



Australian Government

**Australian Transaction Reports
and Analysis Centre**

AUSTRAC Guidance Note

Risk management and AML/CTF programs



AUSTRAC Guidance Note

Risk management and AML/CTF programs

Anti-Money Laundering and Counter-Terrorism Financing Act 2006

Contents	Page
1. Introduction	3
2. Risk management framework	4
3. Main types of ML/TF risks	5
4. Components of a risk management framework	6
5. Legal requirements for risk-based systems and controls in Parts A and B of an AML/CTF program	10
6. Determining appropriate risk-based systems and controls in Parts A and B of an AML/CTF program	10
7. Requirements for Part A of an AML/CTF program	14
8. Other legal requirements for Part A of a standard or joint AML/CTF program	15
9. Requirements for Part B of an AML/CTF program	17
Further information	19

1. Introduction

- 1.1 The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) is designed to assist in combating money laundering and the financing of terrorism. To achieve these aims, the AML/CTF Act places certain obligations on 'reporting entities' (defined in section 5 of the AML/CTF Act).
- 1.2 Under section 229 of the AML/CTF Act, the Chief Executive Officer (CEO) of the Australian Transaction Reports and Analysis Centre (AUSTRAC) may, in writing, make Anti-Money Laundering/Counter-Terrorism Financing Rules (AML/CTF Rules). The AML/CTF Rules are legislative instruments and are therefore binding.
- 1.3 The AML/CTF Rules in Chapters 4, 5, 6, 7, 8 and 9 of *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*, as made under Part 7 of the AML/CTF Act, are relevant to this guidance note. These AML/CTF Rules come into effect on 12 December 2007.
- 1.4 Reporting entities should be aware of their obligations under relevant federal, state or territory legislation, including anti-discrimination laws and the *Privacy Act 1988*, in carrying out activities in order to comply with the AML/CTF Act and AML/CTF Rules. This includes the collection of 'know your customer' (KYC) information, development of risk-based systems and controls and the assessment of money laundering and terrorism financing (ML/TF) risk posed by customers who are politically exposed persons (PEPs) for the purpose of an anti-money laundering and counter-terrorism financing program (AML/CTF program).
- 1.5 The purpose of this guidance note is to:
 - (a) provide general information about risk management frameworks and relevant legislative requirements under the AML/CTF Act and AML/CTF Rules relating to AML/CTF programs
 - (b) assist reporting entities in implementing an AML/CTF program appropriate to their business having regard to the business size, nature and complexity.
- 1.6 The intent of the first section of this guidance note is to provide a broad risk management framework based on high-level principles and procedures that a reporting entity may wish to consider when developing and implementing a risk-based approach to identify, mitigate and manage ML/TF risks.
- 1.7 It should be noted that the lists of relevant factors and examples set out in this guidance note are not exhaustive. They contain some of the matters for consideration by reporting entities in the assessment of ML/TF risk relating to customers and the monitoring of their risk management procedures and controls.
- 1.8 A central purpose of the AML/CTF Act is to minimise the potential that designated services may be used for money laundering or terrorism financing purposes. Designated services are set out in tables 1, 2 and 3 in section 6 of that Act. To achieve this purpose, the AML/CTF Act regulates

certain aspects of a reporting entity's relationship with its customers and its provision of designated services by ensuring that the entity:

- (a) knows who its customers are, so it can identify and appropriately manage ML/TF risks
- (b) puts in place risk-based systems and controls designed to identify, mitigate and manage the ML/TF risk it may reasonably face in providing the services.

