Deloitte.

Tackling financial crime risk when consolidating super and wealth entities

The impact of super and wealth management divestments, mergers and acquisitions on financial crime compliance operating models

The introduction in July 2021 of the Your Future, Your Super legislation in the Australian Superannuation sector is expected to further accelerate the increased volume of mergers & acquisitions (M&A) activity over the short to medium term. While the reforms ultimately aim to enhance the superannuation regulatory framework via the increase of measures such as annual performance tests, they will over time challenge smaller funds that lack scale and comparative performance to achieve scale via merger activity.

Funds facing the potential loss of new and existing members are likely to need to merge with other funds, a trend that has started to unfold in 2022. Additionally, the financial crime regulator, AUSTRAC, has recently highlighted that there is a renewed focus in 2022 on the superannuation and wealth industry which further compounds the challenging regulatory environment in the sector.

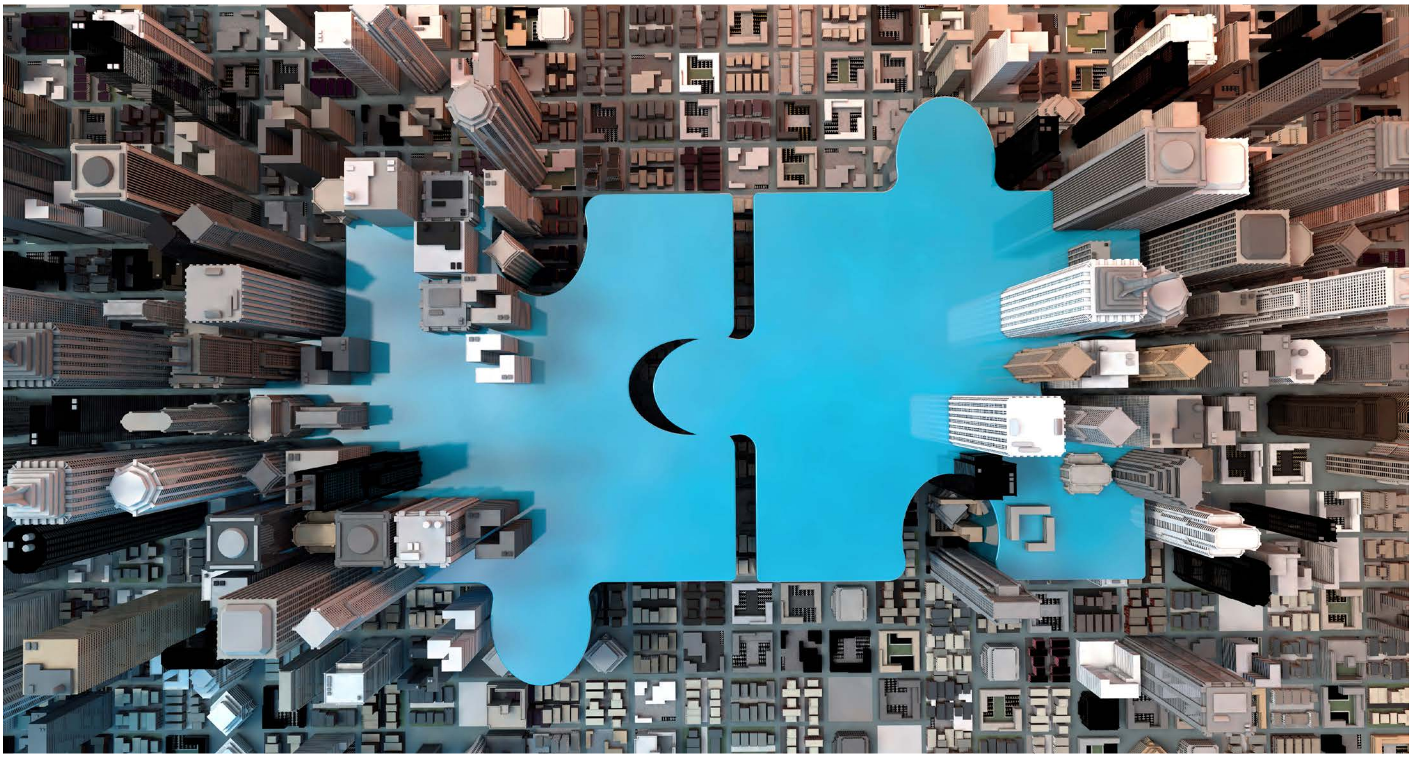
In this article, we consider a number of key questions that organisations in the super & wealth sector should consider in order to manage the financial crime regulatory risks associated with merging with or acquiring a new reporting entity. We also include some practical suggestions to assist organisations in facilitating a smooth transaction.

