Tranche 2 AML/CTF Reform in Australia

What **lawyers**, **accountants** and **real estate** professionals must know – and how to prepare

Author: **Greta Menzies**
Chief Executive Officer
My Databoss

February 2026

My Databoss

Contents

Foreword

Greta Menzies,
Chief Executive Officer,
My Databoss

For decades, Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations have fallen on banks. Professional services have operated outside that system – until now.

Anyone who has worked in financial crime, law enforcement or regulatory policy knows that criminals operate well beyond banks. They rely on professionals like lawyers, accountants and real estate agents to move, structure and legitimise money.

Property is not just a place to live; it is a store of value.

Lawyers and conveyancers are not just trusted advisers; they sit at the point where money, property and ownership change hands.

Professional advice is not just guidance; it is the gateway to financial systems.

This is why Tranche 2 matters.

As of July 2026, up to 100,000 Australian professional services firms are formally recognised as part of the financial system. They are accountable not only for who they act for, but for how money flows through their services, what risks those flows carry and what evidence exists to demonstrate that those risks have been managed.

This shift goes beyond regulation. It is structural. It changes how data, identity, privacy, security and compliance intersect.

At My Databoss, we work at that intersection every day. We see that identity verification, consent, data governance, data security and regulatory compliance must work together if professional firms are to meet their obligations in an efficient, defensible and trustworthy way.

This whitepaper helps leaders in legal, accounting and real estate understand what Tranche 2 really means, why it exists and how to use this moment to go beyond compliance and build lasting competitive advantage.

Executive Summary

Tranche 2 of Australia's Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) reforms represents the most significant expansion of financial crime regulation in a generation.

From **1 July 2026**, law firms, accounting practices and real estate businesses that provide one or more **designated services** are, for the first time, classified as **reporting entities** under the AML/CTF Act. This requires them to:

- Appoint an AML/CTF Compliance Officer
- Enrol with AUSTRAC
- Conduct a risk assessment
- Maintain a formal AML/CTF Program
- Identify and verify clients – known as Customer Due Diligence (CDD)
- Run risk-based client assessments
- Monitor client behaviour and transactions
- Report suspicious matters to AUSTRAC
- Keep auditable records
- Train staff in AML/CTF obligations

These obligations are not theoretical. They are legally enforceable and carry civil, criminal and reputational consequences.

Most professional firms want to comply but lack the systems to do it properly, having never before operated under a regime designed for financial institutions. Identity verification, beneficial ownership, transaction monitoring, record retention and regulatory reporting have historically been fragmented across spreadsheets, emails, trust accounting systems and filing cabinets.

That fragmentation will not withstand regulatory scrutiny.

Proliferation financing (PF):
The reforms also address the funding of weapons of mass destruction. When we refer to AML/CTF in this paper, this includes the requirement to consider proliferation financing risk as part of a firm's overall risk assessment.

Why Tranche 2 and why now?

> In 2023-24, the cost of organised crime to Australia grew to $82.3 billion, a sharp $13.6 billion increase from $68.7 billion in 2022-23."
>
> – Australian Criminal Intelligence Commission, Nov 2025

Money laundering underpins organised crime. Illicit funds from drug trafficking, fraud, tax evasion and corruption all need to be cleaned before they can be used. That requires access to assets, structures and professional services.

Criminals don't solely use banks to do this. They purchase property, establish companies and trusts, move funds through client accounts and use professional services to convert illegal proceeds into legitimate wealth.

Global regulators have recognised this for decades. The Financial Action Task Force (FATF) describes lawyers, accountants and real estate professionals as gatekeepers to the financial system. In Australia, the Criminal Intelligence Commission has flagged increasing recruitment of these same professionals by organised crime.

In the UK, New Zealand, the US and the EU, these sectors have been regulated for years, but Australia has lagged behind. While banks, casinos and remittance services have been subject AML/CTF obligations, professional services have not – until now. This is despite their central role in high-value transactions and ownership structures.

This gap has made Australia vulnerable and a known destination for illicit funds.