2. Risk management framework

- 2.1 The AML/CTF Act is principles based. The Act and the AML/CTF Rules impose some requirements for the systems and controls that must be implemented to address business risks, but do not prescribe any specific methodology for identifying and managing those business risks. Reporting entities are best placed to assess ML/TF risk(s) they may reasonably face in providing a designated service, having regard to their business (size, nature and complexity).
- 2.2 Reporting entities have the flexibility to construct and tailor their risk management framework for the purpose of developing risk-based systems and controls and mitigation strategies in the manner most appropriate to their business structure (including financial resources and staff), their products and/or the services they provide. Such risk-based systems and controls should be proportionate to the ML/TF risk(s) a reporting entity reasonably faces.
- 2.3 Many reporting entities will already have regulatory compliance policies and processes in place in relation to other legislation. If appropriate, a reporting entity may align or incorporate the new AML/CTF regulatory obligations within its existing compliance framework and procedures.
- 2.4 The risk management framework discussed in this guidance note aims to assist reporting entities to develop and implement their AML/CTF programs in compliance with Part 7 of the AML/CTF Act and Chapters 1, 4, 5, 6, 7, 8 and 9 of the AML/CTF Rules.
- 2.5 Generally, AUSTRAC expects reporting entities to develop and maintain logical, comprehensive and systematic methods to address each of the components referred to in section 4 below and that such methods and the entities' approach to ML/TF risk are understood, implemented and maintained, to an appropriate extent, within their organisations.
- 2.6 Reporting entities would be expected to demonstrate to AUSTRAC (for example, when an AUSTRAC audit is being conducted) that their risk-based systems and controls are suitable to their particular businesses (having regard to their size, nature and complexity) and are consistent with prudent and good practices.
- 2.7 Generally, if applying the model suggested by the joint Australian/New Zealand generic guide *AS/NZS 4360:2004 : Risk management (as amended when necessary)*, a risk management framework would consist of:
 - (a) establishing the internal and external context within which the designated service is, or is to be, provided (that is, the customer

types, types of services, delivery methods and any dealings with foreign jurisdictions)

- (b) identifying risks
- (c) evaluating or assessing risks
- (d) treating risks (mitigating, managing, control, monitoring and periodic reviews).

For explanations of each of these components please refer to section 4 below.

3. Main types of ML/TF risks

- 3.1 For the AML/CTF environment, AUSTRAC would expect a reporting entity's risk management framework to deal with ML/TF risks in the context of two main risk categories: regulatory risk and business risk (inherent and residual risk). In a risk-based system, the separation of regulatory and business risks is not as distinct as in a prescriptive regime. Reporting entities are advised to consider the cross-impacts.

Regulatory risk

- 3.2 Reporting entities should understand and manage regulatory risks associated with breaches of relevant provisions of the AML/CTF Act and AML/CTF Rules. This includes the implementation of a robust compliance plan that encompasses relevant obligations and defines the control and review mechanisms needed to ensure compliance. Examples of regulatory obligations include reporting suspicious matters (see Part 3, Division 2 of the AML/CTF Act) and customer identification requirements.
- 3.3 It should be noted that the suspicious matter reporting requirements (Division 2 of Part 3 in the AML/CTF Act) will come into effect on 12 December 2008. In the meantime, the current suspect transaction reporting requirements of Part II, Division 2 of the *Financial Transaction Reports Act 1988* (FTR Act) apply for entities subject to that Act.
- 3.4 AUSTRAC considers that reporting entities must make a concerted effort to know their relevant legislative obligations, understand the ML/TF risks affecting their business and know how to identify, mitigate and manage those risks (see paragraph 4.4 below).

Business risk (inherent and residual risk)

- 3.5 'Business risk' is the risk that designated services may be used to facilitate money laundering or terrorism financing. It is important to note that regulatory and business risks may overlap. Business risk may be categorised as:
 - (a) inherent risk (see paragraphs 3.6 and 3.7)
 - (b) residual risk (see paragraphs 3.8 and 3.9).
- 3.6 Reporting entities may examine the inherent ML/TF risk across their business as a whole and in particular:
 - (a) customer type risk

- (b) products or services risk (types of designated services)
- (c) delivery method risk
- (d) jurisdiction risk.

See also Chapters 8 and 9 of the AML/CTF Rules and paragraph 6.1 below.

- 3.7 Within each of the above categories, reporting entities may consider having in place a model of elements that will influence the risk or potential risk of ML/TF which must be managed. Reporting entities may consider the composite risk posed by the above categories across their businesses and identify what controls, systems and procedures should be put in place in order to identify, mitigate and manage risks.
- 3.8 It is recognised that no matter how robust a risk mitigation and management program is, each reporting entity will still have some exposure to residual ML/TF risk which must be managed.
- 3.9 In recognising the existence of residual risk, reporting entities are encouraged to undertake ongoing due diligence and regularly monitor their ML/TF risk profiles according to the nature, size and complexity of their business operations. The frequency of monitoring should be determined by the level of risk identified, the degree of urgency required for resolving issues and where applicable, the relevant requirements of the AML/CTF Act and/or AML/CTF Rules.

