8.1.5, 8.4, 9.1.5, and 9.4 of the AML/CTF Rules). The programs must also contain a section on implementing enhanced CDD when the reporting entity identifies situations of high risk, or forms a suspicion of ML/TF, or when it is dealing with a prescribed foreign country (Paragraphs 15.8 and 15.9 of the AML/CTF Rules). However, as above, these requirements only apply in a limited way for financial advisers and planners and not at all for those DNFBPs identified in the NTA as presenting a high threat.

a2.13. **Criterion 1.12** – While simplified measures are allowed only if lower risks have been identified and in the absence of any suspicion of ML or TF (as suspicion requires that enhanced measures be applied - see Paragraph 15.9(2) of the AML/CTF Rules), as elaborated above, not all of the requirements of criteria 1.9 to 1.11 have been met.

### *Weighting and Conclusion*

a2.14. Australia uses many processes to identify and assess its ML/TF risks that generally result in a reasonable portrayal of those risks. Australia's NTA was a good first attempt to identify and assess ML risks, but suffers from limitations that likely mean that most main but not all ML risks were identified, nor properly assessed. Efforts to evolve thinking on the ML risks since the NTA have helped address some limitations and the authorities recognise that remaining gaps need to be addressed. The scope of assessments, including the next NTA, and information used needs to be broadened to assess other potential major risks such as customer types and incoming laundered proceeds. Engaging the private sector for input could also strengthen future assessments. The NRA used a more up to date methodology and does identify and assess the TF risks and is current. The AML IDC uses the NTA and NRA to set annual risk-based priorities that guide the work and resource allocation of its member agencies on AML/CTF matters. Australia's risk-based approach to AML/CTF regulation grants regulated entities exemptions and provides for some simplified measures that are not based solely on a proven low risk of ML or TF, or the need to be consistent with the NTA or NRA. In addition, a key moderate shortcoming is that many high risk entities and services identified in the NTA are not regulated under Australia's AML/CTF regime. Those 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. AUSTRAC primarily supervises entities it classifies as high risk to see that they are meeting obligations to identify, assess, and mitigate ML/TF risks. **Recommendation 1 is rated partially compliant.**

A2

### **Recommendation 2 - National Cooperation and Coordination**

a2.15. Australia was rated largely compliant with the previous Recommendation 31. The assessment identified the scope to improve the level of cooperation and coordination between AUSTRAC, APRA and ASIC,

---

11 Some may provide designated services akin to being a financial institution under the FATF Recommendations, and have AML/CTF Act obligations for that particular service, but they will not have such obligations for the list of activities applicable to them as DNFBPs under the FATF Recommendations.

## NATIONAL AML/CFT POLICIES AND COORDINATION

and also to enhance co-ordination at the policy level, possibly through the establishment of a formal national co-ordination mechanism. Recommendation 2 is now more specific about the need for countries to have national AML/CFT policies that encompass identified risks and for coordination to be more formalised.

a2.16. **Criterion 2.1** – The nearest thing that Australia has to a national set of policies and strategies for combating ML/TF informed by the risks identified is the annual work plan of the AML IDC, which combines the views and priorities of its member agencies. While it references the NTA, but not yet the NRA, in a few places, most issues in the plan are driven by considerations not related directly to combating ML or TF; those that are, focus mainly on preventive measures only. Plans and strategies of a range of agencies and task forces both support the AML IDC work plan and inform its development, and some of these are more directly related to combating the ML/TF risks identified in the NTA and NRA. In addition, other government initiatives, such as those that target certain aspects of mainly organised crime also deal with AML. The NOCRP is part of the national framework for combating organised crime. The first NOCRP details strategies for national and multi-jurisdictional approaches to key risks within the organised crime environment – and while it identifies ML as a key enabler of organised crime, it does not really articulate a policy or strategy for combating it. TF risks are addressed both as part of AML/CFT policy and national security and counter-terrorism strategy as appropriate.

a2.17. **Criterion 2.2** – The Attorney-General's Department (AGD) is responsible for national AML/CFT policy.

a2.18. **Criterion 2.3** – Australia has mechanisms in place to co-ordinate domestically on AML/CFT policies and activities:

- On policy matters, the AGD chairs the AML IDC, which meets three times each year to share information and inform the strategic direction and priority setting of federal agencies working on domestic AML/CFT initiatives. Other agencies represented include AUSTRAC, the AFP, the ACC, DFAT, the ACBPS, the Treasury, the ATO and the CDPP. In addition, Australia uses other inter-departmental fora to coordinate policy on matters relevant to combating ML/TF (e.g. the Heads of Operational Commonwealth Law Enforcement Agencies (HOCOLEA) – meets twice a year and serves as the primary forum for 14 federal agencies to discuss law-enforcement policy issues). CTF policy is also coordinated through broader counter-terrorism coordinating bodies, led by the Australia-New Zealand Counter-Terrorism Committee.
- Operational activities are coordinated using a mixture of standing committees and task forces with representation from federal and State and Territory agencies as necessary. A key committee is the ACC Board. The Board determines, among other things, national criminal intelligence priorities and special operations and investigations. A particular feature is the use of task forces targeting specific areas of concern where laundering activity is involved, such as the remittance sector (Eligo National Task Force), criminal gangs (Task Force Attero), serious and organised investment fraud (Taskforce Galilee), and asset confiscation (federal Criminal Assets Confiscation Task Force). There is also the multi-agency TFIU. Criminal intelligence is also coordinated via the ACC National Criminal Intelligence Fusion Capability, with input also from AUSTRAC.
- In addition, AUSTRAC hosts an annual forum with key agencies to shape its annual FIU Intelligence Strategy. More generally, to facilitate operational cooperation, AUSTRAC provides online access to its transaction reports database to all its partner agencies and posts liaison officers in some. In addition, Joint Management Groups (JMGs) operate in each State and Territory to help coordinate operational interaction with federal agencies. Since the last evaluation, both APRA, the prudential regulator, and ASIC, the market integrity and consumer protection regulator, have been added as designated agencies with whom AUSTRAC can share information, thus creating a mechanism for operational coordination on supervisory matters.

A2

a2.19. **Criterion 2.4** – DFAT chairs and services a number of counter-proliferation coordination groups, both at the senior policy level and the working level.<sup>12</sup> These groups bring together all relevant government agencies, including the intelligence community, to share information and coordinate responses to current proliferation issues, including proliferation financing. Meetings are scheduled monthly but can be convened at short notice if needed for operational or policy purposes.

### *Weighting and Conclusion*

a2.20. While Australia does not have a formalised AML/CFT policy that draws on risks identified in the NTA and NRA, it does have an agency that is responsible for national AML/CFT matters. Australia also has many standing committees and task forces in place to coordinate domestically on AML/CFT policies and activities within the federal government (on policy matters), and between the federal and State/Territory levels of Government (on operational matters). Moreover, the NTA and NRA risks get included in some other mainly criminal justice policy initiatives (e.g. the NOCRP). It is worth noting that the coordination efforts encompass State and Territory agencies, which is salient as Australia is a federation. Australia also has coordination mechanisms to combat PF. **Recommendation 2 is rated largely compliant.**

## **Recommendation 33 - Statistics**

a2.21. Australia was rated largely compliant with the previous Recommendation 32. The assessment identified that there was a lack of State or Territory statistics on prosecutions and convictions for ML, no clear statistics on ML/TF investigations at the Commonwealth level, nor adequate statistics on ML/TF investigations at the State or Territory level. While the language of Recommendation 33 has not changed, this Recommendation has taken on more relevance in the context of assessing effectiveness.<sup>13</sup>

a2.22. **Criterion 33.1** – The authorities maintain that the effectiveness and efficiency of Australia's AML/CFT systems are supported by statistics gathered by the FIU, regulators, police and prosecution services, and the ACA (within the AGD). AML/CFT related statistics are maintained comprehensively in some areas (e.g. for AUSTRAC operations), and other data are available or can be produced upon request for some agencies in the AML/CFT system. However, overall, Australia does not maintain a sufficiently comprehensive set of statistics to enable a full appraisal of its AML/CFT systems. In particular, national level information about prosecutions, convictions, and confiscations is not easily collated. Primary attention is paid to counts of various outputs. Other than for AUSTRAC, few maintained statistics focus on the efficiency of the AML/CFT systems. The authorities are also challenged to provide breakdowns of the data that they do hold. Coverage for specific types of statistics is as follows:

- STRs received and disseminated: AUSTRAC maintains a wide range of statistics about SMRs, many of which they publish in the AUSTRAC annual report.
- ML investigations, prosecutions and convictions: Australia does not maintain comprehensive national statistics on all these matters. The assessors were provided statistics on ML investigations by only some States and none at the federal level. Statistics for ML prosecutions and convictions were obtained at the federal, State and Territory level, but the authorities do not maintain national

12 The key Counter-Proliferation Coordination Group comprises: DFAT (Chair), Department of Prime Minister and Cabinet, Department of Defence, AGD, the ACBPS, the Australian Intelligence Community agencies, and other agencies co-opted as necessary.

13 For the assessment of Australia only, the use of the words “comprehensive” and “includes” in R.33 are collectively interpreted as requiring countries to have, as a minimum, statistics (not just data) covering all of the areas listed and which are accurate, national, covering at least three annual time periods, that present some value as well as volume data, and that are also in disaggregated form to show such things as reporting entity types, predicate crime type, country of origin, and type of ML activity as appropriate. “Maintain” and “keep”, are interpreted as indicating that the statistics are readily available. FATF is still considering its approach to R.33 in light of its latest Methodology.

A2

## NATIONAL AML/CFT POLICIES AND COORDINATION

aggregated statistics. Those provided used different bases and time periods, preventing accurate aggregation. The assessors had to compile the data provided or obtained into national level data. Moreover, it was not possible to obtain disaggregated prosecution and conviction data by reference to the associated predicate crime, and reliable national sentencing data for ML convictions does not exist.

- TF investigations, prosecutions and convictions: Comprehensive national statistics on TF prosecutions and convictions, but not on investigations, are available.
- Property frozen, seized, and confiscated: Australia is challenged to compile nationally aggregated statistics on these matters, due mainly to the different ways in which federal and State/Territory agencies maintain their own statistics – and not all States or Territories were able to provide data. The statistics produced allowed for disaggregation back to underlying predicate crimes in only some limited areas. Tax crime related confiscation data is available. Comprehensive statistics on illicit drug seizures are available at the national level.
- MLA or other international requests for cooperation made and received: Australia maintains some comprehensive statistics on AML/CTF related MLA, but is unable to track the timeliness of response and the nature of underlying predicate crime. Only AUSTRAC maintains statistics on AML/CTF related international cooperation requests.
- Other statistics: AUSTRAC maintains a broad range of statistics related to its regulatory and supervisory role (including on enrolment of reporting entities and registration of remittance dealers, its compliance assessment activities, and enforcement action). However, it was challenged to provide comprehensive and consistent statistics on the nature, structure, and size of the financial and DNFBP sectors, and many data sets are challenging to use to assess the efficiency or effectiveness of the regulatory/supervisory system as they are compiled differently.

### *Weighting and Conclusion*

a2.23. While Australia produces many statistics on AML/CTF matters for various parts of its system, it is often challenged to produce statistics at the national level. The statistics most readily available came from AUSTRAC and the AGD (in relation to MLA requests and extradition requests), and on TF prosecutions and convictions, all of which relate to centralised national AML/CTF functions. However, a concern is that 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. **Recommendation 33 is rated largely compliant.**

A2

### 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

#### Recommendation 3 – Money laundering criminalisation

a3.1. Australia was rated largely compliant for Recommendation 1 and Recommendation 2 (ML offence). The main shortcomings that were noted at the time related to lack of effectiveness, and the less than compliant (implementation of the) criminalisation of ML at the State and Territory level. ML is criminalised at the federal and the State/Territory level. This section focuses primarily on the federal level.

a3.2. **Criteria 3.1 and 3.11** – ML is criminalised under Division 400 of the federal *Criminal Code Act 1995* (the Criminal Code, or CC). Vienna Article 3(1) (b) and (c) and Palermo Article 6(1) have been implemented (section 400.2 CC covers receipt, possession, concealment, disposal, import, export and engaging in banking transactions, which also covers transfer, conversion , disguising, and acquisition). Participation, association or conspiracy, aiding and abetting, counselling or procuring, incitement and conspiracy are all covered under part 2.4 of the CC (attempt, complicity and common purpose, joint commission, commission by proxy, incitement and conspiracy). Knowledge is required (beliefs, recklessness or negligence), although section 400.9 CC separately criminalises "dealing in property reasonably suspected to be proceeds of crime".

a3.3. **Criteria 3.2 and 3.3** – The CC applies a threshold approach, with predicate offences for ML comprising all indictable offences—i.e. those offences whose penalty is a minimum of 12 months imprisonment (section 400.1 CC and section 4G *Crimes Act 1914*). An extensive overview was provided by the authorities, a sufficient range of offences within each of the categories of offences are criminalised under Australian criminal law, either at the Commonwealth level, or at the State level/Territory. Federal predicate offences are predicates for the federal ML offence, and State/Territory predicate offences are predicates for State/Territory and federal ML offences.

a3.4. **Criterion 3.4** – The definitions of 'proceeds of crime' and 'property' in section 400.1 CC extend to any money or other property that is wholly or partially derived or realised, directly or indirectly, by any person from the commission of an offence that may be dealt with as an indictable offence. Property is defined as real or personal property of every description, whether situated in Australia or elsewhere and whether tangible or intangible, and including an interest in any such real or personal property. This includes financial instruments, cards and other such items regardless of whether they have intrinsic value.

a3.5. **Criterion 3.5** – Section 400.13 CC explicitly provides that the prosecution does not need to establish that a particular offence has been committed, or that a particular person committed an offence in relation to the money or property, in order for those assets to be considered proceeds of crime. The prosecution must, however, prove beyond reasonable doubt that the proceeds are either the proceeds of a crime, or are intended to become, or are at risk of becoming, an instrument of crime.

a3.6. **Criterion 3.6** – The definitions of "proceeds of crime" and "instruments of crime" both cover crimes against laws of a foreign country.

a3.7. **Criterion 3.7** – Sections 400.1 and 400.2 CC formally apply to persons that commit the predicate offence. However, case law has limited the ability to charge both for the predicate offence and for self-laundering where the criminality of the ML offence is completely encompassed by the criminality of the predicate offence (e.g. the decisions of the New South Wales Court of Criminal Appeal in *Nahlous v R* (2010) 2011 ACrimR 150; *Thorn v R* (2010) 198 ACrimR 135; *Schembri v R* (2010) 28 ATR 159). This has led to the issuing of a litigation instruction (number 10 of May 2013) that restricts the use of the self-laundering provisions in line with case law.

a3.8. **Criterion 3.8** – Intent and knowledge (belief, recklessness, negligence) must normally be proven (sections 5.2 and 5.3 CC) but can be inferred from objective factual circumstances. Under section 400.9 CC (reasonably suspected proceeds), a range of possible examples of such circumstances is given which will satisfy the offence provision. Section 400.9 carries a lower penalty. All other sections require knowledge and

A3

## LEGAL SYSTEM AND OPERATIONAL ISSUES

intent to be proven. Absolute liability applies to the value of the property laundered, but mistake of fact as to the value of the property can be a defence to the particular offence charged (but not the lesser offence).

a3.9. **Criterion 3.9** – CC Division 400 provides for different charges for different monetary thresholds (amounts involved), with the maximum penalties also differing depending on the level of fault (intention, knowledge, recklessness, negligence and reasonable suspected proceeds). This allows for proportionate sanctioning. Sanctions for natural persons range from 25 years imprisonment and/or AUD 255 000 (intentionally laundering AUD 1 million or more), to a fine of AUD 1 700 (negligence, laundering less than AUD 1 000). These sanctions are dissuasive.

a3.10. **Criterion 3.10** – Part 2.5 CC sets out the general principles, physical and fault elements of corporate criminal responsibility. Section 12.1 provides that the Criminal Code applies to bodies corporate in the same way as it does to natural persons (the term corporate body means legal person), and section 4B of the Crimes Act enables a fine to be imposed for offences that only specify imprisonment as a penalty. Section 12.3 indicates that to prove intention, knowledge or recklessness, the fault element must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence. This could be done by proving that the body corporate's board of directors, or high managerial agent, intentionally, knowingly or recklessly carried out the relevant conduct, or expressly, tacitly or impliedly authorised or permitted the commission of the offence; proving that a corporate culture existed within the body corporate that directed, encouraged, tolerated or led to non-compliance with the relevant provision; or proving that the body corporate failed to create and maintain a corporate culture that required compliance with the relevant provision.

a3.11. Sentencing is based on a formula from imprisonment to financial penalty, all based on sections 4AA(1), 4B(2), and 4B(3) of the Crimes Act. This means that the maximum penalties for legal persons under Division 400 of the CC range from a fine of AUD 1 275 000 (intentionally laundering AUD 1 million or more) to AUD 8 500 (negligent laundering less than AUD 1 000).

### *Weighting and Conclusion*

a3.12. **Recommendation 3 is rated compliant.**

## **Recommendation 4 - Confiscation and provisional measures**

a3.13. In its 3<sup>rd</sup> assessment, Australia was rated compliant for Recommendation 3 (confiscation and provisional measures). Most confiscation action is brought under the *Proceeds of Crime Act 2002* (POCA), although each State and Territory has its own complementary system. This section focuses primarily on the federal level.

A3  
a3.14. In addition to what is required by Recommendation 4, authorities can also issue non-conviction based forfeiture orders which are decided upon a civil standard and directed at persons, property, or equivalent value (sections 47, 49 and 116 POCA). Property-based civil forfeiture orders apply to any suspected indictable offence, foreign offence, or offence of "Commonwealth concern", while those directed at a person or equivalent value can be applied for a suspected "serious offence" (defined as an indictable offence punishable by 3 or more years' imprisonment plus other conditions). Finally, unexplained wealth orders (section 179A-T POCA) could be issued that would require a person to pay an amount equal to a portion of the person's total wealth if the person cannot satisfy the court that the money is not derived from certain offences.

a3.15. **Criterion 4.1** – The POCA has broad provisions to confiscate (referred to as "forfeiture" in POCA) proceeds of crime. Part 2-2 (section 48) covers conviction-based forfeiture orders that apply to all indictable offences (i.e. those with 1 year imprisonment or more), which includes ML, TF, and predicate offences. Corresponding value is also covered through Part 2-4 POCA (section 116), where a pecuniary penalty order (fine) can be issued for the value of the benefits from the unlawful activity. POCA (section 329) defines proceeds and instruments of crime. Property is proceeds of an offence, located anywhere, if it is wholly or partially, directly or indirectly derived or realised from the commission of an offence. Property is an instrument of an offence if the property, located anywhere, is used or intended to be used in, or in connection

with, the commission of an offence. Property remains proceeds or instrumentality of crime even after transfer or exchange, except when the property is acquired by a bona fide third person or is inherited (section 330).

a3.16. **Criterion 4.2** – Provisional measures are covered under Parts 2-1A (freezing orders, which apply to financial accounts) and 2-1 POCA (restraining orders, which apply to property) and can be executed on the basis of a reasonable suspicion or conviction. Property can be restrained when a person is charged with an indictable offence (section 17), suspected of committing a serious offence (section 18), or when property is suspected to be the proceeds of an indictable offence (section 19). In addition to the regular investigative measures that are used to investigate offences and that can lead to the application of provisional measures and confiscation (see Recommendation 31), Chapter 3 POCA provides for examination orders, production orders (also for financial institutions relating to accounts and transactions, also over particular periods, and search and seizure of tainted property or evidential material). Section 36 of POCA enables the court to set aside a disposition or dealing with property, which contravenes a restraining order when that disposition or dealing was either not for sufficient consideration or was not in favour of a person acting in good faith.

a3.17. **Criterion 4.3** – Rights of bona fide third parties are protected through sections 29 and 29A POCA, which enable a person whose property is the subject of a restraining order to have his or her property excluded from that order. Sections 69, 72, 73, 77, 81, 94, 94A, 99, 107, and 179L of POCA are also relevant.

a3.18. **Criterion 4.4** – Chapter 4 POCA contains the procedural provisions relating to the management of property, the provision of legal assistance and how confiscated property can be used. The Australian Financial Security Authority (AFSA) is responsible for securing, managing and realising restrained property. Part 4-1 sets out the powers and duties of AFSA which include how it may deal with controlled property. All confiscated money, and the funds derived from the sale of confiscated assets, is placed into the Confiscated Assets Account which is managed by AFSA. Money and assets that are forfeited can only be used for purposes specified in POCA (shared with other jurisdictions in case of joint investigations, the States or Territories). Funds can also be used for local crime prevention, law enforcement, drug treatment and diversionary measures.

### *Weighting and Conclusion*

a3.19. **Recommendation 4 is rated compliant.**

## Operational and Law Enforcement

### Recommendation 29 - Financial intelligence units

a3.20. Australia was rated compliant for Recommendation 26 (FIU). Since Australia's last mutual evaluation, the FATF Standards on FIUs have been significantly strengthened by imposing new requirements which focus, among other issues, on the FIU's strategic and operational analysis functions, and the FIU's powers to disseminate information upon request and request additional information from reporting entities.

a3.21. Australia's FIU is AUSTRAC established in 1989 under the *Financial Transaction Reports Act 1988* (FTR Act) and from 2006 by the AML/CTF Act. AUSTRAC's role as an FIU is discussed under R29. Other functions that AUSTRAC exercises (such as supervision) are discussed elsewhere. The key piece of legislation for AUSTRAC is the AML/CTF Act. However, the FTR Act remains in force as long as its provisions do not contradict the provisions of the AML/CTF Act.

a3.22. **Criterion 29.1** – The AML/CTF Act confirms the establishment and functions of AUSTRAC. AUSTRAC's functions are: "to retain, compile, analyse and disseminate eligible collected information" (sections 209, 210, and 212). "Eligible collected information" comprises all types of reports that reporting entities are required to file with AUSTRAC, as well as other information that AUSTRAC obtains from government bodies and reporting entities upon request.

A3

## LEGAL SYSTEM AND OPERATIONAL ISSUES

a3.23. **Criterion 29.2** – AUSTRAC is the central agency for the receipt of disclosures filed by reporting entities under both AML/CTF Act and FTR Act. These disclosures include reports of suspicious matters (SMRs), reports of threshold transactions, reports of , IFTIs, compliance reports, reports about physical currency and bearer negotiable instruments (see subsections 41(2), 43(2), 45(2), 47(2), 53(8) and 55(5)), as well as reports obliged under the FTR Act-significant cash transactions by cash dealers, reports of significant cash transactions by solicitors, and reports of suspect transactions (SUSTRs) (see sections 3, 7, 15A, and 16).

a3.24. **Criterion 29.3** – Section 49(1) of the AML/CTF Act enables AUSTRAC to collect further information from any reporting entity or even any other persons (legal or natural) once an SMR has been filed by a reporting entity. This goes beyond the standard, which only requires that FIUs can obtain and use additional information from any reporting entities. Other databases are not integrated into AUSTRAC's analytical tool (except for the electoral role). AUSTRAC can gather information from the AFP, ACBPS, ACC, Immigration and public company information database (including the public ASIC database database), other commercial services (including World Check) and State/Territory Police where AUSTRAC staff are posted.

a3.25. **Criterion 29.4** – AUSTRAC's Operations Division is responsible for both operational and strategic analysis. Concerning operational analysis, AUSTRAC employs automated analysis systems to categorise reports of suspicious matters based on a series of rules which are defined and continually reviewed by AUSTRAC in collaboration with its partner agencies. These rules enable AUSTRAC's automated system to identify those reports which relate to specific key risks, for potential further analysis by AUSTRAC (intelligence reports). Intelligence reports are shared with other agencies, spontaneously or upon request. Partner agencies also have direct access to all information in the AUSTRAC database (all types of reported transactions and intelligence reports) and can undertake their own searches or analysis. Concerning strategic analysis, the Operations Support Branch has a dedicated strategic analysis section which includes a typologies team. The typologies team uses data mining technology to develop ML/TF typologies, sanitised case studies, ML/TF indicators, and reporting summaries. Strategic intelligence reports can be used by AUSTRAC business units and by partner agencies for any purpose. The strategic analysis team also produced the NTA and NRA.

a3.26. **Criterion 29.5** – Section 212 (1) of the AML/CTF Act provides the functions of the AUSTRAC CEO which includes disseminating “eligible collected information” (i.e. information received by AUSTRAC). As partner agencies have on-line full access to AUSTRAC's database ('SMRs and analysis) and also use the AUSTRAC analysis tool, dissemination of information is technically not as important as it would be in other countries (sections 125 - 133C AML/CTF Act). Access to the database and disseminations are based on the Australian Protective Security Policy Framework (PSPF, see below). The Egmont Secure Web system is used for international disseminations. The AUSTRAC database tracks all access by each user

A3  
a3.27. **Criterion 29.6** – AUSTRAC protects its information as follows: section 121 of the AML/CTF Act prohibits the disclosure of AUSTRAC information except in cases specified in the legislation. Additionally, the aforementioned PSPF sets detailed requirements for governance, staff members' protective security roles and responsibilities, risk management elements including security vetting, and information asset classification and control, including for AUSTRAC. AUSTRAC has also internal policies for employees who have an obligation to manage and protect the records they create and/or receive in the course of business. Employees are required to ensure that records are retained, classified, and filed according to the provisions of the AUSTRAC Information Management Policy (IMP). The IMP outlines procedures for handling and storage of AUSTRAC information, whilst the AUSTRAC Information Security Policy outlines procedures for securing information, security classification and protective markings, dissemination limiting markers, handling, access and control. All AUSTRAC employees are subject to a security vetting process undertaken by the Australian Government Security Vetting Agency (AGSVA). AUSTRAC's personnel security policy determines that AUSTRAC must also identify designated security assessment positions within the agency that require access to official information and assets. Information security is maintained within AUSTRAC's risk management framework. There are designated IT units that have responsibility to develop, implement, and maintain the security of all AUSTRAC services, in cooperation with AUSTRAC's security advisor. Physical access to AUSTRAC building facilities is also limited to appropriately cleared staff.

a3.28. **Criterion 29.7** – AUSTRAC is established as a statutory authority within the Attorney-General 's Department's Portfolio. The powers and functions of AUSTRAC are set out in detail in Part 16 of the AML/CTF Act. The legal and institutional framework does not grant full operational independence and autonomy,

to allow for accountability to Parliament. The AML/CTF Act provides a reserve capacity for the Minister to issue written policy principles and directions to the AUSTRAC CEO, which the CEO has to comply with (section 213 AML/CTF Act). These written policy principles can relate to any issue but not to a specific case (section 228(2) AML/CTF Act) and must be tabled in Parliament (sections 213(2) and 228(5) AML/CTF Act). AUSTRAC can make arrangements for information exchange with domestic competent authorities and foreign counterparts. AUSTRAC is an independent body and has its own distinct structure and core functions. AUSTRAC has its own operational resources, including financial budget and staff, allocated through the normal governmental processes. Once allocated, there are no specific provisions that would require further approvals from government or partner agencies to obtain and deploy the resources needed to carry out its functions. There is a general consultation requirement; however, any failure to consult in relation to the performance of a function does not affect the decision taken.

a3.29. **Criterion 29.8** – AUSTRAC is a founding and active member of the Egmont Group, and served as Chair of the Egmont Committee in 2008-2009.