Tranche 2 aims to close the loophole. From 1 July 2026, professional services firms of all sizes providing designated services become reporting entities under the AML/CTF Act.

Does Tranche 2 apply to you?

One of the most common misunderstandings about Tranche 2 is that it applies only to large firms or specialist operators. The law is triggered not by size, but by what you do.

The AML/CTF Act does not regulate professions in the abstract. It regulates **designated services** that create a high risk of money laundering or terrorism financing.

If a firm provides even one designated service, it becomes a **reporting entity** for those activities and must comply with the AML/CTF regime in full.

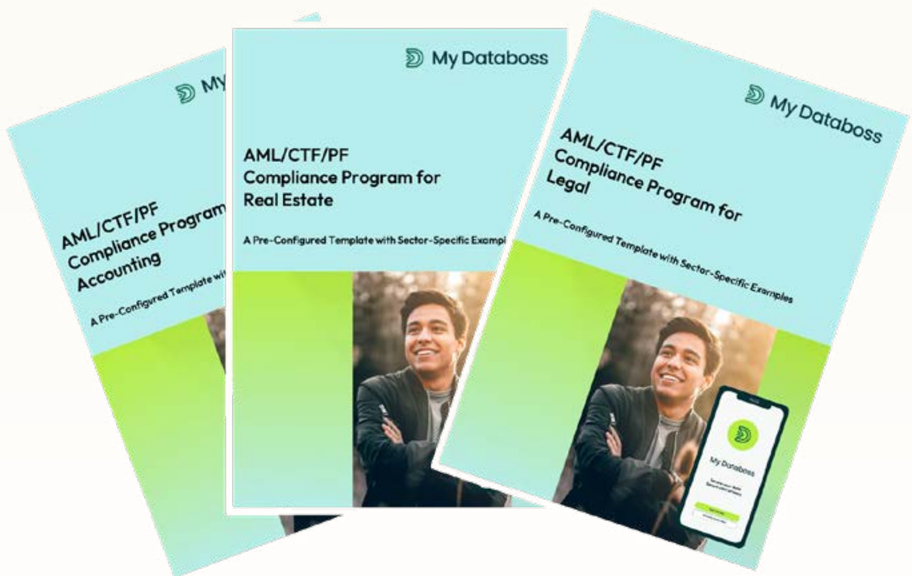
This means thousands of professional practices will fall within scope, regardless of business size.

A sole practitioner law firm holding $200,000 in trust funds carries the same AML risk as a national firm holding $200 million. A suburban real estate agency handling one high-value foreign purchase can face the same regulatory exposure as a major franchise network.

In fact, while corporate breaches get the headlines, regulatory experience suggests criminals often target smaller firms with less mature compliance environments as they can be easier to infiltrate.

Tranche 2 also extends to trust and company service providers, dealers in precious metals and stones, and certain other roles adjacent to property and financial structuring.

If you provide a designated service, you are in scope.



Legal and Conveyancing

Lawyers and law firms become reporting entities when they provide services involving client funds, asset transfers or the creation and control of legal structures.

This covers core commercial and property work from suburban conveyancing to boutique trust work to corporate restructures.

If you provide any of these services, Tranche 2 applies:

- Acting for clients in buying or selling real estate or businesses
- Conducting conveyancing or property settlements
- Holding or transferring client funds through trust accounts
- Establishing or managing companies, trusts or partnerships
- Acting as a nominee director, shareholder or trustee
- Providing registered office, correspondence or principal place of business services
- Managing client assets or financial interests

Many lawyers and conveyancers are unfamiliar with the new AML obligations and unprepared for the changes.

Accounting and Advisory

Accounting and business advisory firms become reporting entities when they move beyond basic tax returns and bookkeeping into financial structuring, entity management or client funds.

This includes tax advisers establishing self-managed super funds (SMSFs), accountants managing client bank accounts, and advisory firms structuring ownership arrangements.