4. Components of a risk management framework

- 4.1 AUSTRAC envisages the following components will be included in a reporting entity's risk management framework:
 - (a) risk identification and assessment (see paragraphs 4.2 and 4.3 below)
 - (b) treatment of risk including mitigating, managing, control, monitoring and periodic reviews (see paragraphs 4.4 to 4.10 below).

Risk identification and assessment

- 4.2 In their risk management framework, reporting entities are encouraged to include a procedure for updating and reassessing risks and identifying new and significant changes to risks, which may assist business decisions regarding the mitigation and management of risks.
- 4.3 For each identified risk, the reporting entity should:
 - (a) assess the likelihood and impact of the risk
 - (b) assess the level of the risk identified
 - (c) identify risk mitigation and control procedures relevant to the level of risk identified.

Treatment of risk including mitigating, managing, control, monitoring and periodic reviews

- 4.4 The reporting entity should, as part of its risk management framework, consider how any identified residual risks should be managed and mitigated. The term 'mitigate' in this context means reducing the seriousness or extent of ML/TF risk(s). This is part of applying appropriate risk-based systems and controls to manage ML/TF risk(s). An example of a mitigation step is a reporting entity implementing adequate controls as necessary for higher risk products, such as setting transaction limits and/or a management approval escalation process. A well-reasoned, comprehensive and effective risk-based approach relevant to a reporting entity's business and circumstances should assist the entity to manage ML/TF risks it may reasonably face. For example, the development and application of risk categories may be used as one of the strategies for managing potential risks by enabling the reporting entity to subject customers to appropriate controls and oversight.
- 4.5 The reporting entity may adopt the following components (where appropriate to the nature, size and complexity of its business), among others, as part of its risk management strategy:
- (a) reviews at senior management level of the reporting entity's progress towards implementing stated ML/TF risk management objectives
 - (b) clearly defined management responsibilities and accountabilities regarding ML/TF risk management
 - (c) adequate staff resources to undertake functions associated with ML/TF risk management
 - (d) specified staff reporting lines from ML/TF risk management system level to board or senior management level, with direct access to the board member(s) or senior manager(s) responsible for overseeing the system
 - (e) procedural controls relevant to particular designated services
 - (f) documentation of all ML/TF risk management policies
 - (g) a system, whether technology based or manual, for monitoring the reporting entity's compliance with relevant controls
 - (h) policies to resolve identified non-compliance
 - (i) appropriate training program(s) for staff to develop expertise in the identification of ML/TF risk(s) across the reporting entity's designated services
 - (j) an effective information management system which should:
 - (i) produce detailed and accurate financial, operational and compliance data relevant to ML/TF risk management

- (ii) incorporate market information relevant to the global AML/CTF environment which may assist the reporting entity to make decisions regarding its risk management strategy
 - (iii) enable relevant, accurate and timely information to be available to a relevant officer (for example, the AML/CTF Compliance Officer) within the reporting entity
 - (iv) allow the reporting entity to identify, quantify, assess and monitor business activities relevant to ML/TF risk(s)
 - (v) allow the reporting entity to monitor the effectiveness of and compliance with its internal AML/CTF systems and procedures
 - (vi) allow the reporting entity to regularly assess the timeliness and relevance of information generated, together with its adequacy, quality and accuracy.
- 4.6 It should be noted that a reporting entity can adopt other strategies in addition to taking into account any of the above factors (where relevant), if it considers this approach appropriate in accordance with its risk management framework.
- 4.7 A reporting entity's ongoing monitoring of its risk management procedures and controls may also alert the entity to any potential failures including (but not limited to):
- (a) failure to include all mandatory legislative components
 - (b) failure to gain board and/or executive approval of the AML/CTF program
 - (c) insufficient or inappropriate employee due diligence
 - (d) frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s)
 - (e) changes in business functions which are not reflected in the AML/CTF program (for example, the introduction of a new product or distribution channel)
 - (f) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging ML/TF risk)
 - (g) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the AML/CTF program
 - (h) legislation incorrectly interpreted and applied in relation to a customer identification procedure
 - (i) customer identification and monitoring systems, policies and procedures that fail to:
 - (i) prompt, if appropriate, for further identification and/or verification when the ML/TF risk posed by a customer increases

