Australian Government
AUSTRAC

INSIGHTS FROM COMPLIANCE ASSESSMENTS >>>

GOOD BUSINESS PRACTICES AND AREAS FOR IMPROVEMENT

CONTENTS

BACKGROUND

Australian business at the frontline

Reporting entities are at the frontline of Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime. They can prevent, detect and disrupt the flow of illicit funds from serious and organised crime and terrorism financing.

That is why AUSTRAC works with reporting entities to help them understand and mitigate the risk of their business being exploited by criminals.

Our regulatory and enforcement approach seeks to maximise the ability of businesses to:

- identify, mitigate and manage their risk of being misused for money laundering and terrorism financing (ML/TF)
- build capability to resist criminal abuse
- identify and report financial and other information – because transaction reports and data from our reporting entities are the source of Australia's financial intelligence
- actively contribute to protecting the integrity of the financial system.

As part of this approach, we are publishing compliance feedback. This provides reporting entities with further information on areas where businesses are performing well and areas for improvement.

Purpose of this report

This report draws on:

- observations made by AUSTRAC during recent assessments of reporting entities' compliance with their AML/CTF obligations
- breach notifications received from reporting entities.

The feedback offers suggestions for all reporting entities to:

- strengthen their AML/CTF systems and controls
- better mitigate and manage the risks they face
- improve their compliance with relevant legislation.

Insights from compliance assessments

AUSTRAC has identified four key areas where reporting entities can improve their AML/CTF outcomes:

1. ML/TF risk assessments
2. applying the risk-based approach to AML/CTF
3. outsourced and automated processes
4. governance issues.

It is crucial that all reporting entities maintain rigorous AML/CTF systems and controls. Reporting entities are invited to consider the issues raised in this report and ensure their AML/CTF program is up-to-date and protecting them from exploitation.

ML/TF RISK ASSESSMENTS

Compliant ML/TF risk assessments

The ML/TF risk assessment is the cornerstone of a compliant AML/CTF program. Understanding the ML/TF risks it may face is a necessary first step for a reporting entity in developing, implementing and maintaining procedures that mitigate and manage those risks.

Reporting entities with appropriate ML/TF risk assessments demonstrated that they understood:

- how their products and services could be misused by criminals to launder money or fund terrorism
- how likely it is that each product or service could be misused.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) requires that risk assessments have regard to the risks posed by:

- the designated services the reporting entity provides
- the types of customers to whom it provides services
- how it provides its services
- the foreign jurisdictions with which it deals.

It is essential that reporting entities undertake an ML/TF risk assessment before introducing any new products, services or delivery channels. This will allow reporting entities to implement compliant AML/CTF processes before providing the product or service to customers.

Reporting entities must also have systems in place to monitor changes in their ML/TF risk over time, and update their policies and procedures accordingly. This is because customers, products, delivery channels and technologies change over time.

Areas for improvements

Generic risk assessments

Many reporting entities engage AML/CTF service providers to help them complete their risk assessments. In some cases, this has resulted in entities adopting what appear to be 'off-the-shelf' risk assessments that are generic and could apply equally to any entity in the industry sector; that is, the risk assessment is not specific to the reporting entity.
A generic risk assessment is not tailored to protect that specific business.

AUSTRAC does not want to discourage reporting entities from seeking assistance from external AML/CTF service providers; however, it is important that external service providers assist the reporting entity to understand the risks it faces, rather than simply develop AML/CTF documentation.

Changes in risk

The ML/TF risk profile of a business changes over time. This can be due to a number of internal and external factors. Common changes include the introduction of new products and services, new delivery channels for existing products and services, or a changing customer base.

AUSTRAC compliance officers assessments have found that many reporting entities only considered the risks posed by their business at a single point in time, typically when they first developed their AML/CTF program.

However, many did not have systems in place that prompted them to update their risk assessments when aspects of their business changed, or when patterns emerged of the misuse of designated services by criminals.

The assessment of risk needs to be ongoing, particularly as customers, products, delivery channels and technologies change over time. Reporting entities need to have systems in place to ensure their risk assessments and methodologies evolve as required. In particular, reporting entities must ensure they review patterns of suspected criminal activity emerging from their ongoing customer due diligence, and the suspicious matter reports they lodge with AUSTRAC, and update their risk assessment accordingly.

For more information about your obligations relating to ML/TF risk assessments, see **Conducting an ML/TF risk assessment** in the *AUSTRAC compliance guide*.

Please also see Chapter 4 and paragraphs 8.1.4 and 8.1.5 of the AML/CTF Rules or Chapter 5, and paragraphs 9.1.4 and 9.1.5 for 'designated business groups' (DBGs).

Terrorism financing risk

Some reporting entities' risk assessments focused almost exclusively on money laundering risks and failed to consider terrorism financing.

While money laundering and terrorism financing can have similar methodologies, it is important that reporting entities consider the different objectives or motivations behind money laundering and terrorism financing. These differences can result in very different indicators of suspicious activity. Knowing the different indicators is important for reporting entities to monitor customer behaviour and detect and report suspicious behaviour to AUSTRAC.

APPLYING THE RISK-BASED APPROACH TO AML/CTF PROGRAMS

Building a compliant risk-based AML/CTF program

AML/CTF regulation in Australia is risk-based. This means our regulations have been developed in a way that gives a reporting entity flexibility to decide how to fulfil many of its AML/CTF obligations.

Reporting entities are expected to do this based on the nature, size and complexity of their business and the types of ML/TF risk they might reasonably face.

This enables each reporting entity to tailor its AML/CTF program to meet the specific ML/TF risks it faces in its day-to-day operations.

In practical terms, an AML/CTF program is a written document that explains how the reporting entity has set up and is running its AML/CTF framework.

The importance of a risk assessment is discussed previously. This aligns with AUSTRAC's observations that compliant risk-based AML/CTF programs are developed and informed by an appropriate ML/TF risk assessment.

Reporting entities must do the things they document in their AML/CTF programs. AUSTRAC has observed that compliant AML/CTF programs:

- contain policies, processes and procedures that are practical and fit-for-purpose in addition to being tailored to the specific ML/TF risks the reporting entity faces
- use clear language that allows reporting entity staff to know what they need to do and when.

For more information about the risk-based approach, please see **Background to AML/CTF programs** in the *AUSTRAC compliance guide*.

Please also see Part 8.1 of the AML/CTF Rules or Part 9.1 for designated business groups (DBGs)

Areas for improvements

Documenting systems and controls

Some of the AML/CTF programs reviewed by AUSTRAC included large sections that were copied from the AML/CTF Rules or the AUSTRAC compliance guide. Those AML/CTF programs did not set out the actual systems and controls that a reporting entity had in place. For example, AUSTRAC has seen transaction monitoring programs with wording like:

> [Reporting entity] has a transaction monitoring program which includes risk-based systems and controls to monitor the transactions of customers. [Reporting entity's] transaction monitoring program has the purpose of identifying suspicious transactions, by having regard to complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or visible lawful purpose.

In this instance, the transaction monitoring program has paraphrased Parts 15.4 to 15.7 of the AML/CTF Rules. It does not outline any systems and controls the reporting entity plans to use to monitor transactions.

A reporting entity stating that it has the systems and controls required by the AML/CTF Rules is not fulfilling its obligation to document those systems and controls in its AML/CTF program. It also fails to demonstrate the reporting entity has actually thought about its AML/CTF obligations, the specific ML/TF risks it faces or the systems it will use to identify, mitigate and manage those risks. This is what AUSTRAC officers look for in assessing compliance with the AML/CTF Act and Rules.

Template programs

AUSTRAC has also observed that many AML/CTF programs are templates obtained from external AML/CTF service providers that have not been tailored to suit the reporting entity's business.

Templates can be useful to get people thinking about their business and to make sure they have considered everything necessary. However, it is vital that the systems, controls and procedures that make up an AML/CTF program are written to directly accommodate the nature, size and complexity of each reporting entity's business.

Therefore, if a template is used as a basis for an AML/CTF program, AUSTRAC expects that it is customised for the reporting entity so that it addresses the specific ML/TF risks faced by the reporting entity.

Use of non-specific language

AUSTRAC has observed the use of vague or non-committal language in AML/CTF programs. For example, AUSTRAC has observed wording similar to the following:

> Our transaction monitoring program consists of reviewing customers' transactions. Unusual transactions will be escalated to the compliance officer who will consider lodging a suspicious matter report (SMR), where appropriate.

In this example, it is not clear:

- how transactions will be monitored, including how frequently
- how transactions will be assessed against indicators of suspicious activity
- what type of transactions will be considered suspicious and therefore reported to AUSTRAC as an SMR.

This weakens the program significantly. Clear, straightforward language helps employees of the reporting entity to understand:

- what they need to do
- circumstances that trigger additional action
- the nature of risk in the business, such as the types of transactions that the reporting has identified as posing ML/TF risks.

OUTSOURCED AND AUTOMATED PROCESSES

Effective outsourcing and automation

Reporting entities are responsible for the proper functioning of an AML/CTF program even when AML/CTF activities have been outsourced and/or automated.

AUSTRAC has observed that some reporting entities engaged others to undertake aspects of their AML/CTF program on their behalf. In cases where this was done effectively, the reporting entity had considered the impact this would have on its ability to meet its AML/CTF obligations. This included:

- ensuring that the roles and responsibilities of the reporting entity and its service providers, including the AML/CTF activities each party would undertake, were clearly documented in a contract
- proactive monitoring and testing of AML/CTF systems and processes provided by others through those contracts.

Where automated systems are used to undertake AML/CTF process, AUSTRAC recommends that reporting entities place importance on regularly monitoring those systems to ensure they are functioning as intended and mitigate the risk of non-compliance.

Reporting entities should ask themselves these types of questions when assessing their automated functions:

- in the case of transaction monitoring programs, have all business rules been configured correctly? For example, will the rules trigger enhanced customer due diligence processes or further investigation if unusual or suspicious transactions occur? Are the rules and triggers up-to-date with the changing ML/TF environment?
- have we considered the impact of IT changes, such as systems upgrades or new automated processes, on automated AML/CTF functions?
- where an automated function is designed to produce reports or alerts, are they being communicated effectively and promptly to someone who is adequately trained and authorised to deal with them appropriately, such as the AML/CTF compliance officer? Is the AML/CTF compliance officer appropriately resourced to consider automated alerts in a timely and thorough manner?
- are automated reports to AUSTRAC (such as threshold transaction reports and international funds transfer instruction reports) reconciled against the source transactional data?

Areas for improvement

Insufficient oversight of outsourced functions

AUSTRAC has observed that some reporting entities assume that the processes they, or their service providers, have implemented are working correctly and are compliant. Often, discovery of non-compliance occurs after a substantial breach or adverse assessment from AUSTRAC.

Where the reporting entity has outsourced procedures, systems and controls, they remain responsible for complying with the law. This is the case regardless of whether the service provider is a reporting entity in its own right.

A service provider's failure to follow compliant procedures places the reporting entity in breach and, at times, at risk of incurring financial penalty and reputational damage. Most importantly, it also increases the risk that ML/TF events will occur undetected.

For more information about the use of outsourced service providers (agents), see section 37 of the AML/CTF Act and Chapter 7 of the AML/CTF Rules.

Please also see *Public Legal Interpretation No. 10: Agency and the AML/CTF Act*.

Insufficient oversight of automated functions

AUSTRAC's interactions with reporting entities have indicated that some entities assume their automated processes are functioning in a compliant manner – however, this is not always the case.

Many reporting entities rely on automated systems to fulfil some of their AML/CTF obligations. Common examples include:

- transaction reporting systems
- automated transaction monitoring programs, which assess customer transactions and use predetermined business rules to detect and flag potentially suspicious transactions.

However, AUSTRAC has observed that that these automated systems do not always function as expected. Systems upgrades have been a common cause for automated processes to stop working as expected.

AUSTRAC expects reporting entities to understand how changes or upgrades to their IT systems will impact compliance with their AML/CTF programs. Reporting entities need to regularly test the systems to ensure they continue to function as expected and remain compliant. This should be the case even when IT changes do not relate directly to AML/CTF projects. For example, automated reports to AUSTRAC should be reconciled against the source transactional data at appropriate intervals.

GOVERNANCE ISSUES

Independent review

AUSTRAC has observed instances where the entity conducting an independent review of a reporting entity's AML/CTF program was closely associated with, or the same as, the entity that drafted the reporting entity's program.

For example, a reporting entity may have engaged the same consultancy firm to design, and then later review, its AML/CTF program. While this does not necessarily mean the review is not independent, reporting entities must satisfy themselves that the reviewer

- is truly undertaking an independent review of the AML/CTF program
- does not have a vested interest in the outcome of the review.

Additionally, many of the independent review reports that AUSTRAC has examined did not cover all the matters required by Part 8.6 the AML/CTF Rules. Of concern is that some reporting entities had not independently identified this omission.

The independent review should assess:

- the effectiveness of Part A of the program in addressing the ML/TF risk of the reporting entity or each reporting entity in a designated business group
- whether Part A complies with the requirements outlined in the AML/CTF Rules
- whether Part A has been effectively implemented
- whether the reporting entity has complied with Part A of its program.

For more information on independent reviews, see **Regular independent review of Part A** in the *AUSTRAC compliance guide.*

AML/CTF program oversight

Part A of an AML/CTF program must be subject to ongoing oversight by a reporting entity's Board of Directors or equivalent.

It is good practice for a reporting entity to document procedures to ensure Board oversight of Part A of their AML/CTF program.

AUSTRAC has observed that where AML/CTF programs did not include procedures to ensure Board oversight, further investigation often found that the Board had not overseen the functioning of the reporting entity's AML/CTF program as required.

For more information on board oversight, see **Approval and oversight by boards and senior management** in the *AUSTRAC compliance guide.*

RESOURCES

Updating enrolment details

Many reporting entities failed to include in their AML/CTF programs, their obligation to update their enrolment details within 14 days of any change occurring.

It is a legal obligation to maintain current and correct AUSTRAC enrolment details, including earnings and contact details.

AUSTRAC uses enrolment information to calculate levy amounts for the AUSTRAC industry contribution. Reporting entities whose enrolment details are not up-to-date risk being incorrectly invoiced.

For more information on updating your enrolment details, see **Chapter 4** of the *AUSTRAC compliance guide*.

The *AUSTRAC compliance guide* is available on our website and provides more information about general AML/CTF compliance obligations.

The case studies hub is a valuable resource that reveals the diversity and seriousness of organised crime and terrorism financing threats facing industry and the wider community. The case studies help reporting entities to understand the methodologies criminals may use to exploit products and services for criminal gain.

Case studies can be searched by:

- keyword
- industry
- offence type
- jurisdiction
- channel.

For more information about the legislation AUSTRAC administers, refer to the AML/CTF Act and the AML/CTF Rules.

Reporting entities can direct enquiries to AUSTRAC's Contact Centre:

- by phone: 1300 021 037
- email: **contact@austrac.gov.au**.

The Contact Centre is available from Monday to Friday, 8.30am to 5.00pm (Australian Eastern Standard Time).

Suggested topics

If you have any suggestions for future feedback products, please contact AUSTRAC's Contact Centre.

www.austrac.gov.au

DECEMBER 2016