Our members' biggest worry is making sure they stay on the right side of the law."
– CPA Australia

If you provide any of these services, Tranche 2 applies:

- Setting up companies, trusts, partnerships or SMSFs
- Acting as company secretary, trustee or nominee
- Managing or controlling client bank accounts
- Providing registered office or corporate services
- Structuring ownership, control or financial arrangements
- Holding authority over client funds

Real Estate and Property

Real estate is one of the highest-risk sectors for money laundering globally, as it converts large sums of money into long-term, appreciating assets.

This captures sales agents, conveyancers, settlement agents and anyone facilitating property transfers or handling transaction funds. AML/CTF obligations apply before a designated service is provided.

If you provide any of these services, Tranche 2 applies:

- Acting for buyers or sellers of property
- Facilitating the transfer of property ownership
- Receiving or handling deposits or settlement funds
- Managing trust accounts for property transactions
- Acting for foreign, corporate or trust-based buyers
- Assisting with property development or structuring

Most real estate agents report concern about preparing for new compliance obligations.

So, you're a reporting entity. What now?

Your legal obligations

As a reporting entity under the AML/CTF Act, you enter an ongoing regulatory relationship with AUSTRAC. These are continuous governance responsibilities, not one-off compliance tasks.

The law requires you to actively manage money-laundering risk, document your decisions and produce evidence on request. Each obligation below outlines what you must do and what you'll need to prove.

1. Appoint an AML/CTF Compliance Officer

Your firm must appoint a Compliance Officer to oversee your AML/CTF Program. This person is accountable for ensuring obligations are implemented and maintained, and acts as your primary contact with AUSTRAC.

The Compliance Officer must be senior enough to influence policies, procedures and resourcing – typically a principal, partner or senior manager. They don't need to be an AML specialist, but must have the capability and independence to perform the role effectively and seek specialist support where required.

Responsibilities typically include:

- Overseeing the AML/CTF Program's operation
- Monitoring compliance with obligations and internal controls
- Supporting the identification and escalation of suspicious matters
- Ensuring staff receive appropriate training
- Reporting on compliance to senior management

Tasks may be delegated, but accountability remains with the Compliance Officer.

What you'll need to prove: Formal appointment, documented responsibilities, evidence of active oversight and records of decisions, training and reporting.

2. Enrol with AUSTRAC

Obligations commence 1 July 2026, with AUSTRAC enrolments opening 31 March 2026. You must enrol within 28 days of obligations commencing. This establishes your identity in the regulatory system and creates the foundation for all future reporting and supervision.

You'll need to provide your legal and trading names, ownership and control details, the designated services you offer and your principal compliance contacts.

What you'll need to prove: Current enrolment and accurate details on file with AUSTRAC. Keep your enrolment current as your firm evolves.

3. Conduct a risk assessment

Your firm must conduct and maintain an enterprise-wide risk assessment for money laundering and terrorism financing. This assessment drives your entire compliance program.

The purpose is to understand what services you provide, who you provide them to, how money flows through those services and where you're most exposed to misuse. Common risk areas include:

- **Legal:** Property settlements, trust account movements, offshore clients, complex ownership structures.
- **Accounting:** Entity formation, SMSF administration, nominee arrangements, cash-intensive businesses.
- **Real estate:** High-value properties, foreign buyers, rapid resales, unusual payment methods.

What you'll need to prove: A documented, firm-specific risk assessment that reflects your services, client base and risk exposures. Keep it current as your business evolves.

4. Maintain a formal AML/CTF Program

Your firm must maintain a written AML/CTF Program that documents how you will identify and verify clients, assess and manage risk, train staff, monitor activity, keep records and report suspicious matters.

This becomes your compliance rulebook. AUSTRAC will ask for it during audits and investigations. The program must reflect what your firm actually does. A generic template that doesn't match your operations is not adequate.

What you'll need to prove: A written AML/CTF Program tailored to your services, risk profile and operating procedures that is updated as your business or risk environment changes.

5. Implement Customer Due Diligence (CDD)

Before providing a designated service, you must identify and verify your client using CDD – commonly called Know Your Customer (KYC) for individuals and Know Your Business (KYB) for entities. It answers three questions: who are you dealing with, who owns or controls them and is the relationship legitimate?