- (ii) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service
 - (iii) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check
 - (iv) take appropriate action where the identification document provided is neither an original nor a certified copy
 - (v) recognise foreign identification documentation issued by a high-risk jurisdiction
 - (vi) record comprehensive details of identification documents, for example, the date of issue
 - (vii) consult appropriate resources in order to identify high-risk customers
 - (viii) identify when an expired or old identification document (for example, a driver's licence) has been used
 - (ix) collect any other name(s) by which the customer is known
 - (x) be subject to regular review
- (j) lack of access to information sources to assist in identifying higher risk customers (and the jurisdictions in which they may reside), such as PEPs, terrorists and narcotics traffickers (see paragraphs 6.6 to 6.8 below)
- (k) lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:
- (i) customer identification policies, procedures and systems
 - (ii) identifying potential ML/TF risks
- (l) acceptance of documentation that may not be readily verifiable.
- 4.8 AUSTRAC expects reporting entities to put in place appropriate systems to ensure that their risk management processes for managing ML/TF risks are subject to regular review.
- 4.9 Reporting entities are encouraged to periodically review and evaluate their risk management framework to ensure that it is adequate, appropriate and effective and to identify improvement opportunities that may arise. Such a review may include assessment of risk management resources such as funding and staff allocation and may also identify any future needs relevant to the nature, size and complexity of the reporting entity's business.
- 4.10 The review may be undertaken by independent internal or external audit staff, who should have unlimited access to the records, personnel and property of the reporting entity, within the context of the reporting entity's obligations under the *Privacy Act 1988*. Internal staff should be impartial and objective in performing their duties and should not be inappropriately influenced by management of the reporting entity.

5. Legal requirements for risk-based systems and controls in Parts A and B of an AML/CTF program

- 5.1 Part 7 of the AML/CTF Act requires a reporting entity to have a written AML/CTF program comprising Part A – general (see section 7 below) and Part B – customer identification (see section 9 below).
- 5.2 Chapters 4, 5, 6, 7, 8 and 9 of the AML/CTF Rules require reporting entities to implement appropriate risk-based systems and controls to comply with certain legal obligations.
- 5.3 Chapters 8 and 9 of the AML/CTF Rules set out the requirements a reporting entity must comply with in implementing Part A of a standard or joint AML/CTF program.
- 5.4 The purpose of Part A of a standard AML/CTF program is to identify, mitigate and manage the ML/TF risk the reporting entity may reasonably face in providing designated services. Chapter 4 of the AML/CTF Rules requires Part B of a reporting entity's standard AML/CTF program to set out its customer identification procedures, including the collection and verification of minimum KYC information about customers and agents of customers.
- 5.5 In a joint AML/CTF program, the purpose of Part A is to identify, mitigate and manage the ML/TF risk each of the reporting entities in a designated business group may reasonably face in providing designated services. Part B of the joint program must set out customer identification procedures in relation to *each* of the reporting entities in the designated business group which have chosen to adopt the joint AML/CTF program. In these cases, each of the reporting entities may have different ML/TF risks. Parts A and B of the joint AML/CTF program would therefore need to be capable of identifying, mitigating and managing ML/TF risks which may be faced by different reporting entities in the group.
- 5.6 Chapter 5 of the AML/CTF Rules sets out the requirements for a special AML/CTF program, which applies where a reporting entity provides only designated services covered by item 54 of table 1 in section 6 of the AML/CTF Act. A special AML/CTF program is a written program for the sole or primary purpose of setting out the reporting entity's applicable customer identification procedures (in the AML/CTF Rules, the requirements are the same as for Part B of an AML/CTF program).
- 5.7 Civil penalties may apply to a reporting entity for any failure to adopt or maintain an AML/CTF program (see also AUSTRAC's Enforcement Policy, available at: http://www.austrac.gov.au/enforcement_policy.html).
- 5.8 For other legal requirements, see also sections 6, 7, 8 and 9 below.