### *Weighting and Conclusion*

a3.30. The power of the minister to provide written policy principles or instructions to AUSTRAC is a limitation to the operational independence and autonomy of the FIU and a technical shortcoming. Because the assessors are of the view that the instruction powers cannot be used in practice because of likely public disapproval, it is a shortcoming that should not have an effect on the overall compliance. Australia is also to be commended for providing AUSTRAC with the legal tools to be able to obtain and use additional information from any other natural or legal person, which goes beyond the FATF requirement to obtain information from reporting entities. **Recommendation 29 is rated compliant.**

## **Recommendation 30 – Responsibilities of law enforcement and investigative authorities**

a3.31. In its 3rd assessment, Australia was rated largely compliant for old Recommendation 27 (law enforcement authorities). The deficiency related to effectiveness, which is not assessed in this section under the 2013 Methodology. The new Recommendation 30 contains much more detailed requirements.

a3.32. **Criterion 30.1** – The AFP is the primary law enforcement agency for the investigation of federal offences, including ML associated predicate offences, and TF. The *Australian Federal Police Act 1979* (AFP Act) establishes the AFP which is the federal police force (section 8 AFP Act), chiefly responsible for federal crimes, and its functions also include the investigation of State/Territory offences that have a federal aspect (section 4AA AFP Act). A State offence may be identified as having a federal aspect where it potentially falls within federal legislative powers because of the elements of the State offence or the circumstances in which it was committed, or because the investigation of that State offence is incidental to an investigation of a federal or Territory offence.

a3.33. The AFP had three permanent Money Laundering Short Term Teams. First established in January 2012, these teams focused solely on ML investigations. One team was merged into a general crime squad before the on-site, one team was merged with a joint task force on alternative remittance (Eligo National Task Force), and the third team is still in place (7 staff in Melbourne). State and Territory police forces also have responsibility for investigating ML offences set out in State legislation.

a3.34. The AFP also has a dedicated TFIU to focus on TF investigations, intelligence, education and liaison. The TFIU is a multi-agency unit and includes representatives from a number of Commonwealth and State Government agencies.

a3.35. In addition, The *Australian Crime Commission Act 2002* (the ACC Act) establishes the ACC, mainly a law enforcement intelligence agency. The functions of the ACC include the investigation, when authorised by the ACC Board, of matters relating to federally relevant criminal activity (section 7A ACC Act). The ACC uses its coercive powers in collaboration with its partner agencies: it does not conduct investigations into criminal activity on its own since its role is primarily to be the national criminal intelligence hub and not

A3

## LEGAL SYSTEM AND OPERATIONAL ISSUES

a supra-national police force. The ACC Board (which includes the heads of federal, State and Territory law enforcement agencies) approves Special Investigations and Special Operations in which the ACC may use coercive examination powers (set out in Division 1A and 2 of Part II of the ACC Act). The ACC's far-reaching coercive powers means it has broader investigative powers than those available to the police forces and it operates in effect as a standing Royal Commission. ML is relevant to ACC investigations, such as the current Targeting Criminal Wealth Special Investigation.

a3.36. **Criterion 30.2** – AFP and State and Territory Police investigators are authorised to undertake both predicate and ML investigations in tandem or individually depending on the nature and desired outcomes of the particular investigation. However, this is not the case for Queensland where there is a legal requirement for the DPP to request the Queensland Attorney General to authorise a ML prosecution.

a3.37. **Criterion 30.3** – The bodies described above have the authority to identify, trace, and initiate the freezing and seizing of property. In addition, the AFP-led CACT conducts investigations and litigation arising from the POCA (POCA) and is responsible for the majority of POCA work. The CACT has the ability to identify and pursue criminal assets and also works in partnership with relevant Commonwealth, State, Territory and international law enforcement agencies to identify, investigate and litigate appropriate asset confiscation matters at the federal level.

a3.38. **Criterion 30.4** – Australia recognises tax and social security fraud as an ML predicate offence. Regarding tax, the ATO has the primary responsibility for investigating tax evasion and tax fraud and conducts both (civil) audits and (criminal) investigations of taxation-related matters. The ATO undertakes investigations either of its own accord, or with partner law enforcement agencies, or in multi-agency task force operations (for example Project Wickenby). The ATO investigators have recourse to a number of Acts which impose criminal sanctions (*Tax Administration Act 1953*, *Crimes (Taxation Offences) Act 1980* and the CC). Where a tax-related matter intersects with an associated non-tax related offence (e.g. drug-trafficking), the investigation would be considered 'serious and/or complex' and the ATO will liaise with the AFP and CDPP to coordinate the various aspects of such an investigation. However, the ATO investigators do not conduct 'stand-alone' (i.e. without a predicate tax offence) ML investigations as these are the responsibility of the AFP and ATO's scope is somewhat limited. The ATO investigators are required to be qualified in accordance with "Australian Government Investigation Standards" and are able to prepare complex briefs of evidence for use in criminal court matters. Department of Human Services investigators have powers and procedures similar to the ATO, in order to focus on social security fraud.

a3.39. **Criterion 30.5** – In July 2014, the AFP launched the Fraud and Anti-Corruption Centre, responsible for operational fraud and anti-corruption efforts at the federal level. At the State level (but not at the federal level), independent anti-corruption bodies exist in New South Wales, Queensland, Western Australia, Victoria, Tasmania and South Australia. Like Royal Commissions, these bodies have extensive investigate and coercive powers. Cases may be referred to the (C)DPP.

### *States and Territories:*

A3

a3.40. Australia also provided extensive information for Recommendation 30 for the state level. In general, states follow the same model as the federal government, with one unified police force and a centralised DPP body.

### *Weighting and Conclusion*

a3.41. Besides the limitation in Queensland where the Attorney-General needs to authorise a ML prosecution, the responsibilities of law enforcement are sufficient. **Recommendation 30 is rated largely compliant.**

## **Recommendation 31 - Powers of law enforcement and investigative authorities**

a3.42. In its 3rd assessment, Australia was rated compliant for old Recommendation 28. In February 2010, existing relevant provisions in the Crimes Act were replaced with new regimes based on national model

legislation. The new Recommendation 31 contains much more detailed requirements in the area of law enforcement and investigative powers.

a3.43. **Criterion 31.1** – Australian authorities have authority to obtain information from financial and other institutions and seize and obtain evidence in law enforcement investigations of ML, TF, and predicate offences. State and Territory authorities have similar authority as that provided to the federal authorities under POCA and the Crimes Act. General information gathering powers pursuant to warrants in the Crimes Act can be utilised, as well as the specific information gathering power set out in section 49 of the AML/CTF Act. ACC also has the power to obtain documents (section 29 ACC Act 2002). POCA (section 213) requires financial institutions to provide any information or document relating to accounts and certain transaction information. For any other information held by financial institutions and for information held by anyone else (including DNFBPs), POCA section 202 allows a magistrate to issue a production order, requiring a person to produce one or more property-tracking documents to an authorised officer, or make one or more property-tracking documents available for inspection. POCA (section 225) also authorises a magistrate to issue a warrant to search premises (for evidence gathering). Similar general powers are available to investigate predicate offences (section 3E(1) Crimes Act). Ordinary and frisk search powers are available to officers (sections 228 POCA and 3E(2) and 3E(6)(b) Crimes Act). Tainted property and evidence can be seized (sections 228(1)(d) POCA) and 3E(6) and 3E(7) of the Crimes Act). The ACC may apply for a warrant to enable the search of premises and seizure of evidence (section 22 ACC Act). The ATO can use sections 263 and 264 of the *Income Tax Assessment Act 1936* to search premises and require people to provide information in tax related cases. The AFP and other law enforcement agencies can obtain witness statements in any matter when a witness is prepared to provide a statement. There is no legal basis necessary, as this is not a coercive power. A witness statement is not admissible as evidence in criminal proceedings (except in some limited situations where a witness has died or is not able to give evidence), but witnesses can be subpoenaed to go to court to give evidence. The ACC has the power to compel witnesses to give evidence on themselves and others under investigation.

a3.44. **Criterion 31.2** – The Crimes Act (Part IAC and 15KA and 15KB) authorises undercover operations and obtaining of evidence. The *Telecommunications (Interception and Access) Act 1979*, Parts 2-5, authorises the AFP, ACC, the Australian Commission for Law Enforcement Integrity, and State law enforcement agencies to intercept communications for investigations of a “serious offence”. This includes ML, terrorism, and TF, serious cartel offences, cybercrime offences, offences involving organised crime, murder, kidnapping, serious drug offences, and certain other offences punishable by at least seven years imprisonment. The *Surveillance Devices Act 2004* authorises Commonwealth and State and Territory law enforcement agencies to access computer systems for a “relevant offence”, i.e. offences punishable by three years imprisonment and certain other offences. The Crimes Act allows for controlled delivery operations (sections IAB, 15HA, and 15GE) involving a serious Commonwealth offence, which includes ML, terrorism and TF, and a number of other offences punishable by three years imprisonment. It is not clear whether this covers all predicate offences, unless the investigation also includes a ML offence.

a3.45. **Criterion 31.3** – While there are mechanisms in place to identify in a timely manner which natural or legal persons own or control a specific account, there is no (general) mechanism in place to identify in a timely manner whether specific natural or legal persons own or control accounts.

a3.46. **Criterion 31.4** – The competent authorities investigating ML, TF, and associated predicate offences are able to ask for all information collected and held by AUSTRAC. Subsection 126(1) of the AML/CTF Act allows the AUSTRAC CEO to designate officials or a class of officials to access this information. Forty-one authorities or agencies, including national security agencies and federal, State and Territory Police and Crime Commissions, are currently so designated.

### *Weighting and Conclusion*

a3.47. Law enforcement and investigative authorities generally have all the powers that they need to investigate ML/TF. However, 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). **Recommendation 31 is rated largely compliant.**

A3

### Recommendation 32 – Cash Couriers

a3.48. In the 2005 evaluation Australia was rated partially compliant on Special Recommendation IX. The main deficiencies identified were that (i) there was no system for declaration or disclosure of bearer negotiable instruments (BNIs) and, therefore, (ii) no sanctions for false declaration or disclosure relating to BNIs and (iii) no ability to stop or restrain BNIs in relation to a false declaration or disclosure. Recommendation 32 contains new requirements that were not assessed under the 2004 Methodology, but which are assessed under criteria 32.2 and 32.10 of the 2013 Methodology.

a3.49. **Criteria 32.1, 32.2 and 32.3** – Australia implements a combination of declaration (for cash) and disclosure (for BNI) systems for incoming and outgoing cross-border transportation of currency and BNIs. For cash (whether Australian or foreign), the AML/CTF Act requires a declaration for all physical cross-border movements above the threshold of AUD 10 000, whether by travellers or through mail and cargo. For BNIs, the traveller must, if required to do so by a police officer or a customs officer: (i) disclose whether or not the person has with him or her any BNIs; and (ii) disclose the amount payable under each BNI that the person has with him or her; and (iii) produce to the officer each BNI that the person has with him or her. The definition of the BNI is given in section 17 of the AML/CTF Act, in line with the FATF definition. The Outgoing Passenger Card contains a question for outgoing currency and BNI, and directs travellers to the related CBM-PC or CBM-BNI form. The Incoming Passenger Card contains the same questions; however, it does not inform passengers about the need to obtain CBM-PC or CBM-BNI (neither of which is easily available online) (sections 53, 55 and 59 AML/CTF Act).

a3.50. **Criterion 32.4** – Sections 199 and 200 of the AML/CTF Act authorise police and customs officers to require a person to declare or disclose currency and BNIs, search the person, and seize the currency or BNI. In case of a false/failure to declare/disclose, regular law enforcement powers will be used (see Recommendation 31).

a3.51. **Criterion 32.5** – If a person fails to make a declaration of currency (under sections 53 or 55), there are two types of sanctions available: civil or criminal. Under the civil penalty (section 186), the person is subject to a fine of (i) AUD 850 if the total amount of the physical currency involved in the alleged contravention is AUD 20 000 or more, or (ii) AUD 340 otherwise. Under the criminal penalty, the person is liable to imprisonment of 2 years or a fine of AUD 85 000, or both for failure to make a report. Sections 136 and 137 also provide for imprisonment of 10 years or a fine of AUD 1.7 million for (i) giving false or misleading information, or (ii) producing a false or misleading document to competent authorities, including the customs, the police and AUSTRAC. These provisions apply to information and documents in relation to cross-border movement of currency or BNIs. Overall, the sanctions envisaged under civil responsibility appear to be proportionate, but not dissuasive (a fine of AUD 850 is more than 20 times smaller than the amount of undeclared currency if it is more than AUD 20 000, for example). On the other hand, the sanctions under criminal responsibility appear to be dissuasive, but not proportionate as they are rather high.

A3

a3.52. **Criterion 32.6** – Declarations of physical currency have to be made either to AUSTRAC or a police or customs officer. That officer must forward the report to AUSTRAC within 5 business days (section 56 AML/CTF Act). Therefore, the FIU receives all declarations of physical currency transportation. BNI-disclosures are made available to AUSTRAC within 5 days (section 60 AML/CTF Act). Detected BNI-declaration failures require follow-up by AFP officers. AUSTRAC has access to AFP and ACBPS databases.

a3.53. **Criterion 32.7** – Domestic cooperation in relation to the cross-border transportation of currency and BNIs is based on a number of MOUs concluded between the ACBPS, Department of Immigration and Border Protection (DIBP) and AUSTRAC. In addition to that, AUSTRAC provides access to its information both to ACBPS and DIBP. The ACBPS also co-ordinates its efforts in monitoring cross-border activity with AFP and ACC, and also through liaison officers. ACBPS investigations that contain proceeds of crime elements and/or indications of ML are referred to the CACT within the AFP as a matter of course. ACBPS officers undertake customs as well as immigration checks at all ports of entry into Australia. Also, the Border Management Group (including with AUSTRAC) was established. It coordinates border security activities, including cash smuggling issues, across government agencies and is led by the ACBPS.

a3.54. **Criterion 32.8** – Subsections 199(5) and 199(10) of the AML/CTF Act allow competent authorities (the customs and the police) to seize physical currency (no specific time limit) where there is suspicion that it may afford evidence of a false declaration (under section 53). This provision is somewhat broader than the requirement under 32.8(b), as a mere suspicion of false declaration is sufficient to seize the currency. Subsections 200(12) and 200(13) provide for the seizure of BNIs where a person has made a false disclosure. In case of a suspicion of ML/TF, sections 199(3) - 199(5) allow customs to examine the traveller and his belongings, and seize currency. Section 200 has similar provisions for BNIs, and section 201 allows for an arrest warrant based on suspicion of ML/TF.

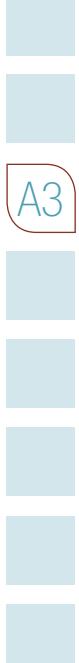
a3.55. **Criterion 32.9** – AUSTRAC is able to exchange information that it has access to with its foreign counterparts with whom it has an MOU or an exchange instrument.

a3.56. **Criterion 32.10** – For information security in relation to AUSTRAC: see Recommendation 29. These general government provisions equally apply to the ACBPS.

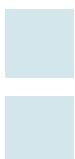
a3.57. **Criterion 32.11** – See criterion 3.9, Recommendation 4 and criterion 5.6.

### *Weighting and Conclusion*

a3.58. The lack of dissuasive and proportionate sanctions is a shortcoming, considering the overall risk profile of Australia. The attractiveness of the use of cash smuggling (caused by the tracking of every international wire transfer) and the abundance of typologies related to smuggled cash are risk factors taken into account in this conclusion. **Recommendation 32 is rated largely compliant.**



## LEGAL SYSTEM AND OPERATIONAL ISSUES



A3



## 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

### Recommendation 5 - Terrorist financing offence

a4.1. Australia was rated largely compliant for Special Recommendation II (criminalisation of terrorist financing). The main shortcoming at the time was that the collection of funds for a terrorist organisation and the collection or provision of funds for an individual terrorist, were not covered.

a4.2. **Criteria 5.1, 5.2, and 5.5** – Australia has criminalised TF, mainly on the basis of the TF Convention. Terrorist acts are defined in the CC under section 100.1, and section 103.1 criminalises the financing of these acts. Section 102.6 criminalises the financing of a criminal organisation, and section 103.2 targets the financing of a terrorist.

a4.3. Section 103.1 CC criminalises the collection or provision of funds (without specifying that this could be directly or indirectly) if the person is reckless as to whether the funds will be used to facilitate or engage in a terrorist act. Under section 100.1, an act has to meet three conditions to be considered a “terrorist act”: 1) it falls into a category of behaviours such as causing serious harm to a person or property, endangering another person’s life, creating a serious risk to public health or safety, interfering or disrupting an electronic system; 2) there is the intention of advancing a political, religious or ideological cause; and 3) there is the intention of coercing or intimidating the federal, State, Territory or foreign government or intimidating the public.

a4.4. In relation to the first condition, Australia did demonstrate how each of the acts in the Convention annex is criminalised in Australia. However, the acts must also meet the two additional intent elements to come within the Australian definition of terrorist act, whereas Article 2(1)(a) of the Convention requires that these should be considered as terrorist acts as described in the CT Conventions, and some of these Conventions do not allow terrorist intent to be a condition for a conduct to be considered terrorism (e.g. the theft of nuclear material should be considered terrorism no matter what the actual intent of the suspect is). The Australian definition of terrorist act does not cover all acts in Article 2(1)(b) of the CTF Convention (“any other act, intended to cause death or serious bodily injury...”) either, since the second condition above is not foreseen in Article 2(1)(b), and the third condition does not cover intimidating/influencing an international organisation as foreseen in Article 2(1)(b). Furthermore, subsection 100.1(3) clarifies that acts in relation to lawful advocacy, protest, dissent or industrial action are not terrorist acts unless they are intended to cause serious harm etc. to a person or create a risk to the health or the safety of the public, although this is more of an issue of effectiveness.

a4.5. Section 103.2 criminalises making funds intentionally available to, or collecting funds for (both directly and indirectly) another person while being reckless as to whether the other person will use the funds to facilitate or engage in an act. However, the collection or provision of funds to an individual terrorist to be used for any other purpose is not covered. In addition, Australia has criminalised getting funds to, from, or for a terrorist organisation in section 102.6 CC. “Terrorist organisation” can be specifically designated by regulation or more generally be one that engages in, prepares, or assists in fostering terrorist acts. Section 102.6 covers intentional support / receipt, whether directly or indirectly, and either knowledge or recklessness that the organisation is a terrorist organisation. For all three provisions (103.1, 103.2 and 102.6) intention, knowledge and recklessness are covered in section 5. 2-4 CC. Recklessness requires the prosecution to establish that a person is aware of a substantial risk that the funds would be used, and that having regard to the circumstances known at the time to the person, taking the risk was unjustifiable. Section 5.4 CC also provides that proof of knowledge or intention satisfy the recklessness element (although proof of knowledge itself carries a higher penalty than recklessness).

a4.6. **Criterion 5.3** – All funds are covered under section 100.1 CC (the broad definition covers property and assets of any kind, tangible or intangible, movable or immovable, however acquired, as well as legal

A4

## TERRORIST FINANCING AND FINANCING OF PROLIFERATION

documents and instruments in any form, titles and financial or monetary instruments). The source (legitimate or illegitimate) is irrelevant.

a4.7. **Criterion 5.4** – Section 103 CC specifically indicates that offences are committed even if an act does not occur, or the funds will not be used in a specific act, or if the funds will be used for more than one act.

a4.8. **Criterion 5.6** – The maximum penalty for natural persons under 103.1 and 103.2 CC is life imprisonment, and under 102.6 it is 25 years (when the person knows it is a terrorist organisation) or 15 years (when the person is reckless as to whether the organisation is a terrorist organisation).

a4.9. **Criterion 5.7** – See also criterion 3.10 for the basics on corporate criminal liability. Sentencing is based on a formula from imprisonment to financial penalty, all based on 4B(2), (2A) and (3) Crimes Act. This means that the maximum penalties for legal persons under 103 CC is AUD 1.7 million (knowledge and recklessness), under 102.6 it is AUD 1 275 000 (knowledge) or AUD 765 000 (recklessness). Fines are calculated in penalty units; section 4AA defines a penalty unit to be AUD 170.

a4.10. **Criterion 5.8** – 2.4 CC extends criminal responsibility to attempt, aiding and abetting, incitement, and conspiracy to commit an offence, and to participation as an accomplice (through aid, abet, counsel, procure the commission of, section 11.2 CC) and organisation and directing (through joint commission, commission by proxy, incitement or conspiracy, sections 11.2A and 11.5).

a4.11. **Criterion 5.9** – All TF offences meet the threshold for predicate offences. See Recommendation 3.

a4.12. **Criterion 5.10** – TF offences apply regardless of geographic location (CC 15.4, 102.9, and 103.3).