- **For individuals**, this means identifying and verifying the client's identity using reliable and independent sources.
- **For businesses**, it extends to registration details, directors, shareholders and beneficial owners – the people who ultimately own or control the entity, even if they're not named on company documents.
- **Higher-risk clients** require enhanced due diligence (EDD): deeper verification, more detailed risk assessment and closer ongoing scrutiny. Triggers include complex ownership structures, politically exposed persons (PEPs), high-risk jurisdictions or unusual transaction patterns.

What you'll need to prove: Verified identity records for every client, documented beneficial ownership and evidence of EDD where risk factors apply – all completed before the designated service begins.

6. Run risk-based client assessments

Beyond verifying identity, you must assess the risk each client represents – evaluating their business, the services requested, the jurisdictions involved and the source of funds.

A suburban homeowner purchasing a family property presents a different risk profile than an offshore entity acquiring commercial real estate through a nominee structure. Your controls should reflect this and apply enhanced scrutiny, requesting additional documentation where required and managing engagements within your firm's documented risk tolerance.

What you'll need to prove: Documented risk assessments for each client, evidence that controls were adjusted to match risk level and records of decisions to apply EDD or decline an engagement.

7. Implement ongoing monitoring

AML compliance doesn't end once a client is onboarded. You must monitor for changes in client behaviour, unusual transaction patterns, changes in ownership or control and emerging risk factors.

For example, if a property buyer suddenly changes settlement funding, a company adds a foreign shareholder or a trust restructuring occurs mid-transaction, each client's risk rating may need to be reviewed and updated. This is where manual systems with static files often fail.

What you'll need to prove: Records of ongoing monitoring activity, evidence that risk ratings were reviewed when circumstances changed and documentation of any actions taken in response.

8. Submit Suspicious Matter Reports (SMR)

When you suspect a client, transaction or behaviour may involve money laundering or criminal activity, you must submit a Suspicious Matter Report to AUSTRAC. This obligation is strict:

- Report promptly
- Do not disclose to the client (tipping-off is an offence)
- Base your report on documented observations and evidence

Professional firms often struggle with this. Staff may be unsure what constitutes suspicion, evidence is scattered across systems or there's no clear escalation path. Training and processes are essential to ensure your team knows what to look for and how to act.

What you'll need to prove: A documented process for identifying and escalating suspicious matters, records of any SMRs submitted and evidence that staff are trained to recognise red flags.

9. Keep auditable records

From a regulator's perspective, what you cannot prove did not happen. Every step of your AML/CTF process must be recorded, retained for the required period, stored securely and available for production during an audit. This includes:

- AML/CTF Program
- Identity documents
- Risk assessments
- Verification and screening outcomes
- Monitoring results
- Staff training
- Reports lodged with AUSTRAC

What you'll need to prove: A complete, secure and accessible record of all AML/CTF activity ready to produce when AUSTRAC asks.

10. Staff training and governance

AML/CTF compliance is as much about governance as it is about technology. All staff involved in designated services must understand their AML responsibilities, recognise red flags and follow documented procedures.

Training must be regular, relevant to each role and recorded. Senior leadership must ensure the program is implemented, reviewed and resourced appropriately. Leaders can delegate compliance tasks, but not their accountability.

What you'll need to prove: Training records for all relevant staff, evidence of regular refresher training and documented oversight by senior leadership.