01. Are you aware of Chapter 28 of the AML/CTF Rules and do you intend to rely upon it?

An acquirer/buyer of a reporting entity may rely upon an exemption in Chapter 28 of the AML/CTF Rules (the Rules) to avoid having to conduct applicable customer identification procedures (ACIP) with respect to transferring customers, provided a number of conditions have been met prior to completion of merging with or acquiring an entity. Those conditions include but are not limited to:

- A designated service is provided to a transferring customer
- The acquirer has "reasonably determined" the Money Laundering/Terrorism Financing (ML/TF) risk in providing the designated services to the transferring customers
- The acquirer has "reasonably determined" that there are appropriate risk-based systems and controls to manage the ML/TF risk. This may be demonstrated by conducting a review of Know Your Customer (KYC) procedures along with sample testing of customer KYC records
- It is reasonable, based on the above assessments, to rely upon the entity's previous ACIP or continue to treat pre-commencement customers of the seller as pre-commencement customers of the buyer.

Where the entity has either assessed ACIP as not suitable or chosen not to rely upon the exemption in Chapter 28 of the Rules, it will need to conduct ACIP for all transferring customers—an onerous process not often factored into the acquisition cost.



02. Have you undertaken appropriate design and operating effectiveness due diligence to identify all financial crime risks and assess the maturity of financial crime compliance?

When financial crime risks are identified early, acquirers are better prepared to manage the risks and understand the time, cost and effort to manage any issues ahead of or following the transaction. It is important to assess how mature the target entity is in identifying, managing and mitigating its financial crime risks including a view on what the "tone from the top" is in relation to financial crime risk culture.

At a minimum, due diligence should include:

- **Reviewing the AML/CTF Program** to ensure its compliance with local AML/CTF laws and any other relevant financial crime policies and procedures that support the AML/CTF Program
- **Reviewing the effectiveness of risk-based ML/TF controls**; as part of this it is important to sample test customer records and transactions to ensure that controls are functioning as intended
- **Assessing the maturity of the organisation** in complying with its AML/CTF Program
- **Assessing the organisation's understanding** of its ML/TF risks by reviewing its enterprise-wide risk assessment, methodology and reporting. This should specifically include an assessment of the organisation's customer risk profile and any jurisdictional risk exposure
- **Reviewing the organisation's level of investment** in financial crime resourcing and capacity to handle existing financial crime operations processes
- **Evaluating recent independent reviews** and/or internal assurance reports, testing and audits to understand findings and actions taken (including how swiftly and thoroughly) to address identified deficiencies
- **Considering any current or upcoming internal investigations** or regulatory inquiries with respect to financial crime compliance
- **Assessing the training, compliance culture and governance**, specifically regarding financial crime risk, including within senior management and trustee boards
- **Understanding the status** of all in-flight projects impacting financial crime obligations including the progress of any remediation or transformation projects

Issues and weaknesses in financial crime risk management programs require significant cost, time and effort to remediate, and can lead to significant reputational and financial impact if not properly managed. These factors can be hard to quantify and as such minimising the risk during mergers and acquisitions requires early identification and a detailed understanding of the target entity's risks. It is important to understand what deficiencies have been previously identified, the degree of exposure and the costs to remediate and how those deficiencies are currently being addressed.

03. Do you have an established and comprehensive target operating model for the management of financial crime risk once the merger/divestment has taken place?