### *Weighting and Conclusion*

a4.13. Australia's TF criminalisation largely follows the TF Convention; the financing of terrorist acts and terrorist organisations for any purpose is covered, as is the financing of individuals while being reckless as to whether the other person will use the funds to facilitate or engage in a terrorist act. However there are shortcomings: the Australian definition of terrorist act is somewhat narrower than the definition in Articles 2(1)(a) and (b) of the TF Convention, and the provision or collection of funds to be used by an individual terrorist for any purpose is not covered. **Recommendation 5 is rated largely compliant.**

## **Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing**

A4

a4.14. Australia was rated largely compliant for Special Recommendation III (freezing of terrorist assets). The main shortcoming was that Australian law did not explicitly cover funds of terrorists and those who finance terrorism or terrorist organisations outside of specific terrorist acts.

a4.15. **Criterion 6.1:** Sub-Criterion 6.1a – DFAT is responsible for proposing entities to the 1267/1989 and 1988 Committees for designation, based on the Administrative Arrangements Order (AAO) of 12 December 2013 (relations and communications with the UN). Sub-Criterion 6.1b – DFAT (coordination), AFP, AGD, ASIO and other intelligence agencies are responsible for identifying targets, each on the basis of the AAO, or their organic law. Sub-Criterion 6.1c – The legal framework allows an evidentiary standard of reasonable grounds in deciding whether or not to make a proposal for designation is applied, and there is no legal requirement that designations would be conditional upon the existence of criminal proceedings. Sub-Criterion 6.1d – The authorities indicate that the procedures and standard forms for listing are used (and required by the UN in the case of UNSCR 1989), also as a basis for domestic awareness outreach. Sub-Criterion 6.1e is not applicable as no names have been unilaterally proposed by Australia to date.

a4.16. **Criterion 6.2:** Sub-Criteria 6.2a and 6.2d – Section 15(1) and (2) of the *Charter of the United Nations Act 1945* (CotUNA) identify the Minister for Foreign Affairs as the competent authority to be responsible for designating entities that meet the requirements of the CotUNA. In addition, Section 20 of the *Charter of the United Nations (Dealing with Assets) Regulations 2008* (DAR) links the designation of a person to the relevant

criteria of UNSCR 1373. These sections also provide that any determination and listing must meet the standard of "reasonable grounds". No listing is linked to or conditional upon a criminal procedure. Sub-Criterion 6.2b – Same authorities and legal basis as criterion 6.1a; DFAT's Counter-Terrorism Branch and the Sanctions Section coordinate the review of (de)listing proposals and 3-yearly review, and advise on legal issues. Sub-Criterion 6.2c – The list of persons and entities designated by Australia under UNSCR 1373 includes listings done at the request of foreign governments. The process of considering a request commences the day it is received (through DFAT's Counter-Terrorism Branch). Sub-Criterion 6.2e is not applicable as no such request has yet been made.

a4.17. **Criterion 6.3:** Sub-Criterion 6.3a – Relevant government agencies have the legal authority and procedures to collect, solicit and share information to identify persons and entities that meet the criteria for designation (*Privacy Act 1988*, Australian Privacy Principles, Schedule 1, principle 3.1, AAO 6.1a and 6.1b, and section 35 of the CotUNA). Sub-Criterion 6.3b – The authorities indicate that designations are made ex parte, there is no legal or judicial requirement to hear or inform the potential designee.

a4.18. **Criterion 6.4** – The *Charter of the United Nations (Sanctions – The Taliban) Regulations 2013* (Taliban Regulations) and the *Charter of the United Nations (Sanctions Al-Qaida) Regulations 2008* (Al-Qaida Regulations) contain provisions that prohibit dealing with or making available assets of designated persons and entities (regulations 9 and 10, or 10 and 11). Designated persons and entities are defined in article 3 as any person or entity listed by the UN under UNSCRs 1267/1988/1989 and the designations are therefore automatically incorporated into Australian law. In the case of listings under UNSCR 1373, a listing takes effect as soon as the person or entity is listed in the Gazette (section 15(6) CotUNA), which takes place as soon as practicable after the Minister's decision, usually the following business day.

a4.19. **Criterion 6.5:** Sub-Criterion 6.5a – The requirement to freeze is contained as a prohibition to deal with designated persons or entities in regulation 11 (Al-Qaida Regulations, UNSCRs 1267/1989), regulation 10 (UNSCR 1988, Taliban Regulations) and section 20 CotUNA (UNSCR 1373). Freezing is ex parte and without delay as soon as the legal obligation exists. The prohibition to transfer, conversion, disposition or movement is covered through the prohibition to deal with assets (dealing is a broad term used in other laws as well). Sub-Criterion 6.5b – To cover this criterion, Australia uses the exact language used in each of the relevant UNSCRs. Each UNSCR uses slightly different language to cover the same concepts, language that is slightly different from the general language used in Recommendation 6. The definition of controlled asset (regulation 4 of the Al-Qaida and regulation 3 of the Taliban Regulations for UNSCRs 1267/1988/1989) covers an asset of a designated person or entity; and funds derived from an asset owned or controlled (which includes whole and joint ownership), directly or indirectly, by a designated person or entity; or a person acting on behalf of or at the direction of a designated person or entity.

a4.20. The definition of freezeable asset (section 14 CotUNA for UNSCR 1373) covers assets owned and controlled (whole and joint ownership) (control includes acting on behalf and at the direction of others) by a listed entity, and assets derived or generated from those assets, either directly or indirectly. The definition of asset in CotUNA (Section 2) applies to all sanction regimes. The prohibition requirements are contained in regulation 10 (Al-Qaida Regulations, UNSCRs 1267/1989), regulation 9 (UNSCR 1988, Taliban Regulations) and section 21 CotUNA (UNSCR 1373). DFAT maintains a Consolidated List of designated persons and entities subject to UNSCRs and Australian autonomous sanctions ([www.dfat.gov.au/sanctions](http://www.dfat.gov.au/sanctions)), with a possibility to receive notices if an amended list is issued. DFAT also provides software to assist those that may be holding assets to identify listed assets/entities. Additional guidance is available on the DFAT website. Also, the AFP is designated to assist to guide those that may be holding assets (regulation 41 of the DAR). Regulation 42 of the DAR requires anyone with an opinion about a targeted asset to inform the AFP. AFP, together with the ABA, has developed a referral form for possible matches. Bona fide rights are protected under section 25 CotUNA.

a4.21. **Criterion 6.6** – Under regulation 16 CotUNA, the Minister for Foreign Affairs has the authority to revoke designations that no longer meet the designation requirements (in relation to autonomous sanctions under UNSCR 1373). Under article 15A CotUNA, the Minister for Foreign Affairs has to review all autonomous listings every three years, before they automatically cease to have effect. DFAT informs listed persons and entities of the availability of the UN Ombudsperson (Al-Qaida) or Focal Point (Taliban). One false positive was so far discovered, which was resolved using the procedure highlighted above.



## TERRORIST FINANCING AND FINANCING OF PROLIFERATION

a4.22. **Criterion 6.7** – The Minister for Foreign Affairs is able to authorise access to frozen funds or other assets in accordance with UNSCR 1452. See for UNSCR 1267/1989 regulation 12 of the Al-Qaida Regulations, for UNSCR 1988 regulation 11 of the Taliban Regulation and for UNSCR 1373 section 22 of CotUNA and regulations 30 and 31 of the DAR.

### *Weighting and Conclusion*

a4.23. **Recommendation 6 is rated compliant.**

## **Recommendation 7 – Targeted financial sanctions related to proliferation**

a4.24. This is a new requirement that was not part of the previous assessment. Australia has implemented one system for targeted financial sanctions related to terrorism and TF (Recommendation 6), although specific regulations differ because they target different UNSCRs.

a4.25. **Criterion 7.1** – Pursuant to its authority under subsection 2B (1) of the CotUNA, the Minister for Foreign Affairs has issued and periodically updated two regulations dealing with the requirements in Recommendation 7: The *Charter of the United Nations (Sanctions—Democratic People's Republic of Korea) Regulations 2008* (“the DPRK Regulations”) and the *Charter of the United Nations (Sanctions — Iran) Regulations 2008* (“the Iran Regulations”). These regulations contain provisions that prohibit dealing with assets of designated persons and entities. Designated persons and entities are defined in regulation 4 of both regulations as any entity listed by the UN under article 8(d) of UNSCR 1718 for DPRK and in the Annex to UNSCR 1737 or designated by the UNSC pursuant to paragraph 12 of UNSCR 1737 (for Iran). Therefore, as the UN periodically updates its designations, targeted financial sanctions automatically apply to these persons and entities in Australia.

a4.26. **Criterion 7.2** – The requirements to freeze are contained in regulation 13 for DPRK Regulations and article 16 for the Iran Regulations. These articles prohibit using or dealing with the asset; allowing the asset to be used or dealt with; or facilitating the use of or the dealing with the asset of the designated person or entity. Freezing is without delay as soon as the legal obligation exists. Other parts of the obligations are similar to those described under criterion 6.5a. Sub-Criterion 7.2b – To cover this criterion, Australia uses the exact language used in each of the relevant UNSCRs. Each UNSCR uses slightly different language to cover the same concepts, language that is slightly different from the general language used in Recommendation 7. The definition of controlled asset (regulation 4 of the Iran and DPRK Regulations) covers an asset owned or controlled by a designated person or entity (whole and jointly), or a person or entity acting on behalf of or at the direction of a designated person or entity. The Iran Regulation covers in addition assets owned or controlled by an entity owned or controlled by a designated person or entity. “Asset” is defined in the CotUNA (section 2), applicable to the Iran and DPRK Regulations. The prohibition requirements are contained in regulations 12 and 14 for DPRK and 15 and 17 for Iran. The first article in each Regulation deals with the prohibition, the second with the licensing.

A4

a4.27. **Criterion 7.3** – Section 30 of CotUNA provides that the head of a designated federal entity (either DFAT, the Department of Defence, the ACBPS or AUSTRAC) may for the purpose of determining whether a UN sanction enforcement law is being complied with, require by written notice, the production of information or documents. Section 32 provides that failure to comply with such a notice is an offence punishable by imprisonment for 12 months. See also Recommendations 26 and 27.

a4.28. **Criterion 7.4** – On its public website, DFAT informs listed entities that they can submit de-listing requests either through the focal point process outlined in UNSC resolution 1730 or through their State of residence or nationality. A link to the Focal Point website is included. A procedure to permit access to assets for humanitarian reasons is established in regulation 14 for DPRK and 17 for Iran. Regulation 5 of the DAR brings these in line with conditions and procedures set out in UNSCRs 1718 and 1737.

a4.29. **Criterion 7.5** – For the Iran sanction regime, this is covered (regulation 5(5), DAR as required also in OP14 of UNSCR1737). For the DPRK regime, this is covered through the general freezing provisions which Australia indicates permit the freezing of interests or other earnings due on an account through addition to

these accounts, in line with UNSCR 1718. Sub-Criterion 7.5b – Regulation 17, and specifically 17(8) of the Iran and DPRK Regulations cover these requirements.

### *Weighting and Conclusion*

a4.30. **Recommendation 7 is rated compliant.**

## **Recommendation 8 – Non-profit organisations**

a4.31. Australia was rated partially compliant for Special Recommendation VIII (non-profit organisations). The main shortcomings that were noted at the time related to the lack of follow-up to NPO sector reviews, and the lack of effective implementation of a system to address TF-related NPO risks.

a4.32. **Criterion 8.1** – Several reviews of the adequacies of NPO laws have been undertaken, but none of these relate to TF abuse risks. No comprehensive reviews were undertaken in order to identify the features and types of NPOs that are particularly at risk of being misused for TF or other forms of terror support. In addition, the regulator of the Australian NPO sector (ACNC) has some information on those NPOs that voluntarily register for tax purposes but none of this relates to TF. The term “terrorism” did not feature on the ACNC’s public website until during the on-site (when a link to an AGD brochure was added). The TF NRA that was provided notes that current conflicts, such as in Syria, may raise the number of NPOs that are misused. However, none of this is a domestic review of the NPO sector; it does not provide the authorities with the capacity to obtain timely information on the NPOs’ activities, size, and other relevant features, as a basis to identify the features and types of NPOs that may at risk for TF. There is no evidence that NPO TF vulnerabilities are periodically assessed.

a4.33. **Criterion 8.2** – The government has only provided outreach to NPOs in relation to TF in the form of a brochure (non-binding guidance) in 2009, which was not available on the website of the ACNC until the on-site. It explains that there is a risk for NPOs to be misused and lists some of the measures that could be taken, but then focuses on Recommendation 6 issues. The ACNC has not issued any information in relation to terrorism or TF. A fact sheet in relation to Syria was developed, but it focuses on targeted financial sanctions breaches by citizens and is therefore not relevant for Recommendation 8.

a4.34. **Criterion 8.3** – Although the main objectives of the *Australian Charities and Not-for-Profits Commission Act 2012* (ACNC Act) are to promote minimum governance standards for NPOs, these standards only apply to those NPOs that voluntarily register for tax purposes (approximately 40 000 of the estimated 140 000 known NPOs that have taken legal personality and 20 000 without legal personality have done so, for tax purposes). The ACNC Act does not relate to terrorism, except in relation to external conduct standards of designated terrorist organisations (which is related to the general prohibitions in Recommendation 6).

a4.35. **Criterion 8.4: Sub-Criterion 8.4a** – Firstly, it is not known whether the provisions in the ACNC Act (and therefore all the requirements in Criteria 8.4(a)-(f)) apply to (i) a significant portion of the financial resources under the control of the sector or (ii) a substantial share of the sector’s international activities. It is also not known to what extent they cover the set of charities that should be targeted under this Recommendation (charities that may be at risk for TF may not be the ones that register to seek tax benefits). The ACNC allows certain NPOs to register voluntarily for tax reasons, and in this case they must register certain information and keep certain records. The aim of the information that is recorded is to promote public confidence in the sector (not related to counter terrorism purposes). The voluntary registration information includes the charity’s responsible persons (which include directors, trustees, administrators, receivers) but not information on the purpose and objectives of the stated activities. Although these shortcomings negatively affect most criteria for Recommendation 8, these are not repeated throughout this section to allow for a more succinct presentation of the analysis. Sub-Criterion 8.4b – Medium and large charities that voluntarily register must file annual financial reports and annual information statements; small charities must provide annual information statements. Basic religious charities are excluded from the requirement to provide non-financial information even if registered. However, they must still provide non-financial information in annual information statements. Sub-Criterion 8.4c: see sub-criterion 8.4b. Sub-Criterion 8.4d – There is no licencing or registration requirement. Registration is voluntary and for tax purposes, and is only for charities and not

## TERRORIST FINANCING AND FINANCING OF PROLIFERATION

for other NPOs. Sub-Criterion 8.4e – see sub-criterion 8.4b. Sub-Criterion 8.4f – Record keeping requirements (e.g. sections 55-5(1) and (2)), which includes financial records that explain transactions and financial position and performance) apply only to those that voluntarily register.

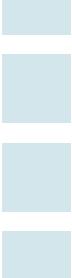
a4.36. **Criterion 8.5** – The ACNC has law enforcement powers for those charities that voluntarily register for tax purposes.

a4.37. **Criterion 8.6** – The domestic cooperation and coordination agreements that ACNC has concluded only cover its work on the charities that voluntarily register for tax purposes. Although ACNC has access to information of NPOs, this only covers those charities that voluntarily register for tax purposes. Although there are information-sharing mechanisms in place, these do not focus on TF. In addition, the information sharing only relates to information that is available on those charities that voluntarily register for tax purposes.

a4.38. **Criterion 8.7** – Australia uses the general procedures and mechanisms for international cooperation to handle requests relating to NPOs, and does not identify specific points of contact or procedures for requests involving NPOs. The assessment of Recommendations 37-40 has not identified any substantial problems which would affect cooperation regarding NPOs (if there would be a domestic recipient for such requests)

### *Weighting and Conclusion*

a4.39. According to the NRA, charities and NPOs are a key channel used to raise funds for TF in or from Australia. However, the lack of a comprehensive sectorial risk assessment (as required by Recommendation 8), the lack of subsequent outreach in relation terrorist financing to the sector, and the lack of adequate preventive requirements or a supervisory framework that covers all relevant NPOs are all shortcomings.  
**Recommendation 8 is rated non-compliant.**



## 5. PREVENTIVE MEASURES

### *Preamble*

a5.1. **Scope of financial institutions** – The chart below sets out the types of entities and persons who carry out the financial activities listed in the Glossary to the Methodology, as well as the licensing authority. Australia advised that debit and credit card schemes (see item 5 below) are licensed by ASIC and supervised for ML/TF purposes by AUSTRAC; however, representatives of such institutions met during the visit to Australia informed the team that they are not regulated or supervised by Australian authorities. AUSTRAC is the supervisory authority for AML/CTF.

**Table A5.1. Types of entities and persons who carry out financial activities**

Activities and operations according to the FATF definition of financial institutions	Financial institutions authorised to conduct these activities and operations	Licensing authority
1. Acceptance of deposits and other repayable funds from the public	Banks <sup>1</sup> (or authorised deposit-taking institutions (ADIs)): 20 Australian-owned Banks 8 Foreign Subsidiary Banks 40 Branches of Foreign Banks	APRA
	9 Building Societies (ADIs)	APRA
	85 Credit Unions (ADIs)	APRA
	4 Other ADIs	APRA
2. Lending	Banks (or ADIs) see item 1 above  9 Building Societies (ADIs)  85 Credit Unions (ADIs)  2 Specialist credit card institutions (ADIs)	APRA
	Finance companies [Total of 5 856 Australian Credit Licensees and 28 201 authorised credit representatives, including ADIs, of which 4 102 licensee provide consumer leases]	ASIC
3. Financial leasing	Lease finance companies	ASIC
4. Money or value transfer services	6 287 Money remittance companies, including hawala ADIs	AUSTRAC
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money)	ADIs, including specialist credit card institutions  Debit and credit card schemes (e.g. Visa, Mastercard, Bankcard) Electronic payment systems providers (e.g. BPAY, Paypal) 641 Ancillary non-cash payment facility providers e.g. phone companies (paying for meter parking or vending machine purchases by SMS), providers of prepaid phone card, providers of gift vouchers etc.	APRA ASIC

1. The size of the activity (assets) is as follows: banks - AUD 3214.1 billion; Building Societies - AUD 23.2 billion; Credit Unions - AUD 41.0 billion; Other ADIs and Specialised Credit Card institutions - AUD 7.7 billion; life insurance - AUD 273.9 billion

A5

## PREVENTIVE MEASURES

**Table A5.1. Types of entities and persons who carry out financial activities (continued)**

Activities and operations according to the FATF definition of financial institutions		Financial institutions authorised to conduct these activities and operations	Licensing authority
6.	Financial guarantees and commitments	Banks	APRA
7.	Trading in: money market instruments (cheques, bills, certificates of deposit, derivatives etc.); foreign exchange; exchange, interest rate and index instruments; transferable securities; commodity futures trading	ADIs  Investment banks/firms (securities/derivatives dealers/market makers) Money market firms (foreign exchange derivatives dealers/market makers) - 26 investment banks, 250 hedge fund investment managers/ responsible entities, 43 retail (over-the-counter) OTC derivative providers  1 079 AFSL holders are authorised to provide financial product advice or deal in foreign exchange contracts. These licensees have 7 853 authorised representatives.	ASIC
8.	Participation in securities issues and the provision of financial services related to such issues	18 financial markets 6 clearing and settlement facilities 136 market participants 800 securities dealers	ASIC
9.	Individual and collective portfolio management	12 Friendly societies	APRA
		28 Life insurers	APRA
		Superannuation funds and trustees: 53 Pooled superannuation trusts 2 979 Small APRA funds 62 Single-members ADFs	APRA
		528 701 Self-managed superannuation funds 200 superannuation fund trustees	ATO
		4 789 Investment advisors (3,394 AFSL holders licensed to provide personal advice and 1,395 AFSL holders licensed to provide general advice)	ASIC
		Funds managers	ASIC
		784 Managed investment schemes (trustees) 4 152 registered managed investment schemes, 494 responsible entities for MIS (as of July 2013), 614 foreign financial service providers, 718 custodial service providers, 26 investment banks, 250 hedge fund managers, and 43 retail OTC derivative providers	ASIC
10.	Safekeeping and administration of cash or liquid securities on behalf of other persons	Licensed financial service providers including: 718 custodial service providers 483 Managed investment operators (responsible entities)	ASIC

A5

**Table A5.1. Types of entities and persons who carry out financial activities (continued)**

Activities and operations according to the FATF definition of financial institutions	Financial institutions authorised to conduct these activities and operations	Licensing authority
11. Otherwise investing, administering or managing funds or money on behalf of other persons	Licensed financial service providers – see item 10 above	ASIC
12. Underwriting and placement of life insurance and other investment related insurance	28 Life insurers 207 Reinsurers	APRA
	Life insurance brokers/ life insurance agents (see 9 for list of investment and general financial advisors) Financial advisors (if holder of an AFS licence)	ASIC
13. Money and currency changing	Bureaux de change / currency exchange providers – 108 bureaux de change enrolled with AUSTRAC ADIs and other businesses performing bureaux de change functions	None

Information as of 31 December 2013.

a5.2. **Exemptions from the AML/CTF Act granted by AUSTRAC under section 248 of the AML/CTF Act** – Section 248 of the AML/CTF Act authorises AUSTRAC to exempt a specified person from one or more provisions of the AML/CTF Act, or to amend the applicable provisions of the AML/CTF Act in relation to a specified person. Pursuant to its internal policy, AUSTRAC considers a number of factors while deciding on granting an exemption or not, including the ‘the level of any potential or existing money laundering and/or terrorism financing risk’. AUSTRAC advised that a number of exemption requests were declined, including because of the ML/TF risk such an exemption would incur. All exemptions granted are publically available on AUSTRAC’s website. However, a sample of exemption decisions reviewed shows that AUSTRAC has granted full exemptions from their AML/CTF obligations to applicants and unconditional exemptions. Australia advised that unconditional exemptions have not been granted since 2010. Exemptions were also granted to businesses operating in the area of private banking, prepaid cards or investment funds. The first two sectors have been identified as a high ML threat in the NTA, while investment funds were rated as presenting medium threat. Moreover, a director from an exempted private bank has been banned by ASIC from the financial service industry for dishonest conduct, including for hiding where investment money would ultimately be placed. APRA also took enforceable undertakings against this company. Neither the exemptions nor AUSTRAC’s policy on exemptions provide for a regular review and the potential revocation of the exemptions granted.

a5.3. **Nature of some requirements applicable to reporting entities** – The AML/CTF Act and Rules contain obligations and prohibitions applicable on reporting entities - financial institutions or other persons, including some DNFBPs - when providing designated services. It should be noted that some of the FATF requirements are translated into the Act as prohibitions accompanied by sanctions (e.g. section 32 prohibits the commencement of the provision of designated service if the reporting entity has not carried out the applicable customer identification procedure; and section 81 prohibits reporting entities from providing designated services if it has not adopted an AML/CTF program or does not maintain such a program). The Rules are issued pursuant to section 229 of the AML/CTF Act and specify the obligations of the Act, in particular with respect to customer identification. The Rules, however, do not impose direct obligation on reporting entities to identify their customer, but require that their AML/CTF programme includes procedures to identify and verify the identity of their customers. Consequently, there is no explicit requirement on reporting entities to apply CDD as specified in the Standard – what they do in each case is determined by their own procedure for how they meet the requirements. Pursuant to the provisions under Part 7 of the AML/CTF Act (section 80 et seq.) reporting entities are required to adopt, maintain and apply an AML/CTF programme that complies with the AML/CTF Rules. AUSTRAC supervises reporting entities’ respect of this obligation and applies sanctions as necessary, see also Recommendations 26 and 35. As a result, from a technical point



## PREVENTIVE MEASURES

of view, the evaluation team is satisfied with the original structure of the AML/CTF obligations for reporting entities opted for by Australia.

a5.4. **Enforceability of the 2014 AML/CTF Rules.** Amendments to the 2007 Rules were adopted in May 2014 and entered into force on 1 June 2014. The 2014 amendments introduced and amended a few, though essential, obligations, most importantly with respect to beneficial ownership, ongoing due diligence and politically exposed persons. In addition to the adoption of the Rules, the *Policy (Additional Customer Due Diligence Requirements) Principles 2014* was issued by the Minister of Justice on 15 May 2014. Provision 213 of the AML/CTF Act allows the Minister to give written policy with which AUSTRAC must comply. According to the policy, for 18 months after the entry into force of the Rules (1 January 2016), a civil penalty or an injunction, the issuing of a remedial direction, or the imposition of a requirement to undertake an external compliance audit, may be applied only if the reporting entity 'has failed to take reasonable steps to comply with the relevant provision'. The policy specifies the matters to consider in determining whether a reporting entity has failed to take reasonable measures or not; they include the adoption of a transition plan and require that the Rules be applied as soon as practical in case of high ML/TF risk, and as soon as reasonable to existing customers. Notions such as 'as soon as practical' or 'as soon as reasonable' are not specified. Transition plans are to be established by 1 November 2014; they should include the necessary action and timeframes to ensure full compliance with the 2014 Rules from 1 January 2016. AUSTRAC advised that the policy reflects how AUSTRAC would have implemented and enforced the Rules in the absence of a formal policy issued by the Minister of Justice. The assessment team took the 2014 Rules into account for the purpose of the TC ratings.

### Recommendation 9 – Financial institution secrecy laws

a5.5. Australia was rated compliant in its 3<sup>rd</sup> round Mutual Evaluation Report. Since the adoption of the 3<sup>rd</sup> round assessment, the AML/CTF Act was adopted in 2006.

a5.6. **Criterion 9.1** – The AML/CTF Act imposes on reporting entities a number of reporting obligations (Parts 3 and 4), in particular a suspicious matter report (SMR). The *Privacy Act 1988* (Privacy Act) exempts from the non-disclosure prohibition where the disclosure is required or authorised by or under an Australian law or a court/tribunal order. As a result, the Privacy Act does not hinder the implementation of the AML/CTF Act.

a5.7. No obstacle that would inhibit the implementation of the FATF Recommendations was identified in the regime for correspondent banking, wire transfers, and reliance on third parties.