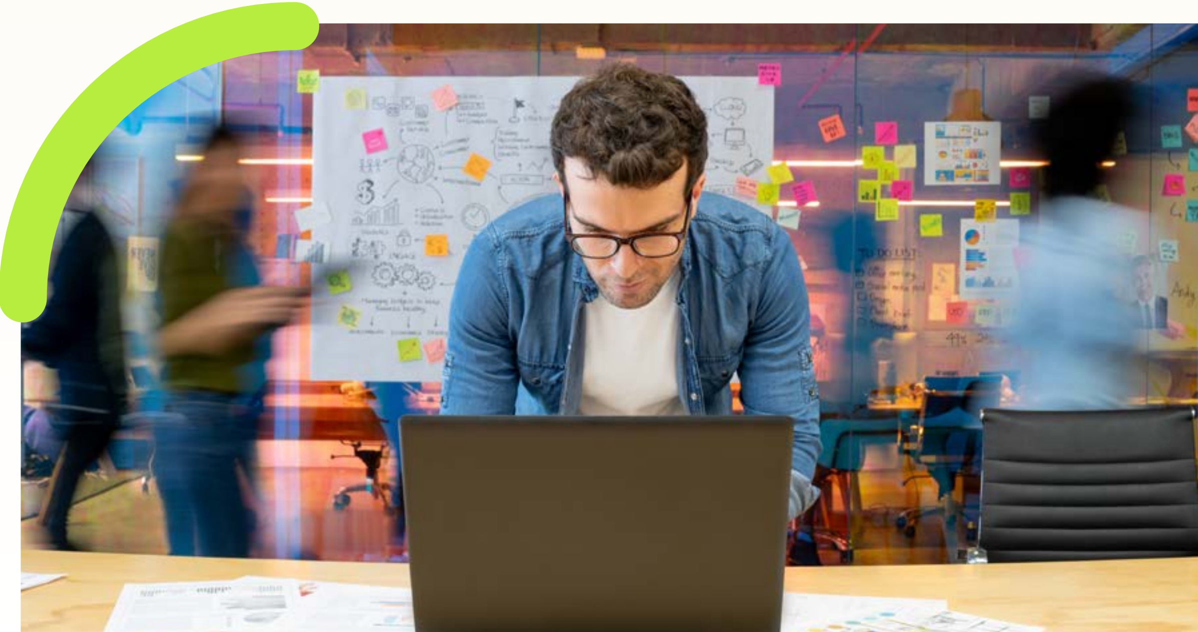
Why most firms are not ready

Broadly, AUSTRAC wants answers to three questions:

- Did you understand your risk?
- Did you apply appropriate controls?
- Can you demonstrate what you did?

The third question is where many firms fall down. AUSTRAC judges compliance by evidence, not effort or intent. Even firms that understood and applied the law have failed because they couldn't show, months or years later, what they actually did.

OLD WAY: Manual processes and fragmented tools	**NEW WAY:** Integrated, end-to-end AML/CTF workflows
Policy documents in a folder	Live compliance system
Identity stored in emails	Verified identity records
Risk in someone's head	Documented, scored risk ratings
Ad hoc monitoring	Ongoing alerts and reviews
Manual spreadsheet reports	Logged, timestamped reports
Training by word of mouth	Recorded, trackable training



The execution gap

By the time Tranche 2 comes into force, most legal, accounting and real estate firms will have prepared a basic risk assessment, an AML/CTF Program and some form of onboarding process.

Yet international experience shows that compliance failures rarely occur at the policy level. The risk lies in the gap between what a firm says it does and what actually happens day to day.

The fragmentation problem

Most professional firms operate with fragmented information. Client identity is held in a scanned passport, an email attachment, a customer relationship management (CRM) system or a trust accounting system. Risk assessments sit in a Word document, a spreadsheet or a PDF on a shared drive. Monitoring exists in the head of a partner, a note in a file or an informal conversation.

From a regulatory perspective, this is an evidence gap. AUSTRAC audits what was checked, when it was checked, what risk was identified and what was done in response. If that information can't be produced in a consistent, time-stamped, auditable form, the firm is exposed – regardless of how good its written policies look.

Fragmentation also drives hidden costs: staff time searching for documents, clients asked to resubmit identity records, partners reconstructing what happened months ago. These costs compound as client numbers grow. And when something goes wrong – a missed verification, an incomplete audit trail, an unreported suspicion – the cost shifts from inefficiency to risks of remediation payments, regulatory scrutiny and reputational damage.

Some firms attempt to close these gaps by combining an ID verification tool, a screening service, a spreadsheet and a shared drive. Each may work in isolation, but they don't integrate closely enough to form a compliance system.