6. Determining appropriate risk-based systems and controls in Parts A and B of an AML/CTF program

- 6.1 Within the risk management framework described in sections 2, 3 and 4 above, each reporting entity must address all the factors below which relate to its particular circumstances, business operations and risk-based systems and controls. When determining risk-based systems and controls in Parts A and B of a standard or joint AML/CTF program, or in a special AML/CTF program, the reporting entity must consider:

- (a) the nature, size and complexity of its business
- (b) the type(s) of ML/TF risk(s) it may reasonably face, taking into account the following in assessing such risk(s):
 - (i) customer types such as companies, trusts, partnerships and any PEPs (see paragraph 6.6 below)
 - (ii) types of designated services provided (for example, a reporting entity may assess that the potential risk related to the provision of a deposit account is different from that related to the provision of an international funds transfer service to a person who does not hold an account with the reporting entity, or who is from a high-risk foreign jurisdiction)
 - (iii) delivery methods of designated services provided
 - (iv) any foreign jurisdictions with which the reporting entity deals.

6.2 A reporting entity may, in considering what systems and procedures to put in place, use the following techniques:

- (a) a risk assessment which matches the designated service it provides against potential risk vulnerabilities, in order to ascertain the strengths and weaknesses of its ML/TF risk environment
- (b) mapping the ML/TF risk associated with designated services across business units, organisational functions, processes and interdependencies, which can reveal areas of control weakness and help inform subsequent action by the reporting entity
- (c) indicators such as relevant statistics which may provide information on the reporting entity's risk position (an example of a relevant statistic is one which relates to the number of customers whose identities were not adequately identified and/or verified).

6.3 A risk-based approach may assist a reporting entity to:

- (a) recognise that ML/TF risks may vary across customers, products, delivery methods and/or jurisdictions
- (b) focus its efforts on high-risk areas in its business.

Customer types and relationships

6.4 Customer types should be considered against the relevant ML/TF risk identified by a reporting entity regarding its provision of designated service(s).

6.5 In assessing the ML/TF risk relating to customers, the reporting entity may consider, where appropriate and among other factors, whether:

- (a) the customer is involved in a complex business ownership structure with no legitimate commercial rationale
- (b) the non-individual customer (for example, a trust, company or partnership) has a complex business structure with little commercial

justification, which obscures the identity of ultimate beneficiaries of the customer

- (c) the customer is in a position which may expose them to the possibility of corruption
- (d) the customer is based in, or conducting business through or in, a high-risk jurisdiction
- (e) the customer is engaged in business which involves significant amounts of cash
- (f) there is no clear commercial rationale for the customer seeking the designated service
- (g) the customer is a PEP (see paragraphs 6.6 to 6.8 below)
- (h) an undue level of secrecy is requested regarding a designated service
- (i) the source of funds is difficult to verify
- (j) the beneficial owners of a non-individual customer are difficult to identify and/or verify
- (k) the beneficial owners of the non-individual customer are resident in a high-risk jurisdiction
- (l) there is a one-off transaction in comparison with an ongoing business relationship or series of transactions
- (m) a designated service can be used for money laundering or terrorism financing (and the extent to which it can be used)
- (n) the customer makes or accepts payments (for example, electronic transfers) to or from accounts which have not been identified by the reporting entity
- (o) the customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts
- (p) the customer makes withdrawal, transfer or drawdown instructions by phone or fax
- (q) the customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer)
- (r) the customer when migrating from one designated service to another carries a different type and level of ML/TF risk
- (s) the customer has income which is not employment-based or from a regular known source
- (t) the customer is new rather than having a long-term and active business relationship with the reporting entity

- (u) the customer's business or provision of designated services is primarily of a money remittance service nature
- (v) the customer's business is registered in a foreign jurisdiction with no local operations
- (w) the customer's business is an unregistered charity, foundation or cultural association
- (x) the designated services provided to the customer are primarily of a private banking and/or wealth management kind
- (y) the customer is represented by another person, such as under a power of attorney.

6.6 As part of customer risk assessment, a reporting entity must put appropriate risk-based systems and controls in place to identify customers who may be PEPs and to determine whether specific customers should be subject to additional checks to identify whether they are a PEP. The Financial Action Task Force (FATF) defines PEPs as:

individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. (FATF, *Glossary to the 40 Recommendations*.)