#### Weighting and Conclusion

a5.8. **Recommendation 9 is rated compliant.**

### Customer due diligence and record-keeping

### Recommendation 10 – Customer due diligence

A5

a5.9. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 5. Deficiencies had been identified under most aspects of the Recommendation, as well as in the scope of the financial institutions covered. In subsequent follow-up reports, progress was made through the adoption of the AML/CTF Act in 2006 and the AML/CTF Rules in 2007. The AML/CTF Rules were amended in 2014.

a5.10. **Criterion 10.1** – Sections 139 and 140 of the AML/CTF Act prohibit the provision and the reception 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.

a5.11. **Criterion 10.2** – Section 32 of the AML/CTF Act requires that the applicable customer identification procedures (hereinafter ACIPs) be applied prior to the provision of a designated service, including operating an account or carrying out an occasional transaction, including wire transfers. Section 39 of the AML/CTF Act provides for general exemptions to the identification requirements. These exemptions can be found in the AML/CTF Rules and apply to:

- Partial or full transfer of business from one reporting entity to another (Chapter 28). This situation is not in contradiction with the requirement of Recommendation 10.
- The identification of signatories of financial institutions with whom the RE has a correspondent banking relationship (Chapter 35).
- The sale of shares up to AUD 500 for charitable purposes (Chapter 38). This case is not in contradiction with the requirement of Recommendation 10. See also Recommendation 8.
- Premium funding loans for a general insurance policy (Chapter 39). This case does not seem to be in contradiction with the requirement of Recommendation 10.
- Superannuation funds, when the total amount of interest to be cashed out does not exceed AUD 1 000, or when the total amount of interest to be cashed out does not exceed AUD 5 000 (Chapter 41). These cases do not seem to be in contradiction with the requirement of Recommendation 10.

a5.12. Section 38 of the AML/CTF Act provides that the ACIP is deemed to be carried out if the customer has already been subject to ACIP consistent with the AML/CTF Act and Rules by another reporting entity. See Recommendation 17 below.

a5.13. With respect to occasional transaction above the USD/EUR 15 000 threshold and structuring: section 6 of the AML/CTF Act sets the scope of the Act and therefore of the application of the CDD obligation. Among them, the issuance of stored value cards is covered by the AML/CTF Act if the value stored on the card is more than AUD 1 000 (if whole or part of the monetary value stored on the card may be withdrawn in cash) or AUD 5 000 (if the monetary value stored cannot be withdrawn in cash) and the increase of the value of a card with the same threshold. The latter case (reloadable cards) is not an occasional transaction and should therefore require that CDD be applied regardless of any threshold, which is not the case under the current Australian legislation. Stored value cards are identified in Australia's NTA as presenting potentially high ML threats. Australia advised that a risk-based approach is applied to these means of payment and that, pursuant to items 21-24 in Table 1 in subsection 6(2) of the AML/CTF Act, the thresholds can be adjusted by regulation if necessary.

a5.14. Section 6 of the AML/CTF Act is completed by Paragraphs 14.2 to 3 of the AML/CTF Rules which sets thresholds for the application of the provisions of Part 4.2 of the AML/CTF Rules (i.e. customer identification). Pursuant to these provisions, cheques drawn on a customer for less than AUD 5 000 or AUD 1 000 for cheques funded by cash; transactions below AUD 1 000 relating to traveller's cheques (i.e. issuing, cashing or redeeming); and currency exchange below AUD 1 000 are exempted from customer identification. These transactions do not exceed the USD/EUR 15 000 threshold set by the standard; however this raises an issue in the absence of a requirement to perform CDD for occasional transactions below the threshold that appear to be linked (i.e. structuring). Australia advised that reporting entities are required to detect structuring, as section 142 of the Act makes it an offence to structure transactions to avoid the reporting threshold (AUD 10 000). This argument is only relevant in the scope of the reporting obligation of section 43 (and its exemptions in section 44).

a5.15. Occasional transactions using wire transfers: 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. See Recommendation 16, below.

a5.16. 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

A5

## PREVENTIVE MEASURES

enhanced CDD must be ‘appropriate to [the] circumstances’. The measures listed include the clarification or update of KYC information already collected on the customer, etc.

a5.17. There is 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. However, Australia advised that pursuant to the provisions of Paragraph 15.10 of the AML/CTF Rules, reporting entities are required to apply enhanced CDD (see criterion 10.17 below) when a suspicion has arisen, including in situations where there are doubts about the veracity or adequacy of previously obtained customer identification data.

a5.18. **Criterion 10.3** – As mentioned in the preamble to the section, there are no direct requirements to identify and verify the identity of the customer in the Act or in the Rules. Reporting entities are required to have AML/CTF programmes that include procedures to identify/verify the identity of the customer and enable them ‘to be reasonably satisfied’ that the customer is who/what he claims to be. Chapter 4 of the AML/CTF Rules requires reporting entities<sup>1</sup> to identify their customer and verify the information received. For each type of customer (i.e. natural persons, legal persons, trusts, etc.) the identification and verification requirements are specified. When the customer is a natural person, including a sole trader (Part 4.2 of the AML/CTF Rules): his/her name, date of birth and address must at a minimum be collected. The name must be verified as well as either the date of birth or the address. Verification is made through ‘reliable and independent documentation’ or electronic data or a combination of documents and electronic data. Parts 4.9 and 4.10 of the AML/CTF Rules specify the verification requirement, either from documentation or from electronic data.

a5.19. Similarly, Parts 4.3 to 4.8 provide for customer identification, and verification of the identification information when the customer is a company, a trust, a partnership, an association, a registered co-operative or a government body.

a5.20. Reliable and independent documentation is defined by the Rules as including but not limited to photographic and non-photographic identification documents, such as birth/citizenship certificates issued by a State/Territory/Commonwealth or foreign government, and secondary identification documents. Secondary identification documents – which can only be used to supplement primary documents to help establish identity, rather than prove identity – may include notices issued by utilities providers or schools; assessors are of the view that these documents cannot per se be seen as reliable documentation. Australia advised that in practice, reporting entities rely on multiple primary and secondary identification documents to verify the identity of their customers.

a5.21. **Criterion 10.4** – Section 89 of the AML/CTF Act specifies that Part B of financial institutions’ AML/CTF programmes must apply to agents purporting to act on behalf of a customer. Part 4.11 of the AML/CTF Rules contains different obligations considering the nature of the customer. Where the customer is a natural person, reporting entities are required under Paragraph 4.11.2 to identify the agent and collect evidence of their authorisation to act on behalf of the customer. There is no obligation to verify the identity of the agent of a customer, as Paragraphs 4.11.3 and 4 leave it to the reporting entities to determine whether and to what extent the identity of the agent must be verified. Where the customer is a ‘non-natural’ person, the name of the agent, his/her position or role with the customer, a copy of his/her signature and evidence of the authorisation to act on behalf of the customer must be verified (Paragraph 4.11.13).

a5.22. **Criterion 10.5** – The beneficial owner is defined (Paragraph 1.2.1 of the Rules) as an individual who ultimately owns or controls (directly or indirectly) the customer. It is specified that *control* includes control

A5

- 1 The AML/CTF Act requires reporting entities to establish an AML/CTF programme, which is divided into two parts – Part A and Part B. The primary purpose of Part A of the standard AML/CTF programme is to identify, mitigate and manage ML/TF risks that a reporting entity faces and includes AML/CTF risk awareness training for employees, employee due diligence programme, oversight by boards and senior management, and procedures for independent review of programme. The primary purpose of Part B is to set out the reporting entity’s ACIPs including beneficial ownership, ongoing CDD and enhanced due diligence. The AML/CTF Rules – including Chapter 4 – lays out items that the reporting entity are required to include in their AML/CTF programme.

as a result of, or by means of, trusts, agreements, etc. and includes exercising control through the capacity to determine decisions about financial and operating policies. *Owns* means ownership (either directly or indirectly) of 25% or more of a person.

a5.23. Pursuant to Part 4.12 of the AML/CTF Rules, reporting entities are required to collect information on the name, and either date of birth or address of each beneficial owner, and to take reasonable measures to verify it before the provision of a designated service, or as soon as practicable after the service has been provided. Pursuant to Paragraph 4.12.2 of the AML/CTF Rules, the obligation may be modified when the customer is a natural person, as the reporting entity may assume that the customer and the beneficial owner are one and the same person, unless there are reasonable grounds to consider otherwise. The obligation does not need to apply when the customer is a company or trust subject to simplified verification (i.e. Australian public listed companies and their majority owned subsidiaries, as well as companies licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator), an Australian Government Entity or a foreign listed public company subject to disclosure requirements concerning beneficial ownership comparable to those applicable in Australia. When the information is to be verified, verification must use reliable and independent documentation and/or electronic data (see above). The definition and obligations 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 with regard to 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.

a5.24. **Criterion 10.6** – Paragraph 8.1.5 of the AML/CTF Rules only provides that an AML/CTF programme ‘enable’ the reporting entity to understand the nature and purpose of the business relationship with its customer types (i.e. natural or legal persons), including, as appropriate, the collection of information relevant to that understanding. The use of ‘enable’ does not require a reporting entity to understand the nature and purpose of the business relationship. However, the AML/CTF 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. Moreover, 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.

a5.25. **Criterion 10.7** – Section 36 of the AML/CTF Act requires financial institutions to monitor their customers with a view to identifying, mitigating and managing ML/TF risks. Chapter 15 of the AML/CTF Rules further details the ongoing due diligence obligation. The transaction monitoring programme is risk-based and must allow a reporting entity to identify suspicious transactions and have regard to complex, unusual large transactions and patterns of transactions, which have no apparent economic or lawful purpose. Little information or guidance is given on how to implement the obligation; 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 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.

a5.26. **Criterion 10.8** – Paragraph 8.1.5(2) of the AML/CTF Rules requires reporting entities to understand the control structure of non-individual customers. There is no explicit requirement to understand the nature of their business and their ownership structure.

a5.27. **Criterion 10.9** – The AML/CTF Rules specifies for each category of legal persons what information is to be collected and/or verified (see below). There is also a general provision, providing in each case that the financial institution should be reasonably satisfied that the legal person exists. The specified information for categories of legal persons and arrangements are as follows:

A5

## PREVENTIVE MEASURES

- Companies: The AML/CTF Rules, Part 4.3, specify the information that financial institutions are required to collect, including: the full name of the company, its addresses of registration and principal place of business, its registration number (either the Australian Company Number or Australian Registered Body Number), the nature of the company and the names of the directors. Only the name, legal form and registration number must be verified. Reporting entities determine on the basis of risk if other information should be verified.
- Trusts: Part 4.4 of the AML/CTF Rules requires financial institutions to collect information on the name of the trust, its type, country of establishment and information on the trustees, beneficiaries and, under specific circumstances, the settlor. Verification only applies to the name of the trust and its beneficiaries and is done using a trust deed, certified copy or certified extract of the trust deed. Reporting entities determine on the basis of risk if other information should be verified.
- Partnership: Part 4.5 of the AML/CTF Rules requires financial institutions to collect information on the name of the partnership, country of establishment, identity and address of each partner. Only the name of the partnership and information about one partner must be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done using the partnership agreement, or a certified copy or extract of the partnership agreement.
- Associations: Part 4.6 of the AML/CTF Rules requires financial institutions to collect information on the name of the association, its address or that of its chairman, secretary or treasurer, name of the chairman, secretary and treasurer and unique identification number. Only the name and identification number are to be verified. In case of unincorporated associations, information on the name and address of the association, on the name of the chairman, secretary and treasurer and on the identity of the members must be collected. Only information on the name of the association and information on the members is to be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done using the constitution or rules of the association, or a certified copy or extract.
- Registered co-operatives: Part 4.7 of the AML/CTF Rules requires financial institutions to collect information on the name of the co-operative, its full address, unique identification number and the name of the chairman, secretary and treasurer. Only information on the name of the co-operative and unique identification number must be verified. Reporting entities determine on the basis of risk if other information should be verified. Verification is done through any register maintained by the cooperative, or a certified copy or extract.
- Government bodies: Part 4.8 of the AML/CTF Rules requires financial institutions to collect and verify information on the name, principal place of operations and whether the government body is an entity or an emanation of the Commonwealth, a State, Territory or a foreign country or is established under the legislation of the Commonwealth, a State, Territory or a foreign country.

a5.28. The identification of companies seems to be overall in line with the criterion. 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 (i.e. apart from the directors and those who appear on the legal person's statutes). 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.

a5.29. **Criterion 10.10** – Part 4.12 of the AML/CTF Rules provide for the identification and verification of the identity of the beneficial owner, see criterion 10.5, above. Paragraph 4.12.9 of the AML/CTF Rules provides for the measures to be undertaken if the reporting entity has not been able to determine who the beneficial owner is. In this case, the reporting entity must identify and take reasonable measures to verify the identity of any individual exercising more than 25% of the voting rights or holding a position of senior managing official. This is in line with the Standard, though there is no gradation between the two measures of Paragraph 4.12.9.

a5.30. **Criterion 10.11** – Part 4.4 of the AML/CTF Rules deals with the identification of trusts. As already described under criterion 10.9 above, the identification of the trust as a customer requires the identification of the trustees (pursuant to the rules applicable to the nature of the trustee) and beneficiaries. Information on the name and address of each trustee is required to be collected, as well as either information on the full name of each beneficiary or collection information on the class of beneficiaries. Amendments introduced in May 2014 now also require reporting entities to identify and verify the name of the settlor, unless the settlor's contribution to the trust is less than AUD 10 000 at the time of its creation, or if the settlor is deceased, or if trust is subject to the simplified trustee verification procedure. Verification on the identity of the trustees and beneficiaries is not required by the Rules. Paragraph 4.4.11 leaves it to the reporting entities to determine whether and to what extent the identity of the agent must be verified. Paragraph 4.12.9 of the AML/CTF Rules requires reporting entities unable to determine who the beneficial owner of a trust is, to identify and take reasonable measures to verify the identity of any individual who holds the power to appoint or remove the trustees of the trust.

a5.31. **Criterion 10.12** – Pursuant to item 39 of Table 1 under section 6 of the AML/CTF Act, the person(s) to whom a payment is made under a life insurance policy is considered as being the customer of the paying financial institution. CDD measures of Chapter 4 of the AML/CTF Rules described above apply to the customer at the time of the payment. No obligation applies in relation to the identity of the beneficiary of a life insurance policy as soon as the beneficiary is identified or designated.

a5.32. **Criterion 10.13** – 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, see criterion 10.17 below.

a5.33. **Criteria 10.14 and 10.15** – 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. Concerning the special circumstances of Chapter 46, a list of eight conditions is provided, including the impossibility for the customer to transfer the amount of the contract and the prohibition for the financial institution to accept cash. It is specified among the conditions of Chapter 46 that it is practically impossible to conduct the ACIP before the transaction, which must be performed rapidly due to the market conditions, and that the financial institution put 'in place appropriate risk-based systems and controls to determine whether and in what circumstances to provide the designated service to a customer before the applicable customer identification procedure is carried out, including in relation to the number, types and/or amount of transactions'. The financial institution is required to carry out the ACIP within five business days (section 34 of the AML/CTF Act and Chapter 46 of the AML/CTF Rules); otherwise, it must not continue to provide any transaction or service or to perform another transaction or service.

a5.34. **Criterion 10.16** – Division 2 of Part 2 of the AML/CTF Act explicitly applies to existing customers. Obligations with respect to existing customers apply when a suspicion arises (section 29); the obligations are set forth in Part 6.3 of the AML/CTF Rules: financial institutions are required within 14 days after the suspicion arose to take at least one of the following actions: (i) perform ACIP; (ii) collect any KYC information; or (iii) verify certain KYC information. As a result, the financial institution should be satisfied that the customer is the person he or she claims to be. This mechanism does not seem to take account of 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 does 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 rather deal with the identification of the customer. Though this is not explicit in section 36 of the AML/CTF Act and in Chapter 15 of the AML/CTF Rules, Australia advised that the requirement to monitor customers and the obligation to apply enhanced due diligence also applies to existing customers.

a5.35. **Criterion 10.17** – Paragraph 15.8 *et seq.* of the AML/CTF Rules provides for the enhanced CDD programme and measures to implement in this context. Such a programme must be implemented when the reporting entity determines that the ML/TF risk is high; when the customer is a foreign PEP; when a suspicion



## PREVENTIVE MEASURES

has arisen; or, when the customer is located in a prescribed foreign country (i.e. Iran). The enhanced CDD measures to be taken must be appropriate to the circumstances. Examples of a range of measures are listed in Paragraph 15.10; some of the measures included in the range seem to address normal due diligence (e.g. clarification and update KYC information, including its activity or business, identification of the beneficial owner, etc.). Other measures, such as identification of the sources of funds and wealth, and seeking senior management approval, are more suited to enhanced due diligence.

a5.36. **Criterion 10.18** – Paragraph 4.3.8 allows financial institutions to apply simplified verification procedures when the customer is a domestic listed company, a majority owned subsidiary of a domestic listed public company or a company licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator. The verification measures are considered to be satisfied provided that the reporting entity at least obtains a search of the relevant domestic stock exchange, of the relevant ASIC database or of the license or other records of the relevant regulator or a public document issued by the relevant company. 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, simplified verification procedures may apply to trusts that are managed investment schemes registered by 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.

a5.37. In Chapter 4 there are a number of provisions allowing financial institutions to apply CDD on the basis of risk. In most cases, it relates to measures other than those that are mandatory according to the Rules, e.g. collection of additional KYC information or verification of information other than in cases required by the Rules. In a few instances, the drafting of the provisions may lead to a complete exemption from CDD measures, in particular the verification obligation but also the obligation to collect information (see for example Paragraph 4.4.11 concerning the verification of the name of any or each trustee or beneficiary or class of beneficiaries or any other KYC information collected; Paragraph 4.11.3 on the verification of the identity of the agents of a customer, etc.) as the Rules leave it to the financial institutions ‘to determine whether [and in what manner] to collect and/or verify’ information.

a5.38. **Criterion 10.19** – 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.

a5.39. **Criterion 10.20** – There is no provision permitting financial institutions 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).

### *Weighting and Conclusion*

a5.40. Several deficiencies have been identified under Recommendation 10 including:

- exemptions provided by the AML/CTF Act and Rules diminish the application of CDD in every situation envisaged by the standard (e.g. signatories of financial institutions in domestic correspondent banking relationships, reloadable stored value cards operating at a threshold, occasional transactions below a threshold which appear linked);
- shortcomings regarding verification requirements in relation to agents;
- exemptions and simplified due diligence do not appear based on proven low risk;
- shortcomings in relation to identification requirements and verification (powers to bind the legal entity and its senior managers) across all legal persons and legal arrangements including ownership structure;

- no requirement to identify the beneficiary of a life insurance policy until payout; limitations in enhanced customer due diligence which may be satisfied by updating identification which is considered normal due diligence; and
- no requirements relating to not proceeding or terminating the business relationship when CDD is unable to be complied with or to stop performing CDD if there is a risk of tipping off.

a5.41. **Recommendation 10 is rated partially compliant.**

## Recommendation 11 – Record-keeping

a5.42. In the 3<sup>rd</sup> assessment, Australia was rated partially compliant for Recommendation 10. The main deficiencies were that the FTR Act did not cover transaction record-keeping for all types of financial institutions, and there were no specific requirements for account files and business correspondence to be retained. Record-keeping requirements were substantially amended respectively in 2006 and 2007 by the AML/CTF Act (Part 10) and AML/CTF Rules, lastly amended in 2014. AUSTRAC has published guidance note 08/04 on record-keeping requirements to assist reporting entities to comply with their record-keeping obligations.

a5.43. **Criterion 11.1** – Sections 106 to 110 of the AML/CTF Act applies to transaction records, and these requirements are comprehensive. Section 106 identifies designated services where a transaction record must be made and retained. If a reporting entity makes a record of information relating to the provision of a designated service, that reporting entity must also keep records for seven years in relation to transaction records, or a copy of transaction records for seven years following the closing of the customer relationship (section 107). A document or a copy of the document provided by a customer relating to the provision of a designated service must also be retained for seven years after the provision of the document (section 108). These are supplemented by broad requirements to keep transaction records in corporate legislation. Under section 286 of the *Corporations Act 2001* (Corporations Act), all companies, registered schemes and other disclosing entities (whether or not they are financial institutions) must keep for seven years financial records that correctly record and explain their transactions and financial position and performance and would enable true and fair financial statements to be prepared and audited.

a5.44. **Criterion 11.2** – Reporting entities must make and keep records of the ACIP, which must include the information obtained in the course of carrying out the procedure (sections 112 – 113 of the AML/CTF Act). These records seem to cover all CCD information collected and must be kept for seven years following the conclusion of the customer relationship. The following must also be kept for seven years: electronic funds transfer instructions, an AML/CTF programme made under Part 7 of the AML/CTF Act, and due diligence assessments of correspondent banking relationships (sections 115 – 117).

a5.45. Pursuant to a designating provision in section 107 of the AML/CTF Act, the AML/CTF Rules (Chapter 29) exempt certain documents in particular customer-specific documents, such as account statements and documents routinely prepared by the reporting entity, correspondence, and records of customer enquiries from the record-keeping requirements. These exemptions mean that not all account files and business correspondence, and results of any analysis undertaken, needs to be kept.

a5.46. **Criterion 11.3** – There is no clear obligation in the AML/CTF Act that transaction records should be sufficient to permit reconstruction of individual transactions. AUSTRAC guidance note 08/04 (section 7.3) indicates that AUSTRAC considers it preferable that transaction records be sufficient to permit the reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for the potential prosecution of criminal activity. However, this is not a legally enforceable requirement. There are additional recordkeeping obligations laid out in the Corporations Act (section 988E) and the *National Consumer Credit Act 2009* (section 92), that require – among other things – that financial records must be kept in sufficient detail to show particular details related to all money received or paid by the licensee. This may be sufficient to permit reconstruction of individual transactions into/out of some financial institutions, but there are gaps in the scope of financial institutions covered by these provisions and it is unclear whether this would capture all types of transactions. In the case of international

A5

## PREVENTIVE MEASURES

wire transfers and for transactions reported to AUSTRAC (either SMR or TTR), more detailed information may be available as it is required in the context of the reporting obligations.

a5.47. **Criterion 11.4** – There is no requirement upon financial institutions to ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority. There are provisions relating to AUSTRAC's monitoring and enforcement authorities (Parts 13-15 of the AML/CTF Act), including the power to give a written notice requiring the person to provide information or produce documents or copies of documents in the manner and within the time specified in the notice. AUSTRAC guidance note 08/04 (section 7.9) does indicate that, pursuant to AUSTRAC's monitoring powers under Part 13 of the Act, records should be stored in a retrievable and auditable manner. However, the actions available under the monitoring and enforcement powers of AUSTRAC do match the swift availability of the records and are limited to AUSTRAC. The guidance note is not enforceable. There are additional provisions in section 49 of the AML/CTF Act for the heads of selected government authorities to request information directly from reporting entities; this authority is limited to information related to reports (SMRs, IFTIs or TTRs) filed by reporting entities.

### *Weighting and Conclusion*

a5.48. Reporting entities are required to keep records of the transactions with their customers and of their identification information for seven years. However, certain customer-specific documents are exempt from record-keeping requirements. There is also no requirement that the records kept be sufficient to permit the reconstruction of the transactions although Australia's reporting framework provides a complementary backstop. Finally reporting entities are not legally required to ensure that the records are available to all competent authorities. **Recommendation 11 is rated largely compliant.**

## Additional Measures for specific customers and activities

### **Recommendation 12 – Politically exposed persons**

a5.49. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 6 as PEPs were not dealt with under the AML/CTF regime in place at that time. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, as amended in 2014.

a5.50. Scope – Part 1.2 of the AML/CTF Rules provides the definition of PEP which is broadly in line with that of the FATF. However, it seems that the status of the PEP ceases with the position or function, as the definition refers to an individual who holds a prominent public position or function. Important political party officials are not explicitly covered by the Rules. Australia advised that they are covered by other categories, such as senior government officials or senior politicians. This may be true in Australia, but may not be adequate to cover important political party officials in foreign countries. Immediate family members are covered while the standard refers more broadly to 'family members'. The notion of 'close associates' requires beneficial ownership of a legal person or arrangement. Australia advised that the definition of PEPs is inclusive.

**A5**  
a5.51. **Criterion 12.1** – Part 4.13 of the AML/CTF Rules deals with PEPs. Pursuant to Paragraph 4.13.1, reporting entities are required to determine whether a customer or the beneficial owner is a PEP. This determination should occur before the provision of a designated service to the customer or as soon as practicable after the provision of a designated service. Paragraph 4.13.3 provides for the measures to be taken in case of foreign PEPs. If the PEP is the beneficial owner of the customer, the ACIP applicable to the customer should apply to the PEP. In all cases, the reporting entity should (i) obtain senior management approval before establishing or continuing the business relationship; (ii) take reasonable measures to establish the PEP's source of wealth and source of funds; and, (iii) comply with the obligations in Chapter 15 on 'Ongoing customer due diligence'.

a5.52. **Criterion 12.2** – In addition to the common measures applicable to all PEPs, measures specific to domestic PEPs and PEPs of international organisations are set out in Paragraph 4.13.2 of the AML/CTF Rules. If the PEP is the beneficial owner of the customer, the ACIP applicable to the customer should apply to the PEP. If the PEP is considered as presenting high ML/TF risk, then the reporting entity should (i) obtain senior management approval before establishing or continuing the business relationship; (ii) take reasonable measures to establish the PEP's source of wealth and source of funds; and, (iii) comply with the obligations in Chapter 15 on 'Ongoing customer due diligence'.

a5.53. **Criterion 12.3** – The obligations described above apply to PEPs. The definition of which includes 'immediate family members' and 'close associates of PEPs'.

a5.54. **Criterion 12.4** – As described under criterion 10.12, CDD measures only apply to the beneficiary of a life insurance policy at the time of the payout. There is no further obligation in case of higher risk situation.