What's missing is a single source of truth with consistent risk logic and an audit trail that connects identity, risk and records into a single auditable workflow.

Why templates and consultants won't cut it

Many firms will start with AML policy templates, compliance manuals or external consultants. These have value, but they don't solve the operational problem.

A consultant can write a risk assessment and a generic template can describe the perfect procedure, but neither can ensure that staff actually follow it, that decisions are recorded or that risk ratings are updated as circumstances change. Once the consultant leaves, the real compliance burden falls back on the organisation.

This is why AML compliance has shifted from a documentation exercise to a systems challenge.

What is your Tranche 2 readiness level?

Level	What it looks like	Regulatory risk
1: Informal	IDs in email, spreadsheets, partner discretion	Very high
2: Documented	AML policy, some checklists, manual tracking	High
3: Systemised	Identity, risk and records in one platform	Low
4: Governed	Real-time monitoring, audit trails, group oversight	Very low

Today, most firms sit at level 1 or 2 and will not withstand audit scrutiny. Level 2 is deceptive because firms often believe they are compliant until an audit reveals they can't prove it. Levels 3 and 4 are where compliance systems become effective and defensible under Tranche 2.

The data governance challenge

AML compliance is fundamentally a data problem. Identity, ownership, consent, transaction history, risk scoring and auditability all intersect with privacy law, cybersecurity, professional confidentiality and information governance.

Tranche 2 amplifies these pressures. Firms must collect and retain some of the most sensitive information they will ever hold – from passports and ownership structures to financial transactions and behavioural data – while privacy laws require them to minimise collection, limit retention and control access. Reconciling these objectives requires a structured data governance framework.

Collecting too much data increases the risk of breaches, while not collecting enough or deleting it too quickly undermines auditability, the legal foundation of compliance. Tranche 2 forces firms to manage this balance properly for the first time.

The shift in legal authority

Professional firms are accustomed to collecting client data for service delivery. AML/CTF changes this. Identity and ownership data is now collected for legal compliance, crime prevention and regulatory reporting.

Firms must be able to demonstrate what was collected, for what purpose, under what authority and for how long it is to be retained.

Continuous compliance

Tranche 2 introduces continuous compliance to professional services. Instead of onboarding once and filing a document, firms must continuously assess risk, update client profiles and monitor behaviour over time.

This mirrors how banks operate, but without their legacy systems or compliance teams. The burden shifts from people remembering to act to systems that enforce and record what must happen.

Tranche 2 brings up to 100,000 Australian professional firms into the financial crime control system.

> **Most understand they must comply. But the challenge isn't intent, it's infrastructure. Fragmented systems won't deliver efficiency or withstand scrutiny over the long term.**

My Databoss: Compliance Infrastructure for Tranche 2

My Databoss makes AML/CTF compliance practical for professional firms of any size, with an enterprise-grade, privacy-first platform built on Microsoft cloud, ISO27001-certified and hosted in Australia.

Accessible and affordable, it connects identity verification, consent, data governance and compliance in one place through plain-English workflows aligned to AUSTRAC requirements – with expert local support to get you compliant.

This is your opportunity to turn regulatory burden into competitive advantage, strengthen client trust and build a firm that's defensible for the long term.

Go beyond compliance

Single system of record

Replace fragmented tools with one platform connecting identity, risk assessments, client profiles, monitoring, compliance records and audit trail. Evidence is produced automatically. Policy, practice and reporting align.

Built for your industry

Pre-populated AML/CTF Program templates for legal, accounting and real estate. Plain English, aligned to AUSTRAC requirements and linked to onboarding, risk and monitoring workflows. Executed every time the system is used.

Consent and privacy by design

Balance the collection of sensitive data with strict privacy obligations. Clients see why their data is collected, how it's used, who sees it and how long it's kept. Transparency builds trust and protection for all parties.

Australian-made, globally assured

Designed, built and hosted in Australia to meet AUSTRAC requirements. Enterprise-grade infrastructure on Microsoft Azure with ISO27001 certification. Security, privacy and regulatory credibility in one platform.

