MANAGING COMPLIANCE TO PREVENT ANOTHER 2019

Anti-Money Laundering / Counter-Terrorism Financingn (AML/CTF)

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

In 2019, the reputation of the financial services sector was hit by critical findings from both the Royal Commissions into Misconduct in the Banking, Superannuation and Financial Services Industry and the Parliamentary Joint Committee on Corporations and Financial Services – Fairness in Franchising.

In addition, three of the big four banks were involved in significant Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) breaches:

- **Westpac (2019)** – Formally accused by AUSTRAC of more than 23 million breaches of anti-money laundering and counter-terrorism finance laws involving $11bn in transactions, including a number potentially linked to child exploitation. As a result of this, CEO Brian Hartzer resigned and chairman Lindsay Maxsted brought forward his retirement. The potential maximum fine is calculated to be $391 trillion based on the lower end of the maximum civil penalty.
- **NAB (2019)** - Faces a significant financial penalty from AUSTRAC after self-reporting a large number of breaches of anti-money laundering and counter-terrorism laws and says there may be more to come with no certainty as to whether it will face a lawsuit over the matter.
- **CBA (2018)** – Fined $700m by AUSTRAC for the late filing of 53,506 transaction reports, not properly monitor transactions on 778,370 accounts, filing 149 suspicious matter reports late or not at all, not performing checks on 80 suspicious customers and failing to properly assess risks relating to its Intelligent Deposit Machines on 14 occasions.

> With the potential of major reputational damage and a significant decrease in investor value, the importance of managing AML risk has never been higher.

Boards and management are required to react quickly to technological changes, criminal behaviours and emerging trends which add further complexities to organisations compliance efforts. These include:

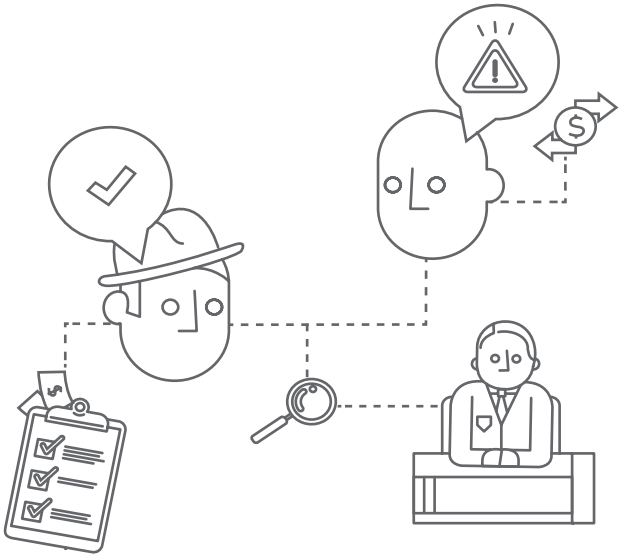
Enforcement Strategies

- Led by ASIC, Australian regulators are adopting a 'why not litigate?' strategy which has significantly increased and accelerated court-based enforcement matters;
- Compared to prior years, AUSTRAC, ASIC and APRA have been acknowledged to be applying a more aggressive stance on compliance;
- A noticeable increase in non-compliance with AML reporting obligations; and
- AUSTRAC's campaign targeting illegal money transfer dealers and a product developed for pubs and clubs to help combat money laundering.

Legislative Amendments

The Global Financial Action Task Force is currently reviewing Australia's AML framework with Parliament considering a new Bill to amend Australian AML legislation. The Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 proposes the following:

- Expand the circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by a third party;
- Explicitly prohibit reporting entities from providing a designated service if customer identification procedures cannot be performed;
- Prohibit financial institutions from entering into a correspondent banking relationship that permits its accounts to be used by a shell bank; require banks to conduct due diligence assessments before entering, and during, all correspondent banking relationships;
- Expand exceptions to the prohibition on tipping off to permit reporting entities to share suspicious matter reports and related information with external auditors and foreign members of corporate and designated business groups; and
- Provides a simplified framework for the use of financial intelligence to fight money laundering and terrorism financing.



With the ever-changing landscape of threats that organisations continue to face, risk management services remain a priority for both board members and shareholders.

What To Do
Combined with adopting the amendments to the AML Act, regulated entities must continually assess their legal, regulatory and reputational risk arising from money laundering and terrorist financing, and then create a system to appropriately mitigate them.

Organisations providing 'Designated Services' under the AML/CTF Act 2006 should re-visit their AML/CTF compliance programs considering both the design and operation.

Given recent events, these reviews should focus on the critical assessment of transaction monitoring system effectiveness, specifically the identification and reporting of suspicious transactions. In addition, organisations should consider the following.