### *Weighting and Conclusion*

a5.55. The AML/CTF Rules Amendment set comprehensive obligations for PEPs.. The notions of close associate, which requires beneficial ownership of a legal person or arrangement, and of family members, which only apply to the spouse, parents and children, are too restrictive. Important officials of political parties are not covered and there is no specific requirement for life insurance. **Recommendation 12 is rated largely compliant.**

## **Recommendation 13 – Correspondent banking**

a5.56. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 7 as correspondent banking relationships were not regulated under the AML/CTF regime in place at that time. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.57. **Criterion 13.1** – Pursuant to sections 97 to 99 of the AML/CTF Act and Part 3.1 of the AML/CTF Rules, financial institutions are required, in relation to the provision of correspondent banking services, to:

- Conduct a preliminary assessment (section 97(1) of the AML/CTF Act) of the risk the financial institution may reasonably face that the correspondent banking relationship might involve or facilitate ML/TF. This assessment is to be carried out before the establishment of the correspondent banking relationship and is to be carried out on a regular basis. No further indication is provided on how such an assessment should be conducted, using what information, etc. Based on the outcomes of the preliminary assessment, financial institutions may be required under section 97(2) of the AML/CTF Act to conduct a 'due diligence assessment'. Pursuant to Paragraph 3.1.2 of the AML/CTF Rules, undertaking a 'due diligence assessment' is not compulsory; a reporting entity determines whether it is warranted based upon the preliminary assessment. This assessment of the ML/TF risk presented by the correspondent financial institutions covers among other things the existence and the quality of the AML/CTF regulation in the country of the correspondent institution; the adequacy of the AML/CTF internal control and compliance of the correspondent institution; information on the ownership, control and management, the reputation of the correspondent institution; information on whether the correspondent institution has been subject to ML/TF related investigations or prosecution, etc. This assessment must be conducted prior to the establishment of the correspondent banking relationship and must be updated on a regular basis. There is however no reference to the ML/TF supervision conducted in the country of the correspondent institution;
- Obtain prior approval from a senior officer of the financial institution;
- Document the respective responsibilities. There is no specification of the AML/CTF responsibilities, which therefore are deemed to be covered (section 99(2) of the AML/CTF Act).

A5

## PREVENTIVE MEASURES

a5.58. However, as noted above, Part 3.1 of the AML/CTF Rules specifies that 'due diligence assessment' is implemented on the basis of risk, which is not permitted under the standard.

a5.59. **Criterion 13.2** – There is no requirement with respect to payable-through accounts. However, in July 2007 AUSTRAC issued a guidance note to assist financial institutions in implementing their obligations in relation to correspondent banking relationships, which provides an example of a payable-through account.

a5.60. **Criterion 13.3** – Section 95 of the AML/CTF Act prohibits financial institutions from entering into a correspondent banking relationship with a shell bank, or with another financial institution that has a correspondent banking relationship with a shell bank. It is unclear whether the prohibition extends to entering into a correspondent banking relationship with a financial institution that does 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. Financial institutions are also required to terminate such business relationships within 20 days after becoming aware that the correspondent institution is a shell bank or within the period of time determined by AUSTRAC.

### *Weighting and Conclusion*

a5.61. The information reporting entities are required to gather and verify in the context of a correspondent banking relationship is insufficient as information on the AML/CTF regulation applicable to the correspondent bank; the adequacy of its internal controls; information on the ownership, etc. is gathered in the due diligence assessment, which a financial institution can conduct or not based upon the risk. There are no specific obligations for payable through accounts. **Recommendation 13 is rated non-compliant.**

## **Recommendation 14 – Money or value transfer services**

a5.62. In its 3<sup>rd</sup> assessment, Australia was rated partially compliant on Special Recommendation VI as a number of deficiencies had been identified, in particular with respect to the licensing/registration of MVTS and limitations of the FTR Act. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.63. **Criterion 14.1** – Part 6 of the AML/CTF Act relates to the Remittance Sector Register. Section 74 provides that a person must not provide a registrable remittance network service or a designated remittance service unless they are registered as a remittance network provider, a remittance affiliate of a registered remittance network provider, or an independent remittance dealer. Sanctions are two-year's imprisonment or 500 penalty units, or both. Pursuant to section 75, AUSTRAC is required to maintain the Remittance Sector Register. The Register indicates the name of the person; the category in which s/he is registered (remittance network provider, or an affiliate of a registered remittance network providers, or independent remittance dealer); as necessary, the name of the network to which the affiliate is affiliated; any conditions to which the registration of the person is subject; the date of effect of the registration; and the registrable details in relation to the person. AUSTRAC's decision to register a person is made according to section 75C after having considered whether the person would involve a significant ML/TF or people smuggling risk that would potentially arise, should registration be granted. Registration is valid for three years; after that period, it must be renewed. AUSTRAC has large powers in the registration process. For example, further conditions to the registration can be imposed; further information can be requested; registration can be cancelled or suspended, in particular in case of significant ML/TF or people smuggling risk, etc. Pursuant to section 75M, any change that could materially affect the person's registration must be notified by the registered person. Civil penalties apply in case of failure to notify substantial change on a registered person.

a5.64. **Criterion 14.2** – Australia advised that a series of measures has been implemented since the commencement of the AML/CTF Act in 2006 in order to identify unregistered MVTS. These measures include advertisements using radio and press in several languages, awareness raising and training sessions and material, the reliance on large money transfer networks to identify unlicensed remitters, etc. As mentioned above there are sanctions applicable to those persons: two years imprisonment and/or 500 penalty units.

A5

a5.65. **Criterion 14.3** – MVTS providers are subject to the monitoring of AUSTRAC for AML/CTF compliance. Australia advised that within AUSTRAC a team is dedicated to MVTS. This team is in charge of maintaining the Remittance Sector Register; dealing with the registration requests; and monitoring MVTS' AML/CTF compliance.

a5.66. **Criterion 14.4** – As described above under criterion 14.1, agents (or affiliates in Australia's AML/CTF Act) are required under section 74 to register with AUSTRAC.

a5.67. **Criterion 14.5** – Pursuant to section 84(5A) of the AML/CTF Act, a registered remittance network provider is required to make a standard AML/CTF programme available to its affiliates. This however does not prevent a remittance affiliate from adopting an individual specific AML/CTF program. Paragraph 54.2 of the AML/CTF Rules specifies that a remittance network provider assumes the TTR and IFTI reporting obligations of its agents. However, this does not entail that a remittance network provider monitors all activities of its agents. Australian authorities believe that there is an implicit requirement for a registered remittance network provider to monitor the compliance of its affiliates with the AML/CTF programme as part of the ongoing customer due diligence and transaction monitoring of the registered remittance network provider conducted on the affiliate, as the AML/CTF Act notes that the affiliates are the customer of the registered remittance network provider. However, the assessors believe that this was not sufficient in requiring the registered remittance network provider to monitor compliance of its affiliates with the AML/CTF programme and would recommend that this be made an explicit requirement.

### *Weighting and Conclusion*

a5.68. MVTS are registered and supervised by AUSTRAC, which has taken a number of initiatives to ensure that all providers are registered. 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. **Recommendation 14 is rated largely compliant.**

## Recommendation 15 – New technologies

a5.69. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 8 in the absence of an AML/CTF regime applicable to new technologies. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.70. **Criterion 15.1** – Australia has identified and assessed in its 2011 NTA the ML risks associated with 'electronic payment systems and new payment methods' which cover ATMs, credit/debit cards and stored value cards, online payment systems, online remittance and digital currencies. It seems to the assessors that among these items, not all can be considered as new technologies. Moreover, the NTA does not cover new business practices nor is it up to date. See also Recommendation 1. However, AUSTRAC also has conducted research on virtual currencies/Bitcoin and issued a policy.

a5.71. Reporting entities are required under section 81 of the AML/CTF Rules to adopt and maintain an AML/CTF programme whose objective, consistently with section 84(2), is to identify; mitigate and manage ML/TF risk. The AML/CTF Rules further specify under Parts 8.1 and 9.1 the factors to be considered for the identification of ML/TF risk, in particular the types of services provided and the methods by which services are delivered. The same provisions also state that the AML/CTF programme must enable reporting entities to assess the ML/TF risk posed by all new designated services prior to introducing them to the market; all new methods of designated service delivery prior to adopting them; and all new or developing technologies used for the provision of a designated service prior to adopting them.

a5.72. **Criterion 15.2** – As described above, reporting entities are required to assess new services, methods of delivery and technologies prior to their adoption or use. However, other than the general obligation to assess the ML/TF risk (section 80 et seq. of the AML/CTF Act and Paragraphs 8.1.5 and 9.1.5 of the AML/CTF Rules), there is no specific explicit requirement for reporting entities to take appropriate measures to manage and mitigate the identified risks in the area of new technologies.

A5

## PREVENTIVE MEASURES

### *Weighting and Conclusion*

a5.73. Australia demonstrated it had assessed ML/TF risks associated with some new products and technologies. Reporting entities are required to identify, mitigate and manage their ML/TF risks, but there is no specific obligation for new technologies. **Recommendation 15 is rated largely compliant.**

### **Recommendation 16 – Wire transfers**

a5.74. Australia was rated non-compliant for Special Recommendation VII (wire transfers). There was no system to implement the requirements, only a reporting obligation for international wire transfers (a requirement which was deemed not-relevant in the context of and for the assessment of the compliance with SRVII, which required, as the current standard still does, that certain information flow to other financial institutions dealing with each wire). Since 2009, Australia has implemented measures intended to solve the shortcomings related to SR.VII. These have not been re-assessed as part of follow-up, but were extensively discussed with the authorities as part of this assessment and seem to address the earlier deficiencies. The requirements for Recommendation 16 have been extensively updated compared to SR.VII.

a5.75. **For all criteria** – Australia meets the requirements regarding the originator information (name, account number or unique transaction reference, address or identity/customer number or date and place of birth). Australia also meets the requirement that originator information is retained with a transfer. However, the legislation does not yet require the new elements of Recommendation 16: verification of the accuracy of the information, beneficiary information, intermediary financial institutions, record keeping (for the information that is not required). There is no threshold in Australia, thus criterion 16.3 does not apply. The current legal framework applies to MVTS but only covers the requirements related to SR.VII. However, in practice, Australia already requires MVTS to report information on originator and beneficiary MVTS transfers when filing an SMR (not in law, but through the relevant report forms). With respect to the freezing obligations, Australia does not ensure that freezing action is undertaken in the context of Recommendation 16.

### *Weighting and Conclusion*

a5.76. Australia has the elements in place to comply with the originator information requirements contained in the old SR.VII; however, the intermediary, beneficiary, verification, MSB and targeted financial sanctions elements have not yet been updated in line with the new Recommendation 16. **Recommendation 16 is rated partially compliant.**

## **Reliance, Controls and Financial Groups**

### **Recommendation 17 – Reliance on third parties**

a5.77. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 9 in the absence of most of the requirements necessary to mitigate the risk posed by reliance on third parties. In subsequent follow-up reports, some progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

A5

a5.78. Section 38 of the AML/CTF Act sets out the conditions in which a reporting entity may rely on the CDD measures performed by a third party. The third party must be a reporting entity and have performed CDD consistent with the AML/CTF Act and Rules. Section 38(d) further provides that other conditions set out in the AML/CTF Rules must be satisfied. Chapter 7 of the AML/CTF Rules sets conditions in relation to financial advisers (i.e. holder of an AFSL) and for reporting entities that belong to the same designated group. Australia advised that only financial advisers and designated groups have expressed interest in the mechanism of section 38. Therefore, in other situations, the sole provisions of section 38 of the AML/CTF Act apply. In practice, reporting entities can only rely on a reporting entity located in Australia. The Explanatory Note of the Declaration, made on 16 March 2009 by the CEO of AUSTRAC, widens the range of third parties

on whom a reporting entity can rely to those that are a subsidiary of an Australian company located in a foreign country and that have customer identification procedures comparable to those prescribed under the AML/CTF regime in Australia. The objective of the declaration is to cover subsidiaries of Australian financial institutions located abroad, in particular in New Zealand.

a5.79. **Criterion 17.1** – Section 38 introduces the presumption that the ACIP has been conducted by the reporting entity that relies on the third party. It is 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 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 is 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.

a5.80. **Criterion 17.2** – As mentioned above, it is possible for Australian REs to rely on third parties located in Australia or abroad, in particular in New Zealand. Australia has not demonstrated that the ML/TF risk presented by New Zealand financial institutions was considered when the declaration expanding the scope of third parties to New Zealand financial institutions was issued. More generally, the Declaration of 16 March 2009 makes 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”.

a5.81. **Criterion 17.3** – Part 7.3 of the AML/CTF Rules sets out similar conditions for relying on a third party within the same DBG to those described above. As demonstrated above, reliance on third parties is limited to those located in Australia and on the subsidiaries of Australian reporting entities located abroad.

### *Weighting and Conclusion*

a5.82. There are several deficiencies in Australia's regulation of third party reliance. It is not explicitly stated that the reporting entity relying on a third party remains ultimately responsible for CDD measures. There is 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. The geographic risk regarding New Zealand or any other country has not been taken into account when considering expanding the scope of third parties to financial institutions from this country was issued. **Recommendation 17 is rated partially compliant.**

## **Recommendation 18 – Internal controls and foreign branches and subsidiaries**

a5.83. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendations 15 and 22 in the absence of an obligation for financial institutions to have AML/CTF internal controls, policies and procedures and to ensure that their foreign branches and subsidiaries apply AML/CTF measures consistent with the Australian requirements. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AMLM/CTF Rules, lastly amended in 2014.

a5.84. **Criterion 18.1** – Section 81 of the AML/CTF Act requires financial institutions to adopt, maintain and apply an AML/CTF programme. A standard programme applies to a particular financial institution; joint programmes apply to each financial institution that belongs to a particular DBG. Such programmes, either standard or joint, are divided into two parts. Part A is general; Part B relates to customer identification (sections 84(1)(b) and 85(1)(b)). Pursuant to sections 84.2 and 85.2, the objective of Part A is for the financial institution or entities of the DBG to identify, mitigate, and manage the ML/TF risk it may face. Chapters 8 and 9 of the AML/CTF Rules provide details as to what Part A and the joint AML/CTF programmes must contain.

- Compliance management arrangements, including the appointment of a compliance officer at the management level - Parts 8.4 and 8.5 and 9.4 and 9.5, require that Part A and the joint AML/CTF programme must be approved by the board and senior management of the financial institution or

## PREVENTIVE MEASURES

group and that an AML/CTF compliance officer must be designated at the management level. There is no other compliance mechanism and the role and functions of the compliance officer are not further detailed.

- Screening procedures when hiring employees – Parts 8.3 and 9.3 provide that Part A of an AML/CTF programme (either standard or joint) must include ‘an employee due diligence programme’, which ‘put in place appropriate risk-based systems and controls for the reporting entity to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of a money laundering or financing of terrorism offence’. Screening of potential employees is based on risk and therefore may not be performed. It is limited to ML/TF aspects. However, it should be noted that a new screening may be conducted in case of transfer or promotion of an employee.
- Ongoing employee training programme – Parts 8.2 and 9.2 provide that Part A of an AML/CTF programme (either standard or joint) must include an ‘AML/CTF risk awareness training programme’ which must be designed so that the reporting entity gives its employees appropriate training at appropriate intervals, having regard to the ML/TF risk it may reasonably face. The objective is to ‘enable employees to understand’ the AML/CTF obligations set out by the Act or the Rules and applicable to a particular financial institutions, the type of ML/TF risk that the financial institution may face, and the processes and procedures established in the AML/CTF programme. The wording ‘enable to understand’ is weaker than requiring that the employee understands AML/CTF obligations.
- Independent audit function - Parts 8.6 and 9.6 provide that Part A of an AML/CTF programme (either standard or joint) must be subject to a regular independent review by an internal or external party. The objective is to assess the effectiveness of the Part A programme, its compliance to the AML/CTF Rules, and effective implementation. The result of the review is to be submitted to the board and senior management. The function is limited to the audit of Part A programmes. There are no indications as to the frequency of the “regular” review, or how to guarantee the independence of an internal audit, etc.

a5.85. **Criterion 18.2** – As mentioned above, section 85 of the AML/CTF Act deals with the AML/CTF programme applicable in DBGs. DBGs are groups of two or more members that have decided to be member of the group. Part A of a programme is to identify, mitigate and manage ML/TF risk that each financial institutions of the DGB may face. The description and conclusions of criterion 18.1 above also apply.

- Sharing information – Part A of a joint programme is not required to contain policies and procedures on the sharing of information. It should be noted that the Act allows any member of a DBG to discharge certain obligations on behalf of other members. Section 123(7) 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 customer to another reporting entity within that DBG, in order to inform the other reporting entity about the risks involved in dealing with the customer.
- Group-level compliance, audit and/or AML/CTF functions – 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 DBGs.
- Confidentiality and use of information exchanged – As mentioned above, 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. There are no further obligations in relation to confidentiality and use of information exchanged.

a5.86. **Criterion 18.3** – Section 6(6) of the AML/CTF Act extends the application of the Act to foreign branches and subsidiaries of Australian financial institutions. Part 8.8 and 9.8 deal with permanent

establishments in foreign countries (i.e. foreign branches). Paragraph 8.8.3 sets out without any further detail that where a foreign branch is regulated by AML/CTF laws comparable to Australia, only minimal additional systems and controls need to be considered by the financial institution. Paragraph 8.8.4 provides that Parts 8.1 to 8.3 (i.e. general provision on Part A programme, risk awareness training and employee due diligence programme) do not apply to foreign branches. Chapter 9 of the Rules contains similar provisions for DBGs. Except for section 6(6) of the Act, there are no provisions applicable to subsidiaries located abroad. There is no obligation for financial institutions 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 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/CTF measures consistent with Australia's AML/CTF regime.

### *Weighting and Conclusion*

a5.87. There are numerous deficiencies with respect to reporting entities' internal controls: there is no obligation beyond the nomination at management level of a compliance officer, the audit function is limited and there is no indication of the frequency of the audit or guarantee of its independence. This also applies at the group level. There are a number of deficiencies concerning branches and subsidiaries located abroad, in particular the obligation to apply the higher standard. **Recommendation 18 is rated partially compliant.**

## **Recommendation 19 – Higher-risk countries**

a5.88. In the 3<sup>rd</sup> assessment, Australia was rated partially compliant for Recommendation 21. The deficiencies noted that while AUSTRAC has the authority under section 38(1)(e) of the FTR Act to indicate other countries as higher risk, it had made limited use of this provision. Also, there was no specific requirement for financial institutions to pay special attention to transactions involving countries that do not adequately apply the FATF Recommendations in accordance with Recommendation 21. Since 2005 specific regulatory measures have been implemented to target higher-risk countries.

a5.89. **Criterion 19.1** – Chapter 15 (On-going Due Diligence) of the AML/CTF Rules requires reporting entities to apply their enhanced CDD programme when they determine the situation to be of higher risk, a ML/TF suspicion has arisen, or when entering, or proposing to enter, into a transaction with a party who is a natural or legal person in a prescribed foreign country. See the analysis in criterion 10.17 regarding what reporting entities must do as part of their enhanced due diligence programmes. Iran has been designated as a prescribed foreign country pursuant to the AML/CTF Regulations (as updated in 2012)—see also criterion 19.2 below. On the other hand, the DPRK has not been designated as a prescribed foreign country via the AML/CTF Regulations. While Australia imposes an autonomous sanctions regime in relation to DPRK, reporting entities are not legally required to apply enhanced due diligence measures to all customers from this country, although Australia notes that reporting entities do so in practice. However, this is not sufficient to meet the Standard.

a5.90. **Criterion 19.2** – Australia is able to apply counter-measures when called upon to do so by the FATF, or independently of any call by the FATF to do so. Part 9 of the AML/CTF Act allows regulations under the Act to impose countermeasures which regulate or prohibit transactions with legal and natural persons physically present in prescribed foreign countries (which includes situations when the FATF calls upon countries to do so or independently of any FATF call). Regulations made under Part 9 are subject to a two-year sunset effect. The AML/CTF Regulations were amended, with effect from 1 March 2012, to make Iran a prescribed foreign country and prohibit transactions of AUD 20 000 or more unless prior authorisation has been granted by DFAT. Reporting entities must also apply enhanced due diligence on customers and transactions involving Iran, including payments sent or received through third-party countries. AUSTRAC guidance note 12/02 states that AUSTRAC expects all Iran-related transactions be treated as high-risk for the purposes of transaction monitoring.

a5.91. **Criterion 19.3** – AUSTRAC Information Circulars (AICs) advise reporting parties of concerns about weaknesses in the AML/CTF systems of other countries. The AICs advise or update reporting entities of significant AML/CTF matters such as modified regulatory obligations, federal government listing of terrorist organisations, and UNSC or autonomous Australian sanctions. The circulars also publish the FATF Public

A5

## PREVENTIVE MEASURES

Statements and Improving Global AML/CTF Compliance documents and state that reporting entities should take into account FATF statements when considering whether transactions should be reported to AUSTRAC as suspicious.

### *Weighting and Conclusion*

a5.92. While reporting entities are required to apply enhanced due diligence (and counter-measures) to their relationships and transactions with Iran, they are not required to do so for DPRK, despite the FATF's call to do so. While reporting entities must apply enhanced due diligence when they themselves determine there to be higher-risk, this does not equate to a requirement pursuant to criterion 19.1. And, among the measures for enhanced due diligence listed in the Rules, some address normal due diligence rather than enhanced due diligence. **Recommendation 19 is rated partially compliant.**

## Reporting of Suspicious Transactions

### **Recommendation 20 – Reporting of suspicious transaction**

a5.93. In its 3<sup>rd</sup> assessment, Australia was rated largely compliant for both Recommendation 13 and Special Recommendation IV. Overall, the regime for reporting suspicious transactions within the FTR Act 1988 was comprehensive except that there was a limitation on the scope of "cash dealers" and a concern that the scope of the TF offence could slightly limit the reporting obligation. Provisions of the FTR Act were amended and updated in the AML/CTF Act(section 41).

a5.94. **Criterion 20.1** – Subsection 41(1) defines a series of "suspicious matter reporting obligation" triggers that then must be reported to AUSTRAC pursuant to subsection 41(2). Civil penalties apply for non-reporting: up to 100 000 penalty units (AUD 17 million) for a body corporate, and up to 20 000 penalty units (AUD 3.4 million) for an individual.

- For ML-related SMRs: these must be reported within 3 business days after the day of forming the suspicion on reasonable grounds that the provision or prospective provision of the service is preparatory to or may be relevant to the investigation or prosecution of ML, a tax offence, or any other offence. "Money Laundering" means any offence against Division 400 of the CC, or any corresponding State, Territory, or foreign offence.
- For TF-related SMRs: these must be reported within 24 hours after forming the suspicion on reasonable grounds that the provision or prospective provision of the service may be preparatory to or may be relevant to the investigation or prosecution of financing of terrorism. "Financing of terrorism" includes: any offence against section 102.6 or Division 103 of the CC; an offence against section 20 or 21 of the CotUNA; or any corresponding State, Territory, or foreign offence. *See the analysis of Recommendation 5 – limitations in the scope of the TF offence may somewhat limit the reporting requirement.*

a5.95. **Criterion 20.2** – Section 41 includes references to a "prospective" provision of a service when suspicion can be formed (and then must be reported), which incorporates the concept of attempted transactions. The reporting obligations apply regardless of the amount of the transaction involved.

### *Weighting and Conclusion*

a5.96. There are some limitations in the scope of the TF offences given that the reporting requirement is directly tied to the criminalisation in the CC. However, the assessors believe that the limitation is sufficiently minor as to not have a material impact on the reporting requirement. **Recommendation 20 is rated compliant.**

A5

## Recommendation 21 – Tipping-off and confidentiality

a5.97. **Criterion 21.1** – Section 235 of the AML/CTF Act protects a person or an officer, employee or agent of this person from any action, suit or proceeding (whether criminal or civil) in relation to any acts made in good faith in carrying out compliance with any requirement in the AML/CTF Act, Regulations, or Rules.

a5.98. **Criterion 21.2** – Section 123(1) indicates that if a SMR obligation arises or has arisen for a reporting entity in relation to a person, and the reporting entity has filed an SMR, the reporting entity must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC that information has been communicated to the AUSTRAC CEO.

a5.99. Section 123(2) further provides that if a reporting entity has formed an applicable suspicion (but has not yet filed an SMR), the reporting entity must not disclose to anyone other than the AUSTRAC CEO or an AUSTRAC staff member about the suspicion or about any other information from which the person to whom the information is disclosed could reasonably be expected to infer that the suspicion had been formed. However, subsection 123(4) specifies a number of cases where section 123(2) does not apply, including when the reporting entity is: a legal practitioner; a partnership or company that carries on the business of using legal practitioners to supply professional legal services; a qualified accountant, or a partnership or company that carries on a business of using qualified accountants to supply professional accountancy services; and the information relates to the affairs of a customer of the reporting entity; and the disclosure is made for the purposes of dissuading the customer from engaging in conduct that could constitute an evasion of a taxation law or evasion of a law of a State or Territory that deals with taxation; or an offence against a law of the Commonwealth, State, or Territory. It is unclear to what extent these exemptions weaken the confidentiality requirements before an SMR is filed. The Australian authorities should clarify in what circumstances this could apply to reporting parties that may be lawyers or accountants but also carry out “financial activities” as defined by FATF.