- 6.7 A variety of domestic and international resources are available to reporting entities to assist in determining the ML/TF risk of their customers, foreign jurisdictions, products and services and methods of designated service delivery. For examples, see the Department of Foreign Affairs and Trade 'Consolidated List' which is available at http://www.dfat.gov.au/icat/freezing_terrorist_assets.html.
- 6.8 AUSTRAC considers that only foreign PEPs will need to be identified, as appropriate, in accordance with the FATF definition and the reporting entity's customer identification procedures and/or ongoing customer due diligence procedures. There is no obligation on reporting entities to identify domestic PEPs on an ongoing basis unless warranted by the ML/TF risk(s) which a reporting entity reasonably faces.
- 6.9 Reporting entities should consider all the risks of a customer relationship, taking into account relevant factors outlined in 6.5 above. Where a reporting entity assesses that its relationship with an individual customer is of medium or lower ML/TF risk, the reporting entity may apply the 'safe harbour' procedures set out in Chapter 4 of the AML/CTF Rules which, if applied, should be included in Part B of its AML/CTF program. However, these safe harbour procedures do not preclude the reporting entity from meeting the requirements of Chapter 4 of the AML/CTF Rules in another way in these circumstances.

Delivery methods

- 6.10 The different methods by which designated services are delivered may have different ML/TF risks. A reporting entity may assess that the potential risk related to face-to-face transactions is different from that related to the provision of services through remote access such as internet banking.

Foreign jurisdictions

- 6.11 A reporting entity will need to consider the risks posed by differences in the legal frameworks and standard AML/CTF controls of foreign jurisdictions with which it deals and factor these into its AML/CTF program. Where relevant, a reporting entity should take into account information from legitimate, respected domestic and/or international bodies.
- 6.12 A reporting entity must also put appropriate systems and controls in place to identify, mitigate and manage any ML/TF risks that it might face regarding its permanent establishment(s) overseas (as defined in section 21 of the AML/CTF Act). This includes customers of the permanent establishment(s), in accordance with Chapter 8 (for standard AML/CTF programs) or Chapter 9 (for joint AML/CTF programs). See paragraph 8.7 below.

7. Requirements for Part A of an AML/CTF program

- 7.1 For Part A of a standard AML/CTF program, Chapters 8 and 9 of the AML/CTF Rules require a reporting entity to implement risk-based systems and controls to:
- (a) identify, mitigate and manage ML/TF risk(s) it may reasonably face
 - (b) enable the identification of significant changes in ML/TF risk(s):
 - (i) in relation to the reporting entity's provision of a designated service for the purposes of Part A of the AML/CTF program
 - (ii) posed by customers for the purposes of Part B of the AML/CTF program
 - (c) recognise such ML/TF risk changes for the requirements of Parts A and B of its AML/CTF program
 - (d) assess the ML/TF risk(s) posed by:
 - (i) all new designated services prior to introducing them to the market
 - (ii) all new methods of designated service delivery prior to adopting them (for example, using a non-face-to-face method or the use of electronic funds transfers)
 - (iii) all new or developing technologies used for the provision of a designated service prior to adopting them

- (e) determine the appropriate level of employee due diligence to apply to its employees, agents and consultants who carry out functions connected with the designated services provided by the entity and who are in a position to facilitate an ML/TF offence (*AS4811:2006 – Australian Standard – Employment Screening*, published in July 2006 and the related *Employment Screening Handbook and Reference Checking Handbook - Financial Services Industry*, currently being developed by Standards Australia in consultation with the Australian Securities and Investments Commission and industry representatives, may be of assistance to reporting entities)
 - (f) design, having regard to ML/TF risk(s) it reasonably faces, appropriate ML/TF risk awareness training programs (applying to its employees, agents and consultants) and determine the frequency and extent of such training.
- 7.2 The minimum requirements in the AML/CTF Rules relating to AML/CTF programs are technology neutral. The reporting entity may determine whether, or the extent to which, it relies upon automated or technological solutions.
- 7.3 An example of the practical operation of subparagraphs 7.1(b) and (c) above is where a reporting entity identifies a new or changed level of ML/TF risk posed by a new or existing service type and makes necessary adjustments to its AML/CTF program to address this finding. Such changes may include collecting and/or verifying additional KYC information about customers seeking this type of service.
- 7.4 A reporting entity's existing risk management policies and processes should be regularly evaluated to ensure they are sufficiently robust and adequate to cover potential new ML/TF risks posed by current or planned designated services.