Upload once, use many times

Clients verify their identity once and consent to reuse it across professional relationships. Each firm maintains its own compliant record and audit trail. Less friction and more privacy for clients, fewer duplicate requests for firms.

Expert local support

Built-in risk assessments, staff training with completion tracking and step-by-step implementation guidance – including 90 days of phone and email support. Get compliant without consultants or expertise you don't yet have.

My Databoss at a glance

Every Tranche 2 obligation maps to a platform capability:

Regulatory obligation	Operational requirement	My Databoss
AML/CTF Compliance Officer	Designated accountability and oversight	Role-based access with clearly defined designated Compliance Officer responsibilities oversight and decision tracking
AUSTRAC enrolment	Firm and service registry	Guided support to ensure accurate enrolment and maintenance of firm and designated service details.
Risk assessment	Structured risk scoring	Pre-populated, industry-specific risk assessments with suggested controls, tailored to each firm's services, client base and risk profile, and mapped to operational workflows
AML/CTF Program	Rules engine and workflows	Industry-specific, pre-populated program templates linked to live, auditable workflows
Client due diligence (CDD)	Identity and ownership verification	Standardised onboarding for individuals (KYC) and businesses (KYB). Politically exposed persons (PEPs), sanctions and adverse media screening. Ownership and control capture within business client profiles
Risk-based client assessment	Client-level risk rating	Risk settings dynamically influence onboarding and data requirements
Ongoing monitoring	Dynamic risk tracking	Continuous monitoring and change of status flagging
Suspicious matter reporting (SMR)	Escalation and reporting channels	Internal escalation workflows, Compliance Officer review and suspicious matter report preparation with complete audit trail
Record keeping	Secure, immutable audit trail	Centralised client, business and compliance records. Complete, time-stamped audit trails and evidence
Staff training	Training and compliance records	Built-in AML/CTF staff training with completion tracking and evidence of ongoing competency

My Databoss enables professional firms to meet their Tranche 2 obligations with confidence and to use this moment to modernise operations, strengthen client relationships and build lasting competitive advantage.

"We needed consistent compliance processes for every office and agent across the network, with one system that works the same way. My Databoss gives us that, as well as full confidence that we'll be protected and audit-ready when Tranche 2 takes effect."

– Daniel O'Brien, Chief Executive Officer, X Commercial

In practice: **Owen Hodge Lawyers**

Owen Hodge Lawyers is a Sydney-based firm with a strong property, commercial and litigation practice. Recognising that Tranche 2 would change how professional firms manage client identity, data and risk, the firm chose to prepare well ahead of the July 2026 deadline.

The challenge

Like many law firms, Owen Hodge faced new requirements for client due diligence, risk assessment, monitoring and record-keeping.

But regulation wasn't the only driver. The firm had already identified operational risks: fragmented identity records, manual verification processes and the cyber exposure that comes with storing sensitive client data on internal systems.

Traditional approaches – policy documents, spreadsheets and manual checks – were unlikely to scale or withstand regulatory scrutiny. The firm wanted a solution that would support compliance while improving data security, efficiency and client experience.

The approach

The firm took a leadership-led approach to Tranche 2 readiness, combining governance, training, change management and technology.

A key decision was implementing My Databoss as a core compliance and data-governance platform. Owen Hodge became an early user, working closely with the My Databoss team during development to ensure it met the practical needs of a legal practice.

My Databoss enabled the firm to:

- Implement structured, risk-based client due diligence and monitoring
- Reduce reliance on manual identity handling and document storage
- Give clients a secure way to share and manage their identity information
- Establish clear escalation pathways and Compliance Officer oversight
- Create an auditable record of compliance activity aligned to AUSTRAC expectations

The rollout included firm-wide training, recognising that AML/CTF compliance is a cultural shift as much as a regulatory one.

The result

Owen Hodge is on track for Tranche 2 readiness well ahead of the deadline. The firm has strengthened its data security by reducing the volume of sensitive identity information held on internal systems, lowering cyber exposure.