### *Weighting and Conclusion*

a5.100. **Recommendation 21 is rated compliant.**

## Designated non-financial businesses and professions

### *Preamble: Scope of DNFBPs*

a5.101. The AML/CTF Act applies to those who provide a service designated in section 6, tables 6.1, 6.2 and 6.3. Tables 6.2 and 6.3 deal with bullion dealers and gambling services, including casinos. Chapter 52 of the AML/CTF Rules exempt persons licensed to operate no more than 15 gaming machines from most of the AML/CTF obligations, in particular CDD, internal control and record keeping obligations. These two categories are the only two DNFBPs explicitly targeted by the AML/CTF Act. Other DNFBPs (i.e. real estate agents, dealers in precious stones, lawyers, notaries, other legal professionals and accountants, and TCSPs) are only covered when they provide one of the designated services – i.e. essentially acting in the capacity of a financial institution under the FATF Recommendations. None of the services designated relates to real estate agents, dealers in precious stones or TCSPs activities. The AML/CTF Act applies to lawyers, notaries and other independent legal professionals when they provide a designated service. Australia specified that lawyers, notaries and other independent legal professionals may provide the designated services listed under Table 6, Items 6, 7 and 54 that relate to money lending and services provided as holder of an AFS licence. These three items are financial activities and dealt with in section 5 of this annex. They are not specific to lawyers, notaries and other independent legal professionals and Recommendation 22. Solicitors are referred to in the FTR Act and require that they report cash transactions exceeding AUD 10 000 (see below).

A5

## PREVENTIVE MEASURES

### Recommendation 22 – DNFBPs: Customer due diligence

a5.102. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 12 as deficiencies had been identified under most Recommendations referred to in Recommendation 12, in particular Recommendations 5 and 10, and in the scope of the DNFBPs covered. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.103. **Criterion 22.1** is not met. Pursuant to Chapter 10 of the AML/CTF Rules, gambling services are required to identify their customer when they carry out transactions above AUD 10 000 (approximately USD 9 000 / EUR 6 000) which exceeds the USD/EUR 3 000 threshold for this criterion. Bullion dealers are also obliged to perform CDD measures for transactions of AUD 5 000 or more, which is in line with the standard. When applicable, CDD obligations for casinos and bullion dealers are similar to those applicable by financial institutions and described in Recommendation 10.

a5.104. **Criteria 22.2 to 22.5** – See Recommendations 11, 12, 15 and 17.

#### *Weighting and Conclusion*

a5.105. Only casinos and bullion dealers are subject to AML/CTF obligations. The AML/CTF Act also 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. See also conclusions under Recommendations 11, 12, 15 and 17. As a result, **Recommendation 22 is rated non-compliant**.

### Recommendation 23 – DNFBPs: Other measures

a5.106. In its 3<sup>rd</sup> assessment, Australia was rated non-compliant on Recommendation 16 as deficiencies had been identified under most Recommendations referred to in Recommendation 16, in particular Recommendations 13, 15 and 21, and in the scope of the DNFBPs covered. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a5.107. Criteria 23.1 to 23.4 - See Recommendations 20, 18, 19 and 21.

#### *Weighting and Conclusion*

a5.108. Given that most DNFBPs 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 for DNFBPs that are subject to the requirements, **Recommendation 23 is rated non-compliant**.

A5

## 6. SUPERVISION

### Recommendation 26 – Regulation and supervision of financial institutions

a6.1. In its 3<sup>rd</sup> assessment, Australia was rated partially compliant on Recommendation 23 because of the low number of AML/CTF inspections, lack of tools, and quality of the supervision. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a6.2. **Criterion 26.1** – Pursuant to sections 212 and 229 of the AML/CTF Act, AUSTRAC is in charge of the “promotion of compliance this Act, regulations and AML/CTF Rules” and is empowered to “make rules prescribing matters required or permitted by the AML/CTF Act to be prescribed by AML/CTF Rules”. Pursuant to section 212(1)(f) of the Act, AUSTRAC has other functions as conferred on the CEO of AUSTRAC under this Act, including monitoring compliance with the AML/CTF Act, Rules and Regulations as mentioned under section 190 of the Act.

a6.3. **Criterion 26.2 –**

a6.4. Core Principles financial institutions:

- Authorised Deposit-taking Institutions (ADIs) (i.e. banks, building societies, credit unions, certain participants in credit card schemes, and providers of certain purchased payment facilities) are required to be licensed to carry on banking business (section 8 of the *Banking Act 1959*). Section 9 provides for the licensing process. In particular, APRA is responsible for granting licenses, as necessary imposing further conditions, and revoking licenses
- Financial intermediaries (i.e. investment banks) that are not operating as an ADI are required to obtain an AFSL before conducting financial services business. AFSLs are issued by ASIC.
- Holders of an Australian Credit License (ACL) are licensed by ASIC. A national licensing scheme is applied for people who want to engage in credit activities in relation to consumers under the *National Consumer Credit Protection Act 2009* and must hold an ACL or be an authorised representative of a licensee.
- APRA registers superannuation funds of trustees regulated by APRA. Their trustees (other than trustees of self-managed superannuation funds which are regulated by the ATO) are licensed and registered by APRA; they may be required to hold an AFSL granted by ASIC depending on the nature of the operation carried out.
- Insurance: general insurers are required to be authorised under section 12 of the *Insurance Act 1973* (Insurance Act) and life insurers are required to be registered under section 21 of the *Life Insurance Act 1995* (Life Insurance Act). In both cases, the authorisation and registration are granted by APRA and are in the nature of a license, as APRA assesses the applications received and can impose additional conditions prior to authorisation or registration.

a6.5. Other financial institutions:

- Remittance sector: Part 6 of the AML/CTF Act sets out the framework for the enrolment (registration) of money remitters. As is the case for the Core Principles financial institutions, registration is not automatic. Additional conditions can be decided by the AUSTRAC CEO and a prior assessment as to whether the registration would involve a significant ML/TF or people smuggling risk is conducted, including the fact key personnel have been charged or convicted for offences and risks deriving from beneficial ownership arrangements.

A6

## SUPERVISION

- Currency exchange houses, (bureaux de change) where physical currency is settled immediately, must enrol (register) with AUSTRAC.

a6.6. The establishment or the operation of shell banks is not expressly prohibited, but the licensing process seems to preclude it. Section 9 of the Banking Act requires institutions to be licensed by APRA in order to conduct a banking business. APRA's Guidelines on Authorisation of ADIs set out a number of criteria, including on the head office, management and supervision, that applicants must fulfil, that seems to make it clear that a shell bank will not be authorised as an ADI.

a6.7. **Criterion 26.3 -**

- Financial institutions regulated by APRA – Section 19 of the Banking Act prohibits 'disqualified persons' from acting for an ADI. Section 20 defines disqualified persons to include persons who have been convicted of an offence under the Banking Act, *Financial Sector (Collection of Data) Act 2001*, Corporations Act, or of an offence of any law, where the offence relates to dishonest conduct or to conduct relating to a company carrying out business in the financial sector. ML/TF offences are not expressly mentioned but Australia advised that they would fall within the scope of offences relating to dishonest conduct or to conduct relating to a company in the financial sector. The Banking Act does not include fitness and propriety as conditions for the licensing. ADIs must have a fit and proper policy and are primarily responsible for the quality of their senior management (i.e. directors, senior managers and auditors). However, a licence may be revoked for lack of fitness and propriety.
- The Insurance Act, Life Insurance Act and *Superannuation Industry (Supervision) Act 1993* contain similar provisions.
- The fit and proper requirement for ADIs, general insurers and life insurance companies is further detailed in the Prudential Standard CPS 520. In particular, it is specified that financial institutions must have a written policy on fit and proper requirements and are responsible for its implementation. Such a policy applies to directors, senior management and auditors; they are required to be skilled, experienced, competent, diligent and honest. The fit and proper policy applies to applicants to certain functions, but also on an annual basis for each responsible person position and in case of suspicion.
- The *Financial Sector (Shareholdings) Act 1998* imposes approval requirements where more than 15% of the voting shares in an ADI are to be held by an individual or a group. Shareholders are not subject to fit and proper obligations; however, the ADI Authorisation Guidelines issued by APRA state that 'all substantial shareholders are required to demonstrate to APRA that they are 'fit and proper' in the sense of being well-established and financially sound entities of standing and substance'.
- AFSL holders – except if licensed by the APRA, applicants to an AFSL are required to meet minimum obligations set out in the Corporations Act. ASIC must grant a licence if a business shows it can meet basic standards such as training, compliance, insurance and dispute resolution. There is no fit and proper obligation. A number of Licensing Regulatory Guides are available on the website of ASIC. One of them elaborates on the basic obligations, including the role and function of senior management, the obligation to provide services in an efficient, honest and fair way, employee screening and training. It should however be noted that regulatory guides are not law and do not constitute legal advice; they only provide guidance.
- There are no fit and proper requirements regarding ACL holders. ACL holders are required to lodge annual compliance certificates which may be verified by ASIC. However, there are no direct obligations regarding fitness and propriety.
- Remittance providers: Pursuant to section 75C of the AML/CTF Act, the ML/TF risks are to be considered by AUSTRAC while deciding to register a remittance provider. Chapter 57 of the AML/CTF Rules specify the other matters that are to be regarded for the registration process; they deal

A6

with the offences for which the applicant has been charged or convicted, the legal and beneficial ownership and control of the applicant, etc.

- There are no fit and proper requirements regarding currency exchange businesses ('bureaux de change').

a6.8. **Criterion 26.4** – AUSTRAC supervises all reporting entities under the AML/CTF Act, including Core Principles financial institutions, money remitters and 'bureaux de change' (or currency exchange businesses). All 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.

a6.9. AUSTRAC supervises all reporting entities under the AML/CTF Act, including Core Principles financial institutions, money remitters and currency exchange businesses ('bureaux de change'). AUSTRAC focuses its efforts on the supervision on groups entities which provide services and products identified as having a higher exposure and vulnerability to ML/TF.

a6.10. **Criterion 26.5** – AUSTRAC applies to a certain extent a risk-based approach in its supervision of reporting entities at a corporate group level for efficiency reasons. Selection for assessment, frequency and intensity of on-site and off-site supervision of corporate groups (reporting entity groups - REGs) and individual reporting entities is determined on the basis of ML/TF risks identified in the NTA, exposure to ML/TF risk because of the size of the group, and the volume and value of transaction reports lodged with AUSTRAC, and specific interest by AUSTRAC's internal risk committee or partner agencies. Through previous direct compliance engagements with REGs and/or individual reporting entities, AUSTRAC has information regarding internal controls and procedures associated within the REG and/or those individual reporting entities. Inherent ML/TF risks are only taken into account to a certain extent; as far as reported transactions may indicate, while size of the REG can be just be one of several factors in determining risk among other factors (for example activities of entities within the REG, geographical risk, product risk, client risk, etc.). Only after selection of individual reporting entities for assessment does AUSTRAC seek to collect further information to get a more complete risk profile of that reporting entity, mainly based on its information lodged through reporting requirements. Regarding ML/TF risks present in Australia, reference is made to industries and channels mentioned in the NTA. However, the NTA gives guidance on the current inherent ML/TF risks in Australia (see Recommendation 1) to a limited extent.

a6.11. **Criterion 26.6** – AUSTRAC does not fully assess or re-assess the REG's risk profile, as insight in compliance risks are yet to be further developed. AUSTRAC advised that the ML/TF risk profiles of the high risk groups are reviewed through yearly cycles, and low risk groups in three yearly cycles. These reviews include regular follow up actions by AUSTRAC monitoring the remediation given by the group. To a limited extent reviews of risk profiles of groups and reporting entities outside these high risk groups are undertaken.

### *Weighting and Conclusion*

a6.12. Licensing or registration requirements and fit and proper obligations are in place regarding the financial sector. AUSTRAC applies to a certain extent a risk-based approach in its supervision of reporting entities at a corporate group level. ML/TF risks are not adequately identified by AUSTRAC, as risks are primarily identified by activity in a sector determined to be high risk by the NTA and mainly through analysis of transaction reporting. Risk profiles of the high risk groups are reviewed through yearly cycles; those of low risk groups in three yearly cycles. These reviews include regular follow up actions by AUSTRAC monitoring the remediation given by the group, but the depth of follow-up varies. To a limited extent reviews of risk profiles of REGs and reporting entities outside these high risk groups are undertaken. **Recommendation 26 is rated partially compliant.**

A6

### **Recommendation 27 – Powers of supervisors**

a6.13. In its 3<sup>rd</sup> assessment, Australia was rated partially compliant on Recommendation 29 due in particular to the limited powers of AUSTRAC and low level of implementation. In subsequent follow-up reports, progress

## SUPERVISION

were made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a6.14. **Criterion 27.1 –**

- *Supervision* - Sections 147, 148 and 150 of the AML/CTF Act list the powers of AUSTRAC's authorised officers, which include the power to enter premises and to search, examine, and inspect documents, etc. in order to monitor compliance with the AML/CTF Act and Rules. However, all of these powers are conditional upon either the consent of the reporting entity to enter the premises or a monitoring warrant. Moreover, the Act permits a reporting entity to revoke the access of AUSTRAC's authorised officers to its premises. Pursuant to section 161, AUSTRAC may require reporting entities to appoint an external auditor. The AUSTRAC CEO must specify what matters are to be covered by the audit and must be given a copy of the audit report.
- *Ensuring compliance* – Section 190 of the AML/CTF Act provides for the situations where violations to the AML/CTF obligations of financial institutions are identified. The following paragraph lists some of the measures ('remedial directions') that AUSTRAC can take in the case of a reporting entity breaching the AML/CTF obligations. Ensuring compliance with the AML/CTF Act is also one of the functions of AUSTRAC's CEO pursuant to section 212 of the Act. Section 212(2) also specifies that AUSTRAC's CEO must consider while performing his functions a number of factors, such as the integrity of the financial system; crime reduction; competition; economic efficiency; the FATF Recommendations and any relevant Convention or Resolution; etc.

a6.15. **Criterion 27.2 –** Pursuant to sections 147 and 148 of the AML/CTF Act, AUSTRAC's officers have the authority to conduct inspections (i.e. to enter the premises of a financial institution and search and examine necessary documents). However, inspections can only take place with the consent of the occupier of the premises or if a magistrate has issued a warrant (section 159). Moreover section 152 allows the financial institution to refuse to consent to the entry in the premises of the financial institution.

a6.16. **Criterion 27.3 –** Section 150 of the AML/CTF Act provides AUSTRAC's officers with the authority to ask questions and seek production of documents. As mentioned above, this power may be completed only with the consent of the occupier of the premises or if a magistrate issues a warrant. Section 167 of the AML/CTF Act authorises authorised officers to ask by a written notice to be provided with information, documents or copies of a document under the forms set in the notice. In both cases, omissions are sanctioned by imprisonment of 6 months and/or 30 penalty units.

a6.17. **Criterion 27.4 –** There is a range of sanctions available for sanctioning violation of the AML/CTF obligations. Civil and criminal penalties can be imposed by a court. Remedial directions and enforceable undertakings are administrative actions that AUSTRAC can impose. See Recommendation 35. Sanctions do not include the power to withdraw, restrict or suspend the reporting entity's licence. AUSTRAC can, pursuant to section 75G of the AML/CTF Act, cancel a remitter's registration in case of significant risk of ML/TF, suspend or impose conditions on the registration. Regarding financial institutions licensed by APRA, AUSTRAC can refer breaches to APRA which maintains the power to withdraw the licence.

### *Weighting and Conclusion*

a6.18. AUSTRAC has powers to supervise and ensure compliance with AML/CTF requirements to the extent that these are conditional upon the consent of the reporting entity. Entering the premises and the search, examination and inspection of reporting entities' documents can be limited by the reporting entity, although where required warrant powers exist. Moreover the Act permits a reporting entity to at any time revoke the access of AUSTRAC's authorised officers to its premises. A warrant is then necessary for AUSTRAC to execute its powers. Therefore, **Recommendation 27 is rated partially compliant**.

A6

## Recommendation 28 – Regulation and supervision of DNFBPs

a6.19. In its 3<sup>rd</sup> assessment, Australia was rated partially compliant on Recommendation 24 as most DNFBPs lack effective AML/CTF regulation and supervision. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a6.20. **Criterion 28.1** – Casinos, gambling and gaming houses are required to be licensed by State or Territory casino control authorities. Under each State or Territory legislation, the licensing authority considers the applicant's suitability. However, the State and Territory licencing authorities do not have express AML/CTF responsibilities to qualify as competent authorities. In addition, not all legislation requires the licensing authority to consider the associates of the applicants (see for example the Gaming Control Act of the Northern Territory). Post-licensing, casinos are subject to the AML/CTF legislation and supervised by AUSTRAC.

a6.21. **Criteria 28.2 to 28.4** – With the exception of bullion dealers supervised by AUSTRAC, other DNFBPs are not subject to AML/CTF obligations, and therefore are not monitored by competent authorities or self-regulated bodies. The entry standards and fit and proper requirements differ across the various DNFBP sectors, and are absent in some instance (e.g. bullion dealers, TCSPs).

a6.22. **Criterion 28.5** – Only casinos and bullion dealers are supervised by AUSTRAC to which it applies the same approach as that applied to the supervision of other reporting entities. See Recommendation 26.

### *Weighting and Conclusion*

a6.23. Only casinos, gaming outlets, and bullion dealers are supervised for AML/CTF compliance. Considering the fundamental deficiencies in the scope of AML/CTF coverage and supervision of DNFBPs as covered under IO.3, **Recommendation 28 is rated non-compliant**.

## Recommendation 34 – Guidance and feedback

a6.24. Australia was rated PC with the previous Recommendation 25. The assessment identified that most of the guidance was heavily focussed on SUSTRs, but inadequate in regard to general detailed CDD guidance. Guidance also did not cover most DNFBPs. On feedback, the assessment indicated that while there was some general and specific feedback on STRs, AUSTRAC could provide more sanitised examples of actual ML cases and/or information on that decision or result of an SUSR. The language of the Recommendation has not changed. However, since the last assessment Australia has adopted a new AML/CTF Act and issued new AML/CTF Rules, archived most of the guidance issued under the previous legislation, and issued some new guidance.

a6.25. **Criterion 34.1** – AUSTRAC issues a wide range of guidance covering most aspects of AML/CTF obligations of reporting entities from its website. Feedback is mainly general but does now include a range of sanitised cases. The guidance does not apply to most DNFBPs as they are not reporting entities.

- Almost all guidance is issued by AUSTRAC – mostly on its website, pursuant to a general obligation of the AUSTRAC CEO to “advise and assist reporting entities in relation to their obligations”. The material issued includes policies, guidance notes, information circulars, legal interpretations, newsletters, guides, information booklets and brochures, risk assessments, annual typology and case studies reports, and typology briefs. In addition, AUSTRAC provides guidance and feedback during consultations with industry as well as via an E-Learning application and a help desk for reporting entities. The issued material addresses a range of issues, with much of it focusing on sending signals to industry about how AUSTRAC will exercise its regulatory functions, particularly for non-compliance. The key document is AUSTRAC’s “Compliance Guide” (available at: [www.austrac.gov.au/austrac-compliance-guide.html](http://www.austrac.gov.au/austrac-compliance-guide.html)) which comprehensively explains the obligations of reporting entities.

A6

## SUPERVISION

- A concern is that the regulatory framework gives reporting entities substantive discretion for applying the AML/CTF requirements and allows simplified measures for all medium and low risk situations, yet there is only limited guidance for identifying high risk customers or situations.
- Feedback provided to reporting entities is mainly general, published, since 2007, in AUSTRAC's annual typologies and case studies report (which contains sanitised examples of actual cases drawn from SMRs). AUSTRAC also highlights positive examples of suspicious reporting, as well as general areas of deficiency (e.g. late reporting, insufficient detail in certain fields) at industry meetings and forums. AUSTRAC does provide specific feedback on SMRs to some reporting entities as part of their compliance assessments and ongoing regulatory engagement. AUSTRAC also provides detailed feedback on regulated entities compliance with requirements as part of its supervisory role (see IO3).

### *Weighting and Conclusion*

a6.26. AUSTRAC issues a wide range of guidance covering most aspects of AML/CTF obligations of reporting entities. The material issued includes a comprehensive "Compliance Guide". Feedback has improved since the introduction of the AML/CTF Act in 2006 and includes a range of sanitised cases. A concern is the limited guidance available for identifying high risk customers or situations. In addition, none of the guidance applies to most DNFBPs. **Recommendation 34 is rated largely compliant.**

## Recommendation 35 – Sanctions

a6.27. In its 3<sup>rd</sup> assessment, Australia was rated partially compliant on Recommendation 17 due in particular to the limited powers of AUSTRAC and low level of implementation. In subsequent follow-up reports, progress was made through the adoption respectively in 2006 and 2007 of the AML/CTF Act and AML/CTF Rules, lastly amended in 2014.

a6.28. **Criterion 35.1** – Sanctions for Recommendation 6: Violations of terrorist and TF related targeted financial sanctions (i.e. UNSCRs 1267/1989, 1989 and 1373) are sanctioned by a maximum of 10 years' imprisonment and a fine the greater of either AUD 425 000 (approx. USD 391 000 / EUR 283 000) or three times the value of the transaction when committed by a natural person, and a fine the greater of either AUD 1.7 million (approx. USD 1.5 million / EUR 1.1 million) or three times the value of the transaction when committed by a legal person.

a6.29. Sanctions for Recommendation 8 to 23: The AML/CTF Act provides for a number of civil penalties and criminal offences when obligations are violated. Moreover, AUSTRAC has some powers to directly impose actions in case of violation of the AML/CTF obligations. In addition, it may apply to a court for a civil penalty order in case of violation of the obligation to apply customer's identification procedures (section 31), to verify the identity of the customer (section 35), to conduct on-going due diligence (section 36), to report suspicious matters (section 41), etc. Pursuant to section 175(4) of the AML/CTF Act the maximum civil penalty that can be imposed is 100 000 penalty units for a corporation and 20 000 penalty units for natural persons, or AUD 17 million and 3.4 million respectively (or approximately USD 15.5 million – EUR 11 million and USD 3 million – EUR 2.3 million). AUSTRAC can also apply to the court for an injunction restraining a person from doing something or requiring a person to do something (section 192). With respect to money remitters, AUSTRAC can, in addition to the measures above, suspend or cancel the registration (sections 75G and H of the AML/CTF Act).

a6.30. Criminal sanctions are also imposed by a court. They are available for a limited number of offences for failure to implement obligations related to R.8 to 23, and are listed in Part 12 of the AML/CTF Act: providing false or misleading information or documents; falsifying documents for use in an ACIP; providing or receiving a designated service using a false name or customer anonymity; structuring a transaction to avoid a reporting obligation; failing to register; failing to respond to questions; and failing to respond to notices. The first three offences are the most severe as they are punishable by 10 years imprisonment and/or 10 000 penalty units. In addition to these penalties and offences provided in the Act, AUSTRAC may give remedial directions (section 192). They are written directions through which AUSTRAC requires a reporting entity to take specified action

A6

towards ensuring that the reporting entity does not breach its AML/CTF obligations. Remedial directions are enforced by a court and are published on the website of AUSTRAC. Criminal sanctions are also available for tipping-off, punishable for two years or 120 penalty units or both.

a6.31. Australia also relies on the powers of the AUSTRAC CEO to give remedial directions (section 191) and to accept enforceable undertakings (section 197 *et seq.*). A remedial direction is a “written direction requiring the reporting entity to take specified action directed towards ensuring that the reporting entity does not contravene the civil penalty provision, or is unlikely to contravene the civil penalty provision, in the future”. An enforceable undertaking is a “written undertaking given by a person that the person will, in order to comply with this Act, the regulations or the AML/CTF Rules, take specified action or refrain from taking specified action”. With respect to remitters, AUSTRAC can refuse, cancel or suspend a registration in case of significant risk of ML/TF. AUSTRAC does not have the power to withdraw, restrict or suspend the reporting entity’s license. For reporting entities licensed by APRA, AUSTRAC can refer breaches to APRA, which maintains the power to withdraw a license. However, APRA does not have the direct ability to put conditions on or revoke a license, or to remove managers and directors for breaches of the AML/CTF Act and Rules. APRA may only revoke a license for breaches of the Banking Act (section 9A), its regulations, or the *Financial Sector (Collection of Data) Act 2001*.

a6.32. There are a range of sanctions available for AML/CTF breaches; the maximum fines seem to be high enough to apply sanctions that are proportionate to the violation and dissuasive. See also criterion 27.4.

a6.33. **Criterion 35.2 – Sanctions for the violation of AML/CTF obligations** apply to the offender, be it a natural or a body corporate. Part 2.5 of the CC provides for the criminal liability of bodies corporate. The offence must be “committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority” and the intentional element “must be attributed to a body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence”. Section 231 of the AML/CTF Act explicitly states that Part 2.5 of the CC applies to the offences against the AML/CTF Act. Sections 232 and 233 relate to the civil liability of corporations and of persons other than corporations.

a6.34. It is not specified in the AML/CTF Act or in the Rules that, in addition to the sanctions applicable to the natural person who violates an AML/CTF obligation of the Act or of the Rules, directors and senior management of financial institutions or DNFBPs are also liable for the violation committed and therefore may be sanctioned (except in the cases where the violation is committed by a director or senior manager).