With merger or divestment activity, there are larger strategic objectives and intent at play. A developed, deployed and fit-for-purpose target operating model (TOM) that includes the management of financial crime risk and compliance obligations enables a business to transition smoothly and move forward confidently.

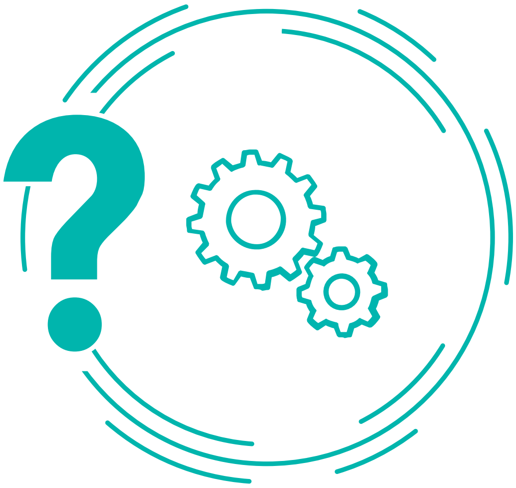
Following an acquisition, two distinctive risk profiles need to be merged to provide a refreshed view of ML/TF risk for the consolidated entity and ensure the new, holistic AML/CTF Program is appropriately scaled and fit-for-purpose. There are a number of factors to consider such as:

- What changes need to be made to the AML/CTF Program to ensure its design and operation is fit for purpose for the new merged entity?
- Are any new designated services being offered and do any additional customer identification procedures need to be applied to ensure compliance with AML/CTF obligations? For example, superannuation products may require identification checks to be performed for certain events such as an early redemption
- Is the operating model fit for purpose for the new merged entity? The scale and complexity of the new entity and its customer base require the operating model to be reconsidered, particularly the appropriateness of outsourced or in-house administration which may need to be bolstered to support new volumes or increased complexity.

In scenarios where an entity is divested from large financial institutions, there is typically a history of heavy reliance on group financial crime operational or compliance functions. These arrangements are often extended into a transition period to rely on legacy financial crime processes and systems which does not enable the divested entity to sufficiently stand on its own two feet in a timely manner, ultimately deferring or impeding the task of establishing a new, fit for purpose financial crime TOM.

"Funds will benefit from robustly assessing the AML/CTF program and membership profile of the incoming fund, assessing the ML/TF risk of the merger and ensuring that controls and transaction monitoring remain fit for purpose during any merger process."

(AUSTRAC, Australia's Superannuation Sector – Money Laundering and Terrorism Financing Threat Update, 2022)



04. How can investments in technology, systems and platforms be leveraged to improve downstream financial crime operations and reduce the cost of compliance?

Divestments, mergers and acquisitions are unique opportunities for organisations to strategically invest in uplift to financial crime technology, systems and platforms to benefit the overall business. This may include investing in:

- **Cloud computing, big data and analytics** to digest increased volumes of structured and unstructured data, enabling operational processes and regular reporting to senior management. These technologies can consolidate data from disparate sources to enhance accuracy and accessibility of information throughout the organisation, creating a single source of truth with near real-time access to data
- **Robotic Process Automation** to streamline manual business processes such as copying information between systems and templates
- **Natural Language Processing** to interpret meaning from the human language and process large volumes of data to judge whether member behaviour is suspicious. Combining these technologies can automate tasks requiring complex reasoning and judgements and help entities direct resourcing to the managing of risk as opposed to burdensome administrative processes.

05. Should the newly merged entity continue with its outsourcing arrangements?

An entity may see the benefits of a third party provider's range of services including ACIP, ongoing customer due diligence and transaction monitoring. However, there are a number of challenges associated with outsourcing these financial crime compliance activities to a third party:

- **Demonstrating the risk-based approach:** Where a trustee outsources elements of its administration of a superannuation fund to a third party, there are instances in the market where that third party will adopt a 'one-size fits all' model across many different funds, running the same transaction monitoring rules with limited ability to adapt the ruleset according to the specific ML/TF risks the fund is facing. In such cases, the trustee remains responsible for ensuring compliance with the Rules which require a risk-based approach driven by its own, unique ML/TF risk profile.
- **Relying on the administrator's rules-based approach:** This can result in numerous false positive alerts being generated on members given the lack of baseline information and the 'one size fits all' models described above. These can ultimately offset the initial benefit of the outsourced approach as large volumes of alerts can come back to the entity for decision making. Further to this, there may also be situations where there is misalignment between the ML/TF rules executed by an administrator and the ML/TF risks identified by the fund relying on these rules.
- **A false sense of security:** an outsourcing arrangement may suggest that the fund doesn't need the resources and capability in-house even though it is the fund (the reporting entity) that remains accountable to ensure these measures are appropriately risk-based for the fund in accordance with AML/CTF legislation. This extends to a reporting entity's broader operational value chain and assessing the level of risk that may in fact be introduced from outsourced provider relationships.
- **A fund's ability to scale up or expand financial crime operations can be significantly hampered:** This has been a key challenge in the recent economic climate resulting from the COVID-19 crisis and the subsequent regulatory changes, including provisions for early access to super. The ATO reported 2.7 million approved early super access applications totalling $19.9 billion[1], placing financial crime operating models under significant strain. Sudden changes in the nature, volume and velocity of financial crime operational alerts may need to be reviewed and triaged, which may prove challenging in cases where there is a high degree of dependence upon a third party.
- **A fund cannot rely only upon a risk assessment that the third party has conducted on its members:** The reporting entity is required to conduct their own risk assessment of its members and determine if additional due diligence is required, rather than relying solely upon the third party's risk assessment.

To overcome some of the above challenges, entities are increasingly subjecting third party service providers to regular risk assessments, audits and compliance reviews to ensure they are sufficiently executing, managing and responding to ML/TF risks that arise in the provision of outsourced services.

1. https://www.ato.gov.au/Super/Sup/COVID-19-early-release-of-super---interim-report--2019-20-applications/?anchor=Applicationsbyfundtype#Applicationsbyfundtype

Concluding remarks

If organisations fail to prioritise the management of financial crime risk ahead, during and following an acquisition, they may encounter legal, regulatory and reputational risks. This is against a backdrop of increasing regulatory enforcement activity with respect to non-compliance with financial crime laws.

In addition to taking a holistic and thorough approach to the management of financial crime risk, an appropriate level of due diligence and rigour is needed to assess the compatibility of the businesses, ensure overall risk is appropriately managed and the transaction aligns with overall business strategy.

In some cases, the acquisition or divestment may even generate opportunities to realise efficiencies through the redesign of the operating model, streamlining of processes and implementation of new technologies.

Deloitte understands the key financial crime risks and practical implications when undertaking M&A transactions. Should you wish to discuss the above or require any assistance with managing financial crime risk throughout the course of a transaction, please do not hesitate to get in touch.

About the team

As a recognised market leader in Financial Crime risk management, regulatory response and investigations, Deloitte offers a unique combination of expertise, local and global experience, deep understanding of the drivers of the AML/CTF regime in Australia, and value through proven global methodologies, tools and deep networks.

Our highly experienced and specialist team brings a diverse range of experience and skills, across regulation, law enforcement, industry, technology, data and forensic investigations/accounting, to assist our clients in meeting their regulatory obligations when tackling these challenges. Clients we have supported and advised include local and offshore regulators and law enforcement, financial institutions, large and emerging payments and technology companies and industry bodies.

We can help with:

- Risk assessments
- Investigations
- Independent reviews and compliance inspections
- Advisory and consulting services
- Implementation
- Remediation and lookback reviews
- Regulatory response

To learn more about Deloitte's financial crime solutions and our latest thought leadership, please click here.

Contacts

Lisa Dobbin

Partner | Financial Advisory | Sydney

ldobbin@deloitte.com.au

Ben Murphy

Partner | Financial Advisory | Brisbane

bemurphy@deloitte.com.au

Amanda Lui

Partner | Financial Advisory | Melbourne

amlui@deloitte.com.au

Created by CoRe Creative Services. RITM1123831