8. Other legal requirements for Part A of a standard or joint AML/CTF program

- 8.1 A reporting entity must also include in Part A of its standard or joint AML/CTF program appropriate procedures relating to:
- (a) oversight by boards and senior management
 - (b) a designated AML/CTF Compliance Officer
 - (c) regular independent reviews
 - (d) dealing with AUSTRAC feedback
 - (e) permanent establishments in a foreign country.

Oversight by boards and senior management (parts 8.4 and 9.4 of Chapters 8 and 9 of the AML/CTF Rules)

- 8.2 Part A of a reporting entity's AML/CTF program must be approved and subject to ongoing oversight by its governing board and senior management. If a reporting entity does not have a board, then approval and oversight must be by the CEO or equivalent. Oversight may include regular reports that are dealt with as part of operational risk reporting

processes (both status and incident reports). In the case of a joint AML/CTF program, approval and oversight of Part A may be undertaken by the board and senior management of the main holding company of a designated business group, where the members of that designated business group are related to each other (within the meaning of section 50 of the *Corporations Act 2001*).

Designated AML/CTF Compliance Officer (parts 8.5 and 9.5 of Chapters 8 and 9 of the AML/CTF Rules)

- 8.3 An 'AML/CTF Compliance Officer' must be designated by the reporting entity or designated business group (where applicable) at the management level, but this officer may have other duties. This does not preclude reporting entities from appointing additional resources to AML/CTF compliance activities (for example, additional compliance staff for separate office or branch locations). The following factors may be relevant when considering the designation of the AML/CTF compliance officer: independence, seniority, accountability, reporting lines, access to executive/board and relevant skills and experience.

Regular independent reviews (parts 8.6 and 9.6 of Chapters 8 and 9 of the AML/CTF Rules)

- 8.4 An independent review of Part A of an AML/CTF program must be carried out on a regular basis by an internal or external party determined by the reporting entity (for example, an internal or external auditor). The results of the review must be provided to the governing board or senior management of the reporting entity, which in relation to a designated business group means the board/management of each reporting entity in the group. The purpose of the review should be to assess:
- (a) the effectiveness of Part A (including the adequacy and performance of ML/TF risk management systems and controls), considering the ML/TF risk(s) of the reporting entity, or of each reporting entity in a designated business group
 - (b) whether Part A complies with the relevant AML/CTF Rules and has been effectively implemented
 - (c) whether the reporting entity, or each reporting entity in a designated business group, has complied with Part A.

AUSTRAC feedback (parts 8.7 and 9.7 of Chapters 8 and 9 of the AML/CTF Rules)

- 8.5 Part A must include appropriate procedures for the reporting entity, or each reporting entity in a designated business group, to have regard to AUSTRAC feedback on the reporting entity's ML/TF risk management performance. This may include requirements and recommendations contained in AUSTRAC audit reports.
- 8.6 AUSTRAC issues information circulars that provide information to reporting entities about domestic and international issues that may affect their business. These include lists of financial sanctions against certain jurisdictions and updates to lists of known terrorist groups. Current information circulars are available on AUSTRAC's website at http://www.austrac.gov.au/information_circular.html.

Permanent establishments in a foreign country (parts 8.8 and 9.8 of Chapters 8 and 9 of the AML/CTF Rules)

- 8.7 Part A of a standard AML/CTF program affects a reporting entity's permanent establishments (defined in section 21 of the AML/CTF Act) in foreign countries (including where the reporting entity is a member of a designated business group), as follows:
- (a) requirements relating to oversight by boards and senior management, designation of an AML/CTF Compliance Officer, independent reviews and consideration of AUSTRAC feedback, *do* apply
 - (b) requirements relating to the implementation of appropriate risk-based systems or controls, AML/CTF risk awareness training program and employee due diligence program, *do not* apply
 - (c) where a reporting entity provides a designated service at a permanent establishment in a foreign jurisdiction which is regulated by AML/CTF laws that are comparable to Australia, the reporting entity need only consider minimal additional systems and controls.