### *Weighting and Conclusion*

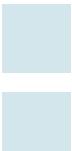
a6.35. Given the scope issues on DNFBPs, the AML/CTF requirements in Recommendations 6, and 8 to 23 do not apply to DNFBPs. The range of sanctions for AML/CTF breaches is limited, particularly what can be directly applied by AUSTRAC, but the maximum fines are sufficiently high to be viewed as proportionate and dissuasive sanctions. 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. **Recommendation 35 is rated partially compliant.**

A6

## SUPERVISION



A6



## 7. LEGAL PERSONS AND ARRANGEMENTS

### Recommendation 24 – Transparency and beneficial ownership of legal persons

a7.1. Australia received a largely compliant rating in 2005 for Recommendation 33 in the 2004 Methodology (the predecessor to Recommendation 24). The only deficiency noted in the 2005 assessment was that administrative measures supporting corporate on-going maintenance did not provide adequate access to beneficial ownership information in a timely manner for the majority of legal persons. Recommendation 33 was not part of the follow-up process for Australia given the strength of this rating. The new Recommendation 24 is much more detailed than the previous standard.

a7.2. **Criterion 24.1** – The principal forms of legal persons in Australia are proprietary companies, public non-listed companies, public listed companies, incorporated limited partnerships, and incorporated associations. All companies (proprietary and public companies) must register with ASIC. ASIC maintains a record of the incorporation, as well as type of incorporation, of each company on its publicly accessible “Companies and Organisations Register”, which is updated and maintained on an on-going basis. The process for the creation of these legal persons and for the obtaining and recording of basic ownership information about them is clear. There is no clear process for the obtaining or recording of beneficial ownership information (as that term is defined by FATF). However, pursuant to the provisions in Part 6C.2 of the Corporations Act, beneficial ownership tracing notices can be issued with respect to a person’s interest in the shares of a public company (listed company or listed investment scheme). Other legal persons, such as incorporated limited partnerships, incorporated associations, are incorporated by the States and Territories. There is no beneficial ownership tracing notice mechanism available for State/Territory entities. The processes for the creation and the public availability (all registers are publically available) of information relating to these types of legal persons, including on beneficial ownership, therefore vary throughout the country.

a7.3. Australia reports that in 2012-13 there were approximately 2 million registrations with ASIC, including 1 990 551 proprietary companies; 21 690 public companies; and 3 324 foreign companies.

a7.4. **Criterion 24.2** – Australia has assessed the threat of ML through corporate vehicles and other legal persons in its (sanitised) NTA and, in the context of organised crime, in the sanitised version of the ACC’s biennial OCTA (Organised Crime in Australia). The NTA made a distinction between corporate entities that can be used to conceal ownership and public companies where shares can be purchased using proceeds of crime. The first scenario was given a high threat rating; the second a medium threat rating. The sanitised version of the NRA is silent about legal persons.

a7.5. **Criterion 24.3** – The Corporations Act (section 117) requires the provision of specific information on company information when an application for registration is made, including the address of the registered office, share structure of the company, name and address of directors (who cannot be legal persons) and whether a registered company will have an ultimate holding company in Australia or overseas. Other required information is registered as well. ASIC maintains a Companies and Organisations Register (on which the information is publicly available). According to section 112 of the Corporations Act, proprietary and public companies are registered under the Act. The registration process for the other types of legal persons, including incorporated limited partnerships and incorporated associations, and the basic information required in this context vary throughout the country. Australia advised that according to State and Territory legislation, the name of the entity, its legal form and status, its address, the basic regulating powers and officeholders and members are registered and that this information is publically available.

a7.6. **Criterion 24.4** – Under section 168 of the Corporations Act companies must set up and maintain a shareholders (“members”) register which contains each member’s name and address, and date of entry of the member’s name in the register. If the company has more than 50 members there must be an up-to-date index of names that is easily accessible. Where the company has share capital, that register must also contain information including the date, number and share class allotted to each member. It must also contain the amount paid for each share. The register must also show the names and details of former shareholders and

A7

## LEGAL PERSONS AND ARRANGEMENTS

the date they stopped being a member. This information is required to be held at the company's corporate registered office (section 172).

a7.7. **Criterion 24.5** – A number of provisions of the Corporations Act require that changes in the information submitted to ASIC be notified within a specified timeframe (usually within 28 days of the change). Failure to notify such changes is punished by an AUD 10 700 fine and/or one year of imprisonment. ASIC also has the power to require a company to respond to a return of particulars (section 348A of the Corporations Act), which may be issued at any time. Failure to respond to such notice is also liable of an AUD 10 700 fine. Every year, on the anniversary date of their registration, legal persons registered with ASIC are subject to an Annual Review Process for the purposes of updating their information registered in the public register. The register of members kept at the registered office of the company must also be kept up to date. However, Australia has not indicated any mechanism to ensure that information on the registers of members kept by companies is accurate, as no diligence to verify the information recorded is required (however, it is an offence under section 1308(2) of the Corporations Act to provide false or misleading information to ASIC; moreover, shareholders may take legal action under section 175 to correct the register).

a7.8. **Criteria 24.6 and 24.7** – While the Corporations Act requires companies to obtain and hold accurate and up-to-date information on the direct owner of the shares of a company there is no requirement in the Act for companies or ASIC to obtain and hold up-to-date additional information to determine the ultimate natural person who is the beneficial owner beyond the immediate shareholder. Nor are companies required to take reasonable measures to obtain and hold this information. As a result, beneficial ownership information is only recorded if the legal owner of the share certificate happens to be the beneficial owner. For public companies (listed company or listed investment scheme) Australia also relies on the provisions of Part 6C.2 of the Corporations Act, according to which ASIC or a company can require any person to disclose the name and address of another person, who has a relevant interest in any of the shares or interests of a public company, or the name and address of each person who has given the person instructions about acquisition, exercise or any other matter relating to the shares. The information disclosed must be recorded in a register kept by the company. This mechanism also provides information on the beneficial owner if the person having an interest or having given instructions happens to be the beneficial owner. It is also not clear how beneficial ownership information could be obtained on foreign companies, which may register with ASIC but which must only maintain a local agent (who can be a natural or legal person). Pursuant to the introduction of the 2014 AML/CTF Rules, reporting entities are now required to identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner (see Recommendation 10.5). For all the information above, Australia has not indicated any mechanism to ensure that the information collected is accurate, as no diligence to verify the information recorded is required.

a7.9. **Criterion 24.8** – Australia partly addresses this issue (through criterion 24.8(a)) by requiring proprietary companies to have at least one director ordinarily resident in Australia. Public companies must have at least three directors, and at least two of them must ordinarily reside in Australia. Proprietary companies must notify ASIC about the details of the top 20 members for each class of shares, including whether the shares are not held beneficially. Companies other than proprietary companies must have a company secretary. ASIC can request and/or compel information that is available from the resident directors and secretaries, but only in relation to the information that this person(s) holds or has knowledge about. Foreign registered companies must have at least one local agent ordinarily resident in Australia, who may be liable for breaches of the Corporations Act.

a7.10. **Criterion 24.9** – The Corporations Act requires that the directors of deregistered companies (or companies which otherwise cease to exist) maintain the books and records of the company ("books" is defined in the Act to include virtually all company records including the members' (shareholders') register, etc.) for a period of three years from the time a company is de-registered. Section 286 of the Act requires financial records to be held for at least five years. Subsection 542(2) of the Corporations Act also requires liquidators to keep books and records for five years. There is no specific provision applicable to ASIC in this context.

A7

a7.11. **Criterion 24.10** – ASIC has sweeping statutory authority to require disclosure of all information held by corporations established under the Corporations Act by virtue of Part 3 of the *Australian Securities and Investment Commission Act 2001* (ASIC Act). ASIC also has the power to issue tracing notices under Part 6C.2 of the ASIC Act (see also criterion 24.6 above). These powers include powers to require production, inspection,

disclosure, attendance, compelling assistance, and other wide powers (including warrants). The AFP and State/Territory Law enforcement authorities in Australia also have wide powers to secure ownership, control and other information from companies incorporated under the Corporations Act.

a7.12. **Criterion 24.11** – Corporations established under the Corporations Act are prohibited from issuing bearer shares (section 254F). There is no prohibition on corporations issuing bearer share warrants. While rarely seen, there are no mechanisms, statutory or otherwise, to mitigate the risk of ML and/or TF posed by these instruments.

a7.13. **Criterion 24.12** – Nominee shareholders and nominee directors are permitted under the Corporations Act. Australia applies the following mechanisms aiming to ensure that such nominees are not abused:

- With respect to nominee shareholders, a shareholder may hold shares for the benefit of another person (including a legal person) either as trustee or nominee or otherwise on behalf of, or on account of, another person. In those cases, under section 1072H of the Corporations Act the shareholder of such shares must advise the company that he/she/it is holding those shares “non-beneficially” and the company must indicate in the share register that those shares are not held beneficially (section 169(5A)). Failure to comply with this requirement is an offence under the Act (section 1311(1)) attracting penalties. ASIC’s power to trace beneficial owners of shares for publicly listed entities (Part 6C.2 of the Corporations Act) means that, where applicable, nominee shareholders are required to disclose the identity of the nominator. The information disclosed must be kept in the company’s register. This mechanism does not apply to the vast majority of legal entities – only to public companies.
- With respect to nominee directors, the Corporations Act refers to these as “alternate directors” (section 201K). A company must notify ASIC within 28 days if a person is appointed as an alternate director. The following details are required when appointing an alternate director: full name and any former names; date and place of birth; residential address; date of appointment; the name of the director for whom the individual is an alternate; and the expiry date (if applicable). If the appointment is open-ended, they must provide the date of appointment only and the terms of appointment. These must include details such as the timeframe of the appointment, capacity to sign instruments and attend meetings.

a7.14. **Criterion 24.13** – ASIC has a range of administrative, civil and criminal remedies under the Corporations Act. The failure to comply with some statutory requirements constitutes an offence punishable by monetary penalties or terms of imprisonment. For example:

- Failure to maintain a member’s register - maximum penalty of AUD 1 170 or imprisonment for three months or both for an individual and AUD 8 500 for a company.
- Failure to notify ASIC about a change to a member register or a change to the company’s share structure - maximum monetary penalty of AUD 10 200 for an individual and AUD 51 000 for a company.
- Failure to notify ASIC about the appointment/cessation of a director or a change in a director’s address - maximum monetary penalty of AUD 10 200 or imprisonment for one year or both, and AUD 51 000 for a company.
- Failure of a person to comply with a tracing notice under Part 6C.2 - maximum monetary penalty of AUD 4 250 or six months imprisonment or both for an individual and AUD 21 250 for a company.
- The Court may disqualify persons from managing corporations in certain circumstances, including repeated contraventions of the Corporations Act.

a7.15. **Criterion 24.14** – Australia is able to provide international co-operation through a range of mechanisms (see Recommendations 37-40 below), including any and all information relating to directors and

## LEGAL PERSONS AND ARRANGEMENTS

shareholders. In addition ASIC has a number of MOUs with both countries and international organisations, and it is also a signatory to the IOSCO Multilateral Memorandum of Understanding. These arrangements are published on ASIC's public website. Public information on legal persons from the ASIC website is also available to foreign competent authorities, and the site is structured to assist with other regulators who are not party to an MOU to request information from ASIC.

a7.16. **Criterion 24.15** – There is no information that Australia monitors the quality of assistance it receives from other countries in response to requests for basic and beneficial ownership information or requests for assistance in locating beneficial owners residing abroad. However, Australia advised that its competent authorities regularly provide feedback to the authorities from which they have received assistance, see also Recommendation 40.

### *Weighting and Conclusion*

a7.17. There are some measures in place to prevent the misuse of legal persons for ML and TF purposes. The registration processes and the necessary supporting information implemented either by the federal, the States or the Territories are diverse. There are a number of deficiencies with respect to the beneficial ownership of legal persons and 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. There are some measures to improve the transparency of legal persons which can have nominee shareholders and alternate directors. **Recommendation 24 is rated partially compliant.**

## **Recommendation 25 – Transparency and beneficial ownership of legal arrangements**

a7.18. Australia received a partially compliant rating for Recommendation 34 (the predecessor to Recommendation 25) in the 2005 assessment, Australia has not reported any progress in relation to correcting the deficiencies noted in relation to Recommendation 34. The assessment noted that “overall the mechanisms to obtain and have access in a timely manner to beneficial ownership and control of legal arrangements, and in particular the settlor, the trustee, and the beneficiaries of express trusts, are insufficient.”

a7.19. **Criterion 25.1** – There is no requirement in Australian law (federal, state or territorial law) that requires trustees of express trusts to obtain and hold adequate, accurate and current information on the identity of settlors, trustees, protectors (if any) and beneficiaries of trusts, including any natural person who exercises ultimate effective control over a trust. While trusts that receive income are required to file a tax return with the ATO, and in doing so state who the trust beneficiaries are, the requirement to state those beneficiaries extends only to the direct beneficiary under a trust and not to other beneficiaries (for instance the shareholders of corporate trust beneficiaries).

a7.20. **Criterion 25.2** – There is no legal requirement for information on trustees, beneficiaries, settlors and others such as protectors (if any) to be held up-to-date and accurate.

a7.21. **Criterion 25.3** – There is no explicit obligation on trustees to disclose their status when entering into a business relationship or conducting an occasional transaction with a financial institution entity or a DNFBP (it is an offence to omit to provide information when entering into a business relationship with a reporting entity where omission of that information would mean that what information is given is misleading under section 139 of the AML/CTF Act). There are however obligations on reporting entities providing designated services. These obligations are described in detail under criteria 10.9 and 11, above.

a7.22. **Criterion 25.4** – There are no prohibitions in law on trustees providing trust-related information to competent authorities.

a7.23. **Criterion 25.5** – Competent authorities including law enforcement (AFP and ACC), tax authorities, and AUSTRAC have powers to obtain information relating to trustees, beneficiaries, trustee residence and assets managed under a trust.

A7

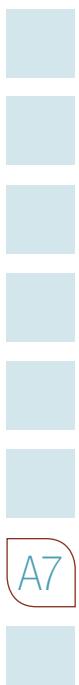
a7.24. **Criterion 25.6** – There is no framework at a State/Territory level governing the exchange of information in relation to trusts. Domestic and international exchanges could be accomplished only within the framework of a criminal investigation, and the use of MLA requests. At the federal level information may be exchanged domestically when agency secrecy requirements allow and MOUs exist between relevant agencies, which hold information relevant to trusts (the ATO and ACNC) and through double tax agreements and international information exchange agreements with foreign counterparts.

a7.25. **Criterion 25.7** – Trust law is contained in State legislation. NSW is the largest state in Australia. Under the NSW Trustee Act 1925, penalties for trustees who fail to perform their duties are not proportionate and dissuasive. The only penalties available in NSW are removal of the trustee (which is not a sanction) or a civil claim for equitable restitution/compensation (also not a sanction) by an affected beneficiary. The Trustee Act 1925 does not provide for fines or other civil or administrative measures to address breaches of obligations imposed upon trustees. Trustees who commit fraud on beneficiaries may be liable under criminal law but not for breaches of the law applicable to them as trustees – only under general criminal law. However, trustees are also legally liable for any failure to perform the duties relevant to meeting the obligations of the trust, as trusts are not separate legal entities. Measures applicable to trustees include the restoration of loss, the account of profit or the liability for legal costs. Injunctive relief is also available against trustees.

a7.26. **Criterion 25.8** – There are proportionate and dissuasive sanctions available (criminal, civil or administrative) to enforce the requirement to grant competent authorities access in a timely manner to information where held regarding trusts. Section 49 of the AML/CTF Act permits a number of agencies to issue notices subject to civil penalties (sections 49(2) and (3)); failure to comply with the ATO's information gathering powers under the *Income Tax Assessment Act 1936* may result in administrative penalties being applied; and the ACC Act and POCA contain criminal penalties where the relevant agencies are not allowed access.

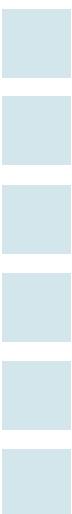
### *Weighting and Conclusion*

a7.27. 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. **As a result, Recommendation 25 is rated non-compliant.**



A7

## LEGAL PERSONS AND ARRANGEMENTS



A7



## 8. INTERNATIONAL COOPERATION

### Recommendation 36 – International instruments

a8.1. Australia received a largely compliant rating for Recommendation 35 (the predecessor to Recommendation 36) in the 2005 MER. One deficiency was noted, namely that Australia has not fully implemented the TF Convention because of insufficient measures to identify beneficial owners of accounts and transactions. Recommendation 35 was not addressed in mutual evaluation follow-up reports given the strength of the rating for the recommendation.

a8.2. **Criterion 36.1** – Australia ratified the following instruments (with dates):

**Table A8.1. Instruments ratified by Australia**

Title	Date	Comments
Vienna Convention	16 November 1992	no reservations
Terrorist Financing Convention	26 September 2002	no reservations
Palermo Convention	27 May 2004	no reservations
Merida Convention	7 December 2005	no reservations

a8.3. **Criterion 36.2** – Deficiencies in the TF offence (i.e. the scope of terrorist acts in the TF Convention covered) affect the implementation of the TF convention (see Recommendation 5).

### *Weighting and Conclusion*

a8.4. Australia has ratified all the relevant Conventions. In terms of implementation, Australia has implemented most of the relevant articles; however, deficiencies in the TF offence affect the implementation of the TF Convention. **Recommendation 36 is rated largely compliant.**

### Recommendation 37 - Mutual legal assistance

a8.5. Australia received a compliant rating for Recommendation 36 and a largely compliant rating for Special Recommendation V (both of which are the predecessors to the combined new Recommendation 37) in the 2005 MER. Neither of the previous recommendations were the subject to follow-up reporting by Australia on the basis of the ratings. The requirements in (new) Recommendation 37 are much more detailed.

a8.6. **Criterion 37.1** – The *Mutual Assistance in Criminal Matters Act 1987* (MACMA) (amended in 2012 to streamline procedures) provides a basis for legal assistance to foreign jurisdictions. Section 11 provides the federal Attorney-General with general power to receive requests from foreign countries. Section 9 provides that assistance may be provided to a foreign country subject to conditions determined by the Attorney-General. MLA treaties are not required in Australia to render assistance. However, Australia has concluded up to 29 MLA treaties (which may be necessary in order for Australia to request assistance from other jurisdictions). Under the MACMA, Australia may provide assistance as follows:

- Non-coercive powers: no applicable offence threshold applies – it must simply be a ‘criminal matter’. Australia can prioritise requests relating to foreign ‘serious offences’ attracting a maximum penalty of imprisonment for at least 12 months, death, or a fine exceeding 300 penalty units.
- Coercive measures: MACMA section 13(1A) and following sections provide for such measures as taking of evidence for criminal proceedings, provision of material, applying for search and/or surveillance warrants, authorisation for proceeds of criminal restraints, etc.

A8

## INTERNATIONAL COOPERATION

a8.7. Australia can also make MLA requests to obtain documents and other evidence (e.g. witness testimony) from foreign countries in a form admissible in Australian courts under the *Foreign Evidence Act 1994*.

a8.8. **Criterion 37.2** – The Australian Central Authority (ACA) within the AGD is Australia's central authority for MLA. The AGD maintains a website that contains fact sheets and other information for countries wishing to make MLA requests to Australia. The ACA also maintains a case management system which records the details of each MLA request. Case officers are responsible for updating the database, and can utilise a function which sets up a timeline of 'next actions' for the case officer to complete certain actions to process the request. The database is accessible by case officers only.

a8.9. **Criterion 37.3** – MACMA section 8(1), (1A) outlines mandatory grounds and section 8(1B) outlines discretionary grounds for the Attorney-General to refuse foreign assistance requests. None of the grounds stipulated in those sections are unreasonable or unduly restricted. They relate, for instance, to requests for assistance where offences are of a political nature or where the death penalty or torture might apply. In addition, section 13 states that there must be a "proceeding" in the foreign country before the Minister can issue an authorisation to take evidence. That term is defined in section 3(1) to include an inquisitorial proceeding before an investigative Magistrate or a grand jury but does not include a criminal investigation. Section 15 allows the use of search and seizure powers based on a request for use in both proceedings and investigations.

a8.10. Discretionary provisions provide that a request may be refused if the provision of the assistance may result in the death penalty being imposed on a person; and after taking into consideration the interests of international criminal co-operation in the circumstance of the case, the request should not be granted (section 8(1B)). Section 9 of MACMA allows the Attorney-General to render the assistance and impose conditions on the requesting country.

a8.11. **Criterion 37.4** – Assistance is not refused on the sole ground that the offence involves fiscal matters, as this is not a ground for refusal under section 8 of the MACMA. Nor is assistance refused on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions or DNFBPs.

a8.12. **Criterion 37.5** – Section 43C of the MACMA provides that a person must not intentionally disclose the existence or nature of an MLA request received by Australia, except insofar as is necessary for the performance of his or her duties (in executing the request), or with the approval of the Attorney-General. An offence against this section carries a penalty of imprisonment for 2 years. A confidentiality clause is also included in the majority of bilateral treaties Australia has concluded on MLA. Further, officers of the ACA who are involved in handling MLA request are subject to section 79 of the Crimes Act , which deals with official secrets. Breaches of this section are an offence under Australian law. Officers also hold security clearances and operate under the 'need to know' principle when sharing information within Government.

a8.13. **Criterion 37.6** – Under section 8(2) of the MACMA a request by a foreign country for assistance may be refused if, in the opinion of the Attorney General, the request relates to the investigation, prosecution or punishment of a person in respect of an act or omission that, if it had occurred in Australia, would not have constituted an offence against Australian law at the time at which the request was received. Dual criminality is, therefore, a discretionary ground of refusal in relation to requests for all assistance (whether the request involves coercive measures or otherwise). If Australia does provide assistance when the offence for which assistance is required is not an offence in Australia, section 9 of the MACMA allows the Attorney-General to impose conditions on the requesting state. Hence, Australia does have a mechanism to provide MLA if dual criminality is a presumptive requirement.

a8.14. **Criterion 37.7** – Australia assesses the alleged conduct of the person to determine whether that conduct, had it taken place in Australia, would constitute an offence under Australian law at the time that the request was received. The dual criminality test does not require that the foreign offence and the notional Australian offence be comprised of the same elements. Australia does not place a focus on the categorisation of the offence but on the alleged underlying conduct involved. Moreover, if an equivalent and qualifying Australian offence could be established based on any part or parts of the total foreign conduct, then dual criminality may be established.

a8.15. **Criterion 37.8** – Australia has a range of powers and investigative techniques available in the international context for MLA request. Those powers under MACMA include:

- The production, search and seizure of information, documents or evidence (including financial records) from financial institutions or other natural or legal persons: Sections 12-13 allow Australia to seek and provide a document or other article. Sections 14-15 allow Australia to seek and provide material obtained by search and seizure subject to the provisions of the MACMA.
- Witness statements: Voluntary witness statements can be obtained at any time including the early investigative stage without the need for a formal MLA request, since this is not a coercive power. Under section 13, a witness who is not a suspect can be compelled to give evidence or produce documents before a court, including via video-link to the foreign court, if foreign proceedings are on foot. Sections 26-27 facilitate the travel of a person in custody to voluntarily give evidence in a foreign proceeding.
- Service of documents: While many of Australia's bilateral treaties specifically refer to the service of documents as a type of assistance that may be provided, Australia will consider a request for service of documents from any country.
- A broad range of other powers and investigative techniques: Surveillance devices (Part IIIBA, section 15C), stored communications warrants (Part IIIA, section 15B), telecommunications data (Part IIIB, section 15D), and forensic procedures (Part IVA, section 28).