Onboarding and verification are now more consistent and efficient. Clients benefit from a more secure and streamlined experience. And the firm has clear oversight, escalation pathways and evidence to support regulatory engagement.

Beyond compliance, the initiative has positioned Owen Hodge as an early mover in Tranche 2 preparedness – reinforcing client trust and demonstrating how regulatory change can drive practice modernisation.

In 2025, Owen Hodge was recognised with the **ALPMA Business of Law – Excellence in Technology and Innovation** award.

“My Databoss has transformed how we handle client identity verification and compliance. It gives us confidence that obligations are being applied consistently, without disrupting how we work.”

– Rolf Howard, CEO & Commercial Litigation Lawyer, Owen Hodge Lawyers

Your roadmap to Tranche 2 compliance

Tranche 2 is one of the most significant regulatory changes to affect Australian professional services in decades. Far more than a box-ticking exercise, it's an opportunity to go beyond compliance and modernise your operations with systems that last.

Compliance has four distinct steps: understand your obligations, design your framework, implement systems and maintain governance.

Even if you're only beginning now, you've still got time.

My Databoss supports you at every stage – from initial risk assessment through to ongoing monitoring and audit readiness – to move quickly into a compliant, defensible position.

You don't need to figure this out alone.

Book a demo → Learn more → Talk to our team →

"My Databoss is a powerful solution that simplifies compliance across AML/CTF, privacy and cybersecurity – making life safer and easier for both professionals and clients."

– Agnieszka Szczepanik, Founder & MD, LYRA Risk and Compliance

Sources and further reading

This paper draws on publicly available guidance from AUSTRAC, the Financial Action Task Force (FATF) and the Australian Criminal Intelligence Commission. For the latest regulatory updates and detailed guidance:

- AUSTRAC: **austrac.gov.au**
- AUSTRAC: **Real Estate Sector Brief**
- FATF: **fatf-gafi.org**
- ACIC: **acic.gov.au**
- My Databoss: **mydataboss.com**

Glossary of terms

Term	Definition
AML	Anti-Money Laundering – laws and processes to detect and prevent the concealment of illegally obtained funds
CTF	Counter-Terrorism Financing – laws and processes to detect and prevent funds from being used for terrorist activities
PF	Proliferation Financing – the funding of weapons of mass destruction; addressed under the same regulatory framework
AUSTRAC	Australian Transaction Reports and Analysis Centre – Australia's financial intelligence agency and AML/CTF regulator
Beneficial owner	The person who ultimately owns or controls an entity, even if not named on official documents
CDD	Customer Due Diligence – the process of identifying and verifying clients before providing services
Designated service	A specific service or activity that triggers AML/CTF obligations under the AML/CTF Act
EDD	Enhanced Due Diligence – additional verification required for higher-risk clients
FATF	Financial Action Task Force – the international body that sets global AML standards
IFTI	International Funds Transfer Instructions — reports submitted to AUSTRAC when funds are transferred into or out of Australia
KYB	Know Your Business – due diligence processes for verifying business clients
KYC	Know Your Customer – due diligence processes for verifying individual clients
PEP	Politically Exposed Person – an individual in a prominent public position, requiring enhanced scrutiny
Reporting entity	An organisation required to comply with the AML/CTF Act because it provides designated services
SMR	Suspicious Matter Report – a report submitted to AUSTRAC when suspicious activity is identified
TTR	Threshold Transaction Reports — reports submitted to AUSTRAC for cash transactions of $10,000 or more

Tranche 2 isn't just regulation. It's reputation.

Get ahead and stay trusted.

Reach out anytime

Call: 1300 512 387 | **Email:** sales@mydataboss.com

Visit: mydataboss.com | **Connect:** On LinkedIn

My Databoss

"Our mission is to help businesses not just meet the AUSTRAC Tranche 2 but to thrive by putting a defensible compliance framework in place that they can manage with confidence, clarity and control."

– Greta Menzies, Chief Executive Officer, My Databoss