9. Requirements for Part B of an AML/CTF program

- 9.1 Chapter 4 of the AML/CTF Rules requires a reporting entity to implement appropriate risk-based systems and controls in Part B of its standard or joint AML/CTF program to address the following.
- (a) Enable the entity to be reasonably satisfied that:
 - (i) an individual customer is who he or she claims to be
 - (ii) in the case of a non-individual customer, the customer exists and in certain cases, the relevant details about beneficial owners (for example, certain companies, partnerships and trusts) as prescribed in Chapter 4 of the AML/CTF Rules have been collected.
 - (b) Establish whether and to what extent any additional KYC information should be collected and/or verified, depending on the risk level the reporting entity has assessed in providing the designated service to that customer. For example, if the reporting entity's appropriate risk-based systems and controls indicate that the customer represents a high ML/TF risk, the reporting entity may obtain other KYC information which may include any other name(s) the customer is known by and the customer's source(s) and origin of funds.
 - (c) Enable the reporting entity to determine what kind of electronic data is reliable and independent for verification purposes. Some electronic data may not have been verified from a reliable and independent source or may not yet have been verified. Such data sources should not be used by a reporting entity for verifying the identity of a customer.
 - (d) Determine whether and to what extent the identity details relating to a customer's agent should be verified.

- (e) Respond to any discrepancies which may arise when verifying information about a customer (individual or non-individual), for example:
 - (i) where the name on a customer's passport does not match the name provided to the reporting entity by the customer
 - (ii) where the name of a director of a company provided by that company (the reporting entity's customer) does not match any current director's name appearing on the historical company extract.
- 9.2 Such procedures should enable the reporting entity to be reasonably satisfied as to the identity of the customer (and beneficial owners where applicable for non-individual customers).
- 9.3 There is flexibility in Chapter 4 of the AML/CTF Rules for reporting entities to develop and apply their own procedures, based on appropriate risk-based systems and controls, which are suitable to the circumstances of special cases. Examples of special cases and appropriate documentation include (but are not limited to):
 - (a) situations where a customer cannot provide, or has difficulty providing, KYC information required by the AML/CTF Rules
 - (b) for children (under the age of 18 years), a reporting entity may rely on a notice issued by a school principal within the preceding three months that contains the name and residential address of the child and records the period of time that the child attended the school (see paragraph (4) in the definition of 'secondary identification document' in Chapter 1 of the AML/CTF Rules), in addition to an original or certified copy of a primary non-photographic identification document such as a birth certificate
 - (c) persons who have recently arrived in Australia
 - (d) non-residents of Australia
 - (e) Indigenous persons or Torres Strait Islanders resident in an isolated area
 - (f) homeless persons
 - (g) social security beneficiaries.
- 9.4 A reporting entity may rely on a health care card issued by Centrelink as a 'primary non-photographic identification document' referred to in Chapter 1 of the AML/CTF Rules.

Further information

AUSTRAC officers are able to assist reporting entities, their staff and the public in providing general information relating to the AML/CTF Act. Enquiries can be directed to the AUSTRAC Help Desk via:

- email to help_desk@austrac.gov.au
- telephone 02 9950 0827 or 1300 021 037 (a local call within Australia).

The information contained in this document is intended only to provide a summary and general overview on these matters. It is not intended to be comprehensive. It does not constitute, nor should it be treated as, legal advice or opinions. This document may contain statements of policy which reflect AUSTRAC's administration of the legislation in carrying out its statutory functions. The Commonwealth accepts no liability for any loss suffered as a result of reliance on this publication. AUSTRAC recommends that independent professional advice be sought.

The information contained herein is current as at the date of this document.

Reporting entities should note that in relation to activities they undertake to comply with the AML/CTF Act, they will have obligations under the *Privacy Act 1988*, including the requirement to comply with the National Privacy Principles, even if they would otherwise be exempt from the Privacy Act. For further information about these obligations, please go to <http://www.privacy.gov.au> or call 1300 363 992.

September 2007

© Commonwealth of Australia

Australian Transaction Reports and Analysis Centre (AUSTRAC)
PO Box 5516
West Chatswood, NSW 1515

Telephone: 1300 021 037
Facsimile: 02 9950 0071
Website: www.austrac.gov.au
Email: help_desk@austrac.gov.au