### *Weighting and Conclusion*

a8.16. **Recommendation 37 is rated compliant.**

## **Recommendation 38 – Mutual legal assistance: freezing and confiscation**

a8.17. Australia received a C rating for Recommendation 38 (numbered the same in the 2013 assessment Methodology) in the 2005 assessment.

a8.18. **Criterion 38.1** – Australia can identify, freeze, seize or confiscate the proceeds or an instrument of a foreign serious offence on request by another country. A foreign serious offence is defined as an offence against a law of a foreign country, the maximum penalty for which is death, imprisonment for a period exceeding 12 months or a fine exceeding 300 penalty units (being AUD 51 000). Sections 34 –35M of the MACMA set out requirements for receiving and dealing with requests made by foreign countries. These provisions provide for the enforcement of foreign orders, including: forfeiture orders (which include laundered property and proceeds), pecuniary penalty orders (which designate a value rather than a property), restraining orders, production orders, monitoring orders, and search warrants to identify and seize property. Action can also be taken against the instruments of offences (used in or intended for use in) if the action is conviction based.

a8.19. **Criterion 38.2** – Section 34(2) of the MACMA provides for the registration and enforcement of non-conviction based foreign forfeiture orders and foreign pecuniary penalty orders. This provision enables the forfeiture of property that is, or is alleged to be, the proceeds or an instrument of a serious foreign offence, or the benefit derived from a serious foreign offence, regardless of whether the person alleged to have committed the offence has been convicted of that offence, or whether charges have been laid against that person. Section 34(3)(b) of the MACMA enables a non-conviction based foreign restraining order to be enforced over property where the identity of the person who committed the serious foreign offence is not known.

a8.20. **Criterion 38.3** – Seizure and confiscation actions are coordinated by the ACA, the central authority for extradition and MLA, in partnership with the CACT within the AFP. Casework officers liaise with government departments and law enforcement on MLA requests.



A8

## INTERNATIONAL COOPERATION

a8.21. The AFP also coordinates arrangements with other countries relating to seizure and confiscation action. Section 34B of the MACMA provides that property subject to a foreign forfeiture order may be disposed of, or otherwise dealt with, in accordance with any direction of the Attorney-General or of a person authorised by the Attorney-General in writing. Section 34D of the MACMA provides that a foreign pecuniary penalty order may be enforced as if it were a debt due to the federal government. Money paid to the federal government under a foreign pecuniary penalty order registered under section 34 of the MACMA is credited to the Confiscated Assets Account. Section 297 of the POCA sets out a number of mechanisms for managing, and when necessary, disposing of payments made into the Confiscated Assets Account. The way in which restrained property is dealt with is covered by Division 3, Part 4-1 of the POCA (section 35C of the MACMA). However, before disposing or destroying of property, the Official Trustee must consult with the foreign country that made the request relating to the property covered by the foreign restraining order (see section 35C(2) of the MACMA and section 278 of the POCA).

a8.22. **Criterion 38.4** – Legislation allows Australia to share confiscated proceeds of crime with any country in the absence of any specific treaty obligations. Under the POCA, the federal Minister for Justice can approve the sharing of confiscated assets with a foreign country if, in the Minister's opinion, the foreign country has made a significant contribution to the recovery of those proceeds or to the investigation or prosecution of the unlawful activity. Australia has bilateral MLA treaties with 29 countries. These treaties generally include provisions relating to dealing with confiscated assets. Additionally, Australia has ratified a number of international conventions that have proceeds of crime and asset sharing provisions, including the Merida Convention. Any request for sharing proceeds of crime made under the Merida Convention, or by a country with which Australia has ratified a MLA treaty that has obligations with respect to proceeds of crime, will be considered by Australia in accordance with the terms of the treaty.

### *Weighting and Conclusion*

a8.23. **Recommendation 38 is rated compliant.**

## Recommendation 39 – Extradition

a8.24. Australia received a compliant rating for Recommendation 39 in the 2005 assessment. In 2012, Australia amended the *Extradition Act 1988 (the Extradition Act)* in order to streamline and modernise the extradition process further. The reforms aim to reduce the length of the process, including the amount of time a person spends in custody, in new and ongoing extradition cases. In particular, the amendments:

- Enable a person to elect to waive the extradition process entirely, subject to appropriate safeguards
- Aim to reduce the time spent by persons in Australian custody, by streamlining the early stages of the extradition process, subject to safeguards
- Extend the availability of bail to the later stages of extradition proceedings, and
- Enable a person to be prosecuted in Australia where extradition has been refused ensuring that refusal to extradite does not mean that a person escapes justice.

a8.25. **Criterion 39.1** – Extradition is governed by the Extradition Act. The Act applies when a country is designated as an "extradition country". This designation generally occurs by way of domestic regulation. Australia has designated by regulation extradition countries individually, with countries which it has treaty and for countries without a treaty, for a group of Commonwealth countries under the London Scheme, and for all countries automatically that are also parties to the Vienna, Palermo, Merida, and CTF Conventions. Countries that have an extradition treaty with the UK, which was inherited by Australia, fall within the definition of "extradition country" without the need for designation by regulation. These provisions make ML and TF extraditable offences in Australia. Under the Extradition Act, generally a person can be surrendered for an "extradition offence", which is an offence against the law of the other country (i.e. the requesting country) punishable by at least 12 months imprisonment. Dual criminality is also a requirement for extradition (section 19(2)). ML is criminalised in the Criminal Code and applies to all serious offences. While deficiencies

in relation to the TF offence have been identified, the underlying conduct of TF has been criminalised with a broad range of TF offences. Therefore, the deficiencies in the TF offence do not apply to Recommendation 39 as the classification of the offence does not affect dual criminality requirements.

a8.26. The Extradition Unit within the ACA coordinates extradition requests. The Unit maintains a casework database allowing cases and ‘next-steps’ to be monitored. It also has processes and practices in place to execute matters in a timely fashion and to prioritise cases effectively. Extradition requests may also involve a number of other agencies including the CDPP, the AFP and other Commonwealth, State or Territory law enforcement, revenue or regulatory bodies. The ACA represents the foreign country in extradition proceedings in Australia. The CDPP only has a role in outgoing extradition cases if the matter is being prosecuted by the CDPP.

a8.27. There are no unreasonable or unduly restrictive conditions on extradition. Section 15B(3) allows the Attorney-General to refuse extradition if the person sought in Australia may be subject to torture or the death penalty. Section 7 of the Extradition Act also provides for “extradition objections” to be determined which relate to offences of a political character, prejudice on account of race, religion etc., offences solely under military law and not the ordinary criminal law, and cases of double jeopardy.

a8.28. **Criterion 39.2** – Australia does not refuse extradition on the basis of nationality. Section 45 of the Extradition Act contains provision for prosecution in lieu of extradition of any person (including Australian citizens). The Attorney-General can consent to a such a prosecution only after: 1) determining not to surrender the person to an extradition country; 2) being satisfied that the conduct occurring outside Australia would have constituted a “notional Australian offence” under the law of the federal government, State or Territory of Australia had it occurred there.

a8.29. **Criterion 39.3** – Under section 19 of the Extradition Act, the dual criminality requirement is assessed as part of a broader assessment of a person’s eligibility for surrender. Section 19(2)(c) sets out the test for when dual criminality is satisfied. Section 10 provides further detail on the interpretation of provisions relating to offences. Section 10(3) provides:

- Where the conduct or equivalent conduct consists of two or more acts or omissions, regard may be had to all or to only one or some of those acts or omissions, and
- Any difference between the denomination or categorisation of offences under the law of the country and the law of Australia, or the law in force in the part of Australia, as the case requires, shall be disregarded.

a8.30. Australia does not therefore assess the dual criminality requirement based on the categorisation or the terminology used to describe the relevant offences.

a8.31. **Criterion 39.4** – There are a number of provisions in the Extradition Act for simplified processes. For instance:

- Part II of the Act provides for simplified extradition procedures between Australia and New Zealand known as the ‘backing of warrants scheme’. The scheme is administered by the police forces in Australia and New Zealand.
- A person may waive their participation in the extradition process subject to certain safeguards. If a person elects to waive the extradition process, not all stages in the extradition process will need to be completed and consequently the time the person spends in custody in Australia can be reduced. A person can elect to waive the process once they have been arrested in Australia (either pursuant to a provisional arrest request or a full extradition request). A person may waive their participation in the extradition process for their return to the requesting country for offences which are ‘extradition offences’ and those which are not classed as such (i.e. those that are punishable by less than 12 months’ imprisonment). If satisfied, the magistrate must commit the person to prison or on bail pending the Attorney-General’s determination whether the person should be surrendered to the requesting country.

## INTERNATIONAL COOPERATION

a8.32. While extradition requests made and received by Australia are transmitted formally through the diplomatic channel, provisional arrest requests can be made and received directly from central authorities or through the Interpol channel. This assists in not delaying the delivery of such requests given the urgency and time sensitivities associated.

### *Weighting and Conclusion*

a8.33. Australia has comprehensive measures for extradition. **Recommendation 39 is rated compliant.**

## **Recommendation 40 – Other forms of international cooperation**

a8.34. Australia received a compliant rating in 2005 for Recommendation 40. The requirements in new Recommendation 40 are considerably more detailed.

a8.35. **Criterion 40.1** – Australian competent authorities including AUSTRAC, AFP, ACC, APRA and ASIC can provide a range of information to their foreign counterpart authorities in relation to ML, predicate offences and TF. Information can be shared both simultaneously and upon request.

a8.36. **Criterion 40.2** –

- 1.** The competent authorities have a lawful basis for providing cooperation. (AUSTRAC: AML/CTF Act, section 132; AFP: the AFP Act), section 8(1) and AML/CTF Act section 132; ACC: the ACC Act , section 59AA, AML/CTF Act, section 132; APRA: the APRA Act ,sections 56(5) (a)–(b); ASIC: the ASIC Act, section 127(4); the NSW Police Force: section 6(2)(c) of the *Police Act 1990* (NSW); the New South Wales Crime Commission (NSWCC): section 13 of the *Crime Commission Act 2012* (NSW); the Queensland Crime and Corruption Commission (QCCC): section 55 of the *Crime and Corruption Act 2001*.)
- 2.** Government agencies in Australia are not only authorised to use the most efficient means to cooperate within existing frameworks, they are required to do so.
- 3.** All authorities use clear and secure gateways, mechanisms or channels. The AML/CTF Act allows AUSTRAC and designated law enforcement and national security agencies to communicate AUSTRAC information with foreign counterparts. AUSTRAC had 67 exchange instruments with counterpart foreign financial intelligence units (FIUs) effective in 2014. AUSTRAC uses Egmont's secure web as the primary channel for international exchange. ASIC has a clear and secured gateway for foreign requests; a dedicated email address is available on the ASIC's website. ASIC plans to improve the level of security of the information exchanged with foreign counterparts in 2015, through for example enhanced encryption. Section 127 of the ASIC Act provides that information received from foreign regulators, including their requests, is treated as confidential information. ASIC complies with the requirements of the Protective Security Policy Framework (PSPF). APRA also communicates and exchanges information with foreign counterparts using encryption tools. State and Territory law enforcement agencies use the AFP Liaison Officer network. Where necessary, State and Territory police services enter into Memoranda of Understanding with the AFP.
- 4.** The competent authorities have processes for prioritising and executing requests: the ACC and ASIC have dedicated teams for coordinating and responding to foreign requests within a maximum of 28 days. The ACBPS also has a dedicated unit for the coordination and operational assistance to and from foreign counterparts. ASIC has a dedicated team, International Cooperation Requests (ICR), which coordinates international requests to and from ASIC. ICR has key performance indicators of 14 days to send out requests and 28 days to respond to international requests. These are subject to complexity of requests, resourcing and other operational issues. Priority is given to requests relating to enforcement matters.

A8

Requests made pursuant to the International Organisation of Securities Commissions (IOSCO) Multilateral Memoranda of Understanding (MMOU) and bilateral Memoranda of Understanding (MOUs) that require authorisation under the *Mutual Assistance in Business Regulation Act 1992* (MABRA) are given highest priority. ICR has and maintains a database (OIRs), which has built in milestones for acknowledgement and request sent/response sent. There is also an ability to categorise an activity as urgent.

5. The competent authorities have clear processes for safeguarding the information received. The PSPF sets for all agencies detailed requirements for a number of matters, including information asset classification. Agencies are also required to have internal policies to manage and protect the records, as well as to ensure that records are retained, classified, and filed. They are also required to have Information Security Policies for securing information, security classification and protective markings, dissemination limiting markers, handling, access and control. The following legislative instruments prescribe details regarding the protection of information held by APRA and ASIC: section 56 of the APRA Act and section 127 of the ASIC Act. Section 60A (Secrecy) of the AFP Act places specific constraints on the AFP in relation to the disclosure of prescribed information.

a8.37. **Criterion 40.3** – AUSTRAC has entered into a range of agreements to give effect to multilateral or bilateral arrangements; APRA and ASIC have entered into Memoranda of Understanding (MoUs) and Multilateral Memoranda of Understanding (MMoUs) with a wide range of foreign counterparts.<sup>1</sup> Similarly, the AFP relies on a range of police-to-police and government-to-government MoUs<sup>2</sup>.

a8.38. **Criterion 40.4** – AUSTRAC seeks feedback from foreign counterparts on assistance received in a timely manner. ASIC also sends feedback to the International Organisation of Securities Commissions (IOSCO), of which it is a member, on the quantity and quality of information exchanged pursuant to the IOSCO Multilateral MoU. APRA participates in international surveys on information exchange and cooperation arrangements conducted through international standard setting bodies such as the International Association of Insurance Supervisors.

a8.39. **Criterion 40.5** – The relevant statutes and agreements that empower the sharing of information by competent authorities as identified in Criterion 40.2 above do not unduly restrict information exchange. Where the statutory provisions provide for an approval process, information sharing is generally limited only by the requirement to establish that the foreign request is relevant and proportionate.

a8.40. **Criterion 40.6** – The MOU which facilitates the exchange of information by competent authorities contains confidentiality provisions which safeguard against improper disclosure of information. Authorities also have the discretion to impose additional conditions to safeguard exchanged information. See, for example, section 56 of the APRA Act and section 127(1) of the ASIC Act. Internal policies of Australian agencies (federal, State and Territory) prioritise the protection of information received from international bodies. It is

---

<sup>1</sup> For a full list of these, please refer to [www.apra.gov.au/AboutAPRA/Pages/ArrangementsandMoUs.aspx](http://www.apra.gov.au/AboutAPRA/Pages/ArrangementsandMoUs.aspx) and [www.asic.gov.au/asic/asic.nsf/byheadline/OIR+-+Memorandum+of+Understandings?openDocument](http://www.asic.gov.au/asic/asic.nsf/byheadline/OIR+-+Memorandum+of+Understandings?openDocument).

<sup>2</sup> See:  
[www.afp.gov.au/media-centre/news/afp/2005/June/singapore-and-australia-sign-cooperation-agreement.aspx](http://www.afp.gov.au/media-centre/news/afp/2005/June/singapore-and-australia-sign-cooperation-agreement.aspx)

[www.afp.gov.au/media-centre/news/afp/2012/july/the-afp-and-fbi-unite-against-terrorism-and-transnational-crime.aspx](http://www.afp.gov.au/media-centre/news/afp/2012/july/the-afp-and-fbi-unite-against-terrorism-and-transnational-crime.aspx)

[www.afp.gov.au/media-centre/news/afp/2011/november/AFP-and-Indonesian-National-Police-sign-new-agreement-to-combat-transnational-crime.aspx](http://www.afp.gov.au/media-centre/news/afp/2011/november/AFP-and-Indonesian-National-Police-sign-new-agreement-to-combat-transnational-crime.aspx)

[www.afp.gov.au/media-centre/news/afp/2012/february/AFP-and-serbian-police-sign-new-agreement.aspx](http://www.afp.gov.au/media-centre/news/afp/2012/february/AFP-and-serbian-police-sign-new-agreement.aspx)

## INTERNATIONAL COOPERATION

a standard operational principle of law enforcement bodies that the information received can only be used for the purposes for which it was provided.

a8.41. **Criterion 40.7** – For AUSTRAC, international exchange information is classified with a protective marking applied to information covered by a specific secrecy provision of an Act, consistent with the PSPF. Part 11 of the AML/CTF Act provides the secrecy provisions in this case. Security containers and system controls provide physical and online protection to stored information. The PSPF protects information holdings, including international exchange information. The provisions allow competent authorities to refuse to disclose information where the requesting competent authority is unwilling or unable to agree with the conditions of disclosure.

a8.42. **Criterion 40.8** – AUSTRAC conducts enquiries within Australia on behalf of foreign counterparts. In addition, sections 8–10 and 18 of the MABRA empower competent authorities (i.e. ASIC and APRA) to provide assistance in response to a request from a foreign regulator. While APRA can only provide such assistance with Ministerial approval (section 8), ASIC senior staff can exercise the Minister's power to authorise the obtaining of information or documents.

a8.43. **Criterion 40.9** – AUSTRAC has an adequate basis for international cooperation on issues related to ML, predicate offences and TF under section 132(1) of the AML/CTF Act. That section authorises AUSTRAC to provide information so long as the foreign government provides undertakings to protect confidentiality, controls the use of the information and ensures that the information should only be used for the purpose for which it is communicated.

a8.44. **Criterion 40.10** – AUSTRAC provides feedback to foreign countries on a range of matters, including on behalf of other Australian domestic agencies receiving information from overseas as the result of a spontaneous disclosure or in response to a request. AUSTRAC has provided feedback on such matters as: the timeliness of the response by the overseas FIU; whether Australian agencies were already aware of the information; and if new information was relevant, how the information was used and whether spontaneous disclosures led to further requests for information. Feedback is requested routinely following each international exchange.

a8.45. **Criterion 40.11** – Section 132(1) of the AML/CTF Act authorises AUSTRAC to communicate AUSTRAC information, including information from reporting entities obtained by authorised officers under AUSTRAC's information-gathering and enforcement powers. Company and business information from ASIC is also exchanged with foreign FIUs. Information obtained by AUSTRAC from a government body becomes AUSTRAC information and is subject to the same protections afforded under the AML/CTF Act.

a8.46. **Criterion 40.12** – As noted earlier, AUSTRAC has statutory authority under the AML/CTF Act to cooperate with foreign counterparts, ASIC and APRA have authority to do so under the MABRA. APRA is also authorised to disclose information to foreign counterparts under section 56 of the APRA Act; ASIC can also release information it holds to assist foreign counterparts pursuant to section 127(4) of the ASIC Act.

a8.47. **Criterion 40.13** – Financial supervisors are able to acquire information from financial institutions and share them with foreign counterparts under the authority of sections 8–10 and 18 of the MABRA. While APRA can only provide such assistance with ministerial approval (section 8), ASIC senior staff are able to exercise the Minister's power to authorise the provision of information, documents or evidence. ASIC and APRA are also able to share the information available to them through their routine operations; section 127(4) of the ASIC Act and sections 56(5)(a)–(b) of the APRA Act.

a8.48. **Criterion 40.14** – APRA and ASIC are not restricted from sharing regulatory and prudential information that is not institution-specific. ASIC can share with foreign agencies the information it holds on financial institutions' business activities, beneficial ownership, and fit and properness under the conditions set in section 127 of the ASIC Act. Disclosure of information on financial institutions' activities by APRA is authorised under certain conditions by section 56 of the APRA Act. It is further provided in section 56(3) of the APRA Act that institution-specific information can be released where the information is disclosed for the purposes of a prudential regulation framework law. APRA and ASIC are also designated agencies under the AML/CTF Act, which gives them access to AUSTRAC information.

a8.49. **Criterion 40.15** – Financial supervisors can provide assistance to a foreign regulator under the MABRA; however, this requires Ministerial approval. See also criteria 40.2, 40.8, 40.13 and 40.18.

a8.50. **Criterion 40.16** – Information conveyed to Australian financial supervisors is protected by secrecy and confidentiality provisions in statutes and relevant MoU. See criteria 40.6 and 40.7 above.

a8.51. **Criterion 40.17** – Law enforcement authorities are able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes. Subsection 8(1)(bf) of the AFP Act includes, as an AFP function, the provision of police services and police support services for the purposes of assisting, or cooperating with, an Australian or foreign law enforcement, intelligence, security or government regulatory agency. “Police services” is defined as including services performed by way of the prevention of crime, including information exchange. “Police support services” includes any service *related to* the provision of services by an Australian or foreign regulatory, intelligence or security, or law enforcement agency. State and Territory police services and the AFP are able to exchange domestically available information with foreign counterparts through the AFP’s International Liaison Officer Network.

a8.52. **Criterion 40.18** – The AFP can use its powers to conduct inquiries, including investigative techniques, and obtain information on behalf of foreign counterparts under sections 8(1)(bf) of the AFP Act. The ACC is permitted to conduct inquiries and obtain information on behalf of foreign counterparts, in the exercise of its general intelligence power under section 7A(a) of the ACC Act. State and Territory law enforcement bodies are able to conduct inquiries on behalf of foreign counterparts under the authority of the MACMA.

a8.53. **Criterion 40.19** – The AFP’s powers provide a basis for the AFP to form joint investigative teams and establish bilateral or multilateral agreements where required. The ACC is afforded similar powers to form joint investigative teams and bilateral/ multilateral arrangements to enable joint investigations under section 17(2) of the ACC Act. ASIO is afforded similar powers in section 19(1)(c) of the *Australian Security Intelligence Organisation Act 1979* (Cth). State and Territory law enforcement bodies have been less likely to require the creation of such joint investigations. However, where the need arises, they have the authority to do so under the MACMA or under the broad authority they are given to perform their functions. See, for example, section 6(2)(c) of the *Police Act 1990* (NSW).

a8.54. **Criterion 40.20** – The relevant statutory provisions identified in response to criterion 40.2 are not limited to direct disclosures of information and do not require that the information only be transmitted between counterparts. For example, subsection 8(1)(bf) of the AFP Act includes, as an AFP function, the provision of police services and police support services for the purposes of assisting, or cooperating with, an Australian or foreign law enforcement, intelligence, security, or government regulatory agency. The majority of information exchanges channelled through AUSTRAC each year is indirect in nature. AUSTRAC facilitates foreign exchanges with all its domestic partner agencies across the regulatory, law enforcement, revenue, intelligence and social justice spheres. Similar provisions for indirect cooperation are provided to APRA (section 56 of the APRA Act, and ASIC (section 127 of the ASIC Act).

### *Weighting and Conclusion*

a8.55. ASIC and APRA may conduct enquiries for purposes of complying with a request from a foreign regulator. As an FIU, AUSTRAC can also provide all the information to foreign requests as required by Recommendation 40; as a regulator, AUSTRAC can share all relevant information that it holds or that it can obtain from reporting parties. **Recommendation 40 is rated compliant.**



A8

## INTERNATIONAL COOPERATION



A8

## Table of Acronyms

ABN	Australian business number
ABR	Australian business register
ACA	Australian Central Authority
ACBPS	Australian Customs and Border Protection Service
ACC	Australia's Crime Commission
ACNC	Australian Charities and Not-for-Profits Commission
AFP	Australian Federal Police
AGD	Attorney General's Department
AIC	Australian Intelligence Community
AML	Anti-money laundering
APG	Asia/Pacific Group on Money Laundering
APRA	Australian Prudential Regulation Authority
ARSN	Australian registered scheme number
ASIC	Australian Securities and Investment Commission
ASIO	Australian Security Intelligence Organisation
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CACT	Criminal Asset Confiscation Taskforce
CDD	Customer due diligence
CDPP	Commonwealth Director of Public Prosecutions
CFT	Countering the financing of terrorism
CotUNA	Charter of the United Nations Act
CT	Combat terrorism
DAR	Dealing with assets regulation
DFAT	Department of Foreign Affairs and Trade
DNFBP	Designated non-financial businesses and professions
FIU	Financial intelligence unit
FTR	Financial transaction report
IDC	Interdepartmental Committee
IFTI	International fund transfer instructions
ILGA	Independent Liquor and Gaming Authority

## TABLE OF ACRONYMS

IMP	Information management policy
IOSCO	International Organisation of Securities Commissions
KYC	Know your customer
MACMA	Mutual Assistance in Criminal Matters Act 1987
ML	Money laundering
MLA	Mutual legal assistance
MMOU	Multilateral memoranda of understanding
NOCRP	National organised crime response plan
NPO	Non-profit organisations
NRA	National risk assessment
NTA	National threat assessment
OCTA	Organised crime threat assessment
OSAS	Online sanctions administration system
PEPs	Politically exposed persons
PSPF	Protective security policy framework
REG	Reporting entity group
REs	Reporting entities
RNP	Remittance network provider
SMR	Suspicious matter report
SUSTR	Suspect transactions
TF	Terrorist financing
TFIU	Terrorism financing investigations unit
TFS	Targeted financial sanctions
TTR	Threshold transaction report
UNSC	United Nations Security Council
UNSCR	United Nations Security Council Resolution





© FATF and APG

[www.fatf-gafi.org](http://www.fatf-gafi.org) | [www.apgml.org](http://www.apgml.org)

April 2015

## **Anti-money laundering and counter-terrorist financing measures - Australia *Fourth Round Mutual Evaluation Report***

In this report: a summary of the anti-money laundering (AML) / counter-terrorist financing (CTF) measures in place in Australia as at the date of the on-site visit (30 July - 12 August 2014). The report analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Australia's AML/CTF system, and provides recommendations on how the system could be strengthened.