easyAML

AML/CTF Compliance: Operational Readiness

What your business needs to do beyond the compliance platform.

/ The easyAML platform handles your compliance obligations. Your business still has to handle everything around it.

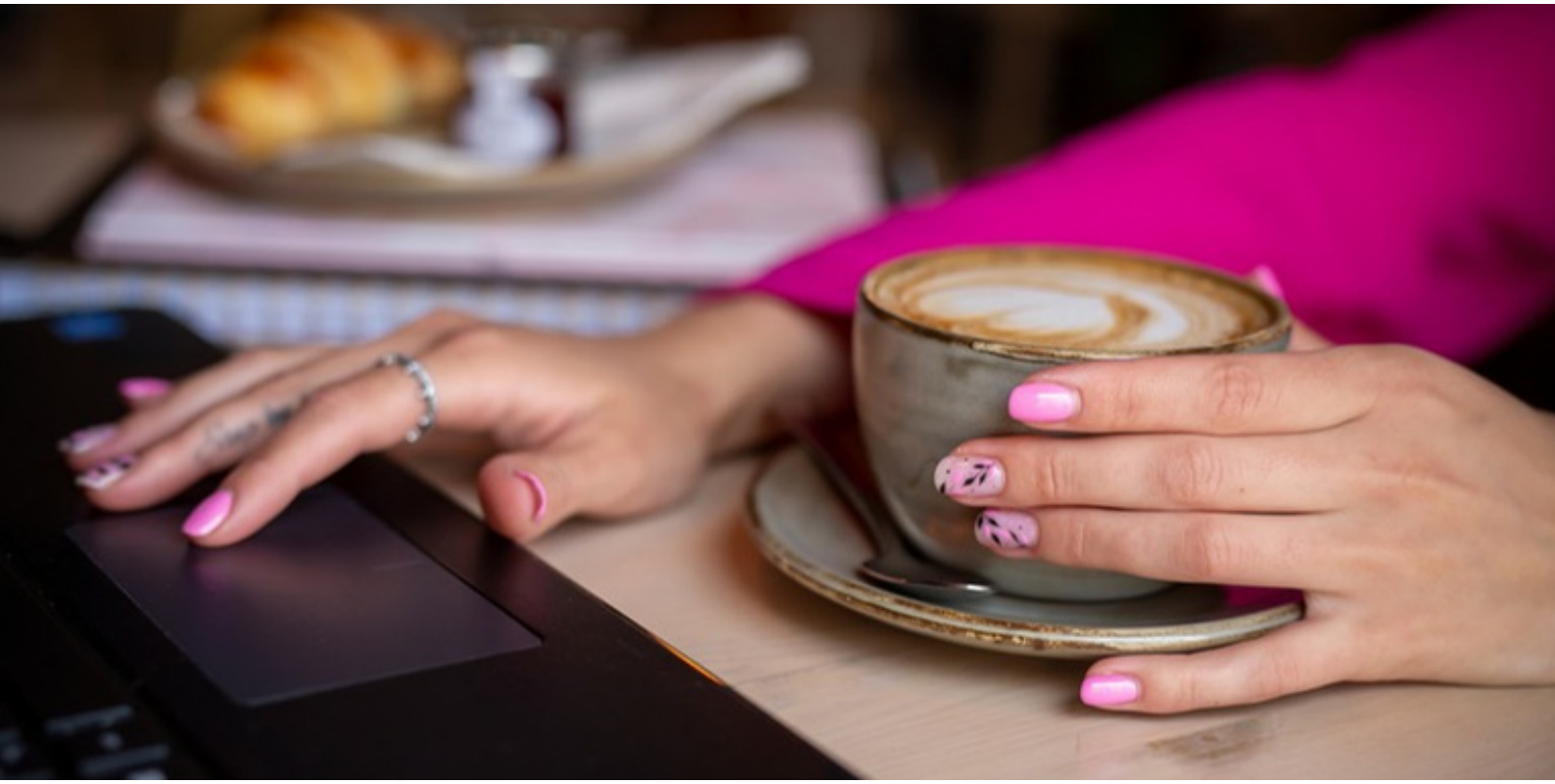
easyAML gives you the AML program, risk assessment, CDD/EDD workflows, training, and record-keeping.

What it cannot do is redesign your internal workflows, update your employment contracts, brief your team, remediate your existing client base, or register your business with AUSTRAC.

The businesses that struggle to meet the deadline are rarely the ones who left choosing a platform too late. They are the ones who underestimated the internal operational lift — and started it too late to get it done properly.

This document covers the list of operational tasks every firm should consider, it is not meant to be definite but a guide to assist you before you Go Live.

Part 1 contains tasks that all businesses should consider.
Part 2 contain tasks that are typically only material for medium and large firms.



PART 1: Common operational readiness

Applies to every firm

1. Decisions that must be made before anything else can proceed

Several downstream tasks cannot start until a principal (this could be CEO, Director, Managing Partner or Licensee) has made an active decision. These are not administrative tasks — they require a judgment call, and they unblock everything else.

Appoint a Compliance Officer and define their authority

Principal* (*CEO/ Managing Partner /Director/ Licensee

Whoever is appointed needs to understand the role before they can do anything in it. If it's an existing staff member, their other responsibilities may need adjusting.

☐ .....

Decide your KYC/KYB pricing model (absorb, on-charge as a disbursement, or build into a fixed fee)

Principal

This decision drives your engagement letter, fee disclosure, quote templates, PMS setup and accounting software. Pick one approach and everything downstream follows from it.

☐ .....

Decide your approach to existing/legacy clients

Principal Compliance Officer

You need to know which clients require retrospective CDD, and whether you will re-verify all active matters, only high-risk ones, or take a risk-based approach. This determines the scope of a substantial internal workload.

☐ .....

Decide who will perform CDD (all staff, paralegal/admin staff, or outsourced)

Principal Compliance Officer

Each option changes who you train, what your workflows look like, and what it costs per matter. This isn't a same-day decision — it sets the operating model.

☐ .....

Decide your cutover model (hard cutover on 1 July or phased pilot on a subset of matters)

Principal Compliance Officer

A hard cutover is simpler but riskier. A phased pilot gives you a lower-stakes test run, at the cost of earlier coordination. Either way, choose deliberately rather than discovering it by default.

☐ .....

PART 1: Common operational readiness

Determine whether a Reporting Group (RG) arrangement applies

Principal

If you have related entities, sharing an AML program and CDD under a RG can simplify compliance significantly — but it requires a deliberate setup decision and AUSTRAC registration of the group.

---

2. Tasks that require external parties

These tasks depend on someone outside your business — a lawyer, an accountant, a vendor, an insurer, or a government portal. They cannot be rushed, and they cannot be delegated away from you entirely.

AUSTRAC registration

Principal Compliance Officer

Registration must be completed directly via AUSTRAC Online before your obligations commence. It is not handled by any compliance platform. Allow time to create the account, identify your designated services correctly, and complete the process.

Update employment contracts and position descriptions for staff with compliance touchpoints

Principal External Lawyer HR

This requires legal input, and existing staff may have questions or concerns. It is not a quick administrative step, particularly if your employment arrangements are varied across roles.

Update Privacy Policy and Privacy Collection Notice (website, intake forms, welcome pack)

Principal External Lawyer

You are now collecting and using identity data for a new regulatory purpose. The Privacy Policy and Collection Notice must accurately reflect this, and the notice has to appear at every point of collection. A lawyer should review it, particularly if you are subject to the Australian Privacy Act.

PMS / practice management system changes

Compliance Officer IT PMS/IT Vendor

Adding AML fields, recording KYC/KYB cost disbursements, updating matter opening checklists and setting trigger points for CDD may require your PMS provider or an IT administrator.

PART 1: Common operational readiness

Accounting software updates for KYC billing

Office Manager Accountant

If you are passing KYC/KYB costs on to clients, your billing system needs to be updated to reflect this correctly. Depending on your software, this may require your accountant or an admin.

☐ .....

Notify your PI insurer of the material operational change and confirm policy response

Principal Insurance Broker

AML compliance is a significant change to your operations. Many policies require notification, and silence can affect future claims. Your broker should also be checking whether your sum insured remains appropriate.

☐ .....

---

3. Technology, data and IT

Tranche 2 introduces new data flows and new sensitivity. Your existing technology stack may not handle these out of the box.

Review and implement 2FA, MFA, SSO and least-privilege access controls

IT PMS/IT Vendor

Identity data needs to sit behind proper access controls. Check with your PMS/CRM and increase your security with 2FA, MFA or SSO. This is highly recommended to reduce your cyber risks.

☐ .....

Confirm data residency and cloud hosting location for all new PII

Compliance Officer IT

Clients and regulators care where their data lives. If your CDD provider stores data offshore, that needs to be disclosed and risk-assessed — and ideally chosen, rather than discovered after the fact.

☐ .....

---

4. Finance, billing and pricing

Once the pricing decision is made (see Section 1), the finance work begins. Each item below is small individually, but the lag adds up if it isn't started early.

Update fee schedules, quotes, proposal templates and scope-of-work documents

Office Manager

If your pricing model is changing, every document that quotes a price needs updating. Don't underestimate how many of these exist — there are usually more than you remember.

☐ .....

Update your chart of accounts to track verification and compliance costs separately

Office Manager Accountant

If verification costs are buried in 'general expenses', you can't manage or recover them properly. Set up the accounts before transactions start flowing.

---

5. The existing client challenge

Most firms focus entirely on new clients. The harder problem is the one already on your books. Every active matter on the day your obligations commence may require CDD — and many of your existing clients have never been asked to provide identity documents in this context.

Audit your current active matters and identify which require CDD

Compliance Officer Office Manager

This is a manual exercise unless your PMS can filter and report by matter status, client type, and transaction type. For most firms, it takes longer than expected.

Prioritise existing clients by risk level for retrospective CDD

Compliance Officer

You may not be able to verify every existing client before the deadline. A risk-based approach requires a documented methodology for prioritisation.

Communicate AML requirements to existing clients

Compliance Officer All staff

A long-standing client who receives an unexpected request for identity documents will often push back. Your team needs a clear, consistent explanation — and the communication needs to go out early enough that you can follow up before the deadline.

Decide what to do with clients who cannot or will not provide CDD

Principal Compliance Officer

This is a real scenario. You need a documented process for declining to continue acting, and your team needs to know what to say. The process should be agreed before it's needed.

PART 1: Common operational readiness

6. Client experience and commercial impact

Tranche 2 changes the front end of every new client relationship. Without deliberate design, that change will introduce friction you didn't intend.

Brief referrers and introducers on new timelines so they set client expectations

Principal BDM

Referrers who promise 'they'll get you sorted today' will create friction with your CDD process. They need a heads-up before the deadline, not after a client complains.

☐ .....

Redesign the new client first-impression journey now that ID collection is the first touchpoint

Compliance Officer Marketing

ID collection becomes one of the first things you ask of a new client. Whether that feels professional or invasive depends entirely on how you frame it and what the experience looks like.

☐ .....

Update public-facing service level commitments

Marketing

If your website promises time guaranteed commitments, make sure you state as soon as CDD is completed.

☐ .....

---

7. Internal documentation and templates

These are largely internal tasks, but each one requires drafting, review, approval, and rollout — and several need decisions to be made first.

Update Appointment to Act / Engagement Letter

Principal Compliance Officer

This document needs to be reviewed, updated, and generally signed off by a principal, and used consistently from a set date. If you have multiple versions across different matter types, each one needs to be updated.

☐ .....

Create client communication scripts for staff

Compliance Officer

Your team may encounter questions or resistance. Have a well-prepared script or FAQ that your team can refer to.

☐ .....

PART 1: Common operational readiness

Update website, welcome packs, email signatures and auto-responders

Principal Marketing

Website changes often require a designer or CMS access. Printed welcome packs need reprinting. Email signatures and auto-responders are easy to overlook, and may contain out of date information.

☐ .....

Prepare a referrer / introducer briefing pack

Marketing BDM

Your referrers are part of your client experience. Consider giving them a one-page explainer about the changes so they can share with clients, rather than letting them improvise their own version.

☐ .....

Update file note standards and matter checklists

Compliance Officer Office Manager

Your team needs to know exactly what to record and where. If this is not documented and communicated before go-live, compliance gaps will appear in audits.

☐ .....

Tipping-off policy and staff awareness

Compliance Officer

Under the AML/CTF Act, disclosing that a Suspicious Matter Report has been filed — even to the subject — is a criminal offence. Staff need to understand this before they are in a position where it matters.

☐ .....

8. Records, privacy and information management

Beyond the Privacy Policy update (Section 2), the back-end of how you hold, find, share and destroy data needs to be made fit for purpose.

Update the firm-wide records retention schedule

Compliance Officer Office Manager

Different categories of data have different retention rules. AML records, matter records, accounting records and HR records each have a clock — they should sit in one schedule, not spread across people's heads.

☐ .....

Review existing outsourcing relationships (offshore admin, VAs, typing) for data implications

Compliance Officer Office Manager

Offshore admins, virtual assistants and typing services may all see client data. Review what each one actually touches, and whether that is still appropriate under your new obligations.

☐ .....

9. Business continuity and resilience

Once you're live, the question is how you cope when something goes wrong. Resilience is built before the incident, not during it.

Establish leave coverage and a key-person risk plan for the AMLCO function

Principal | Compliance Officer

If your AMLCO is on leave and an SMR is required, what happens? A nominated deputy (2IC) with delegated authority — and the systems access to act — needs to be in place before it is tested.

☐ .....

Set a post-go-live lessons-learned cadence

Compliance Officer

Without a scheduled cadence, issues either get fixed reactively or not at all. Lock in the cadence (at least quarterly) before go-live so the first review is already on the calendar.

☐ .....

---

10. Staff training and team readiness

Training is not a once-off tick. It is a program — and setting it up takes more time than delivering it.

Set up initial training for all staff

Compliance Officer | Office Manager

Getting your whole team through training before the deadline requires calendar coordination around existing workloads, client commitments, and leave. For larger teams, this needs to be planned weeks in advance.

☐ .....

Run a team briefing before go-live

Principal | Compliance Officer

Training modules cover the law and the processes. A separate Q&A session with your team is essential for surfacing the practical concerns and edge cases that will actually arise in your practice.

☐ .....

Update your new starter induction process

Compliance Officer | HR

Every person who joins after your obligations commence needs AML training before they can act on a matter. If your induction process is not updated, this will be missed for new starters.

☐ .....

Keep training completion records

Compliance Officer

AUSTRAC expects you to be able to demonstrate that all staff have been trained. Ensure you or your provider maintains training records that are accurate, current, and accessible — not sitting in someone's email inbox.

☐ .....

11. Reporting readiness

Having a compliant AML Program is not the same as being operationally ready to respond to a suspicious matter or lodge a report. These are different things and they need to be tested separately.

Set up AUSTRAC Online access and