Compliance Culture

A consistent tone at the top should reinforce that AML compliance is critical and that the risk associated with it is as serious as those in existence elsewhere in the business. Technical knowledge of AML rules and regulations may not be required by those in leadership, instead, it may be considered appropriate to empower individuals with an overview of their obligations and the ability to raise a question if ever unsure. To assist in building this:

- Review the compliance culture using a behaviour-based methodology which values risk and is structured in a way which provides valuable insights as opposed to ticking-a-box;
- Consider the sufficiency of AML compliance resources and the level of education and training being provided. In all the recent scandals, the fines for non-compliance were far in excess of the compliance costs;
- Boards and management to carefully consider how remuneration and incentive schemes drive AML compliance behaviours;
- Validate that the information generated to assist in compliance is complete, accurate and being used for the appropriate purpose by the right people; and
- Ensure roles, responsibility and compliance accountability is clearly communicated and comprehended.

Risk Assessment Updates

Within an AML/CTF risk assessment, an organisation would identify risks, develop mitigation policies and procedures, and assess the likelihood and severity of facilitating or assisting in money laundering or terrorism financing.

As a key control to ensure completeness of the AML framework, these assessments should be reviewed consistently and regularly, including assessing the impact of the any changes to the AML landscape and legislation.

To ensure this occurs, it is recommended for the review to be included as an agenda item for the Board or at the very least the Risk Committee.

AML Technological Alignment

AML software should form part of an organisations effort to combat financial crime, specifically to detect, identify, and report money laundering activities. This would usually form part of a wider AML compliance program, implemented as part of a risk-based approach to a financial institution's unique profile.

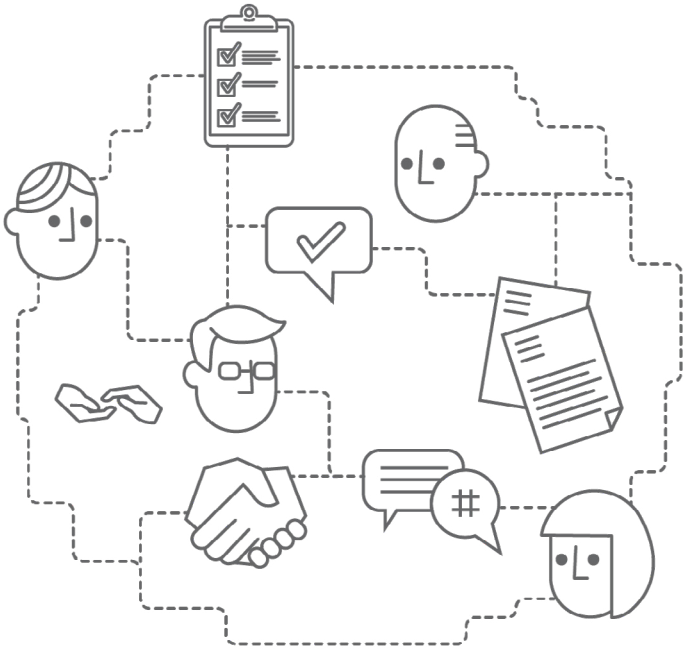
Implementing and adapting this and other technology solutions has become essential for managing AML risk with the need for continual adaptation to ensure they are kept current when the changes occur in the business and methods undertaken by criminals to exploit control weakness.

To assist in the effective integration between IT systems and communication to risk owners, organisations, and their AML Officers, organisations could consider the following:

- Review the selected AML compliance software program carefully, considering how it has been, or will be, implemented and the level of ongoing support available from the vendor. As the person responsible for the AML compliance program, the AML Officer may be held personally liable for any breaches of the law, and potentially face criminal consequences;
- Determine the extent of the organisations needs and consider whether the AML software platform is suitable. Vendors should collaborate with AML officers to assist in this, identifying specific requirements and ensuring that the chosen platform addresses them. With legislation change, and as software capabilities improve, organisation need to ensure the software is updated to its latest version and remains fit for purpose; and
- Apply first principles when making changes to systems, policies and processes. Failing to ask when unsure of the rational or consequence could result in risks being misunderstood and potential exposure to money laundering;
- Ensure the completeness, appropriateness and frequency of training on the use and awareness of the AML software. The effectiveness of AML software is dependent on the ability of its users.

Independent Review

Given the extent and fast pace of developments within AML, boards and senior management are being recommended to obtain third-party independent advice. This both assists in fulfilling AML obligations and providing valuable guidance on the how to manage potential instances of non-compliance to encourage customer retention and business continuity.



Related insights

Receive the latest instalment of RSM's Mega Trends Series where we take a deeper look into how to drive better compliance outcomes. Click here to subscribe.

For further information

If you have any questions about this article, please contact:

Jeremy Elman
Prinicpal
Risk Advisory Services

+612 8226 4500
rsm.global/australia/jeremy-elman
jeremy.elman@rsm.com.au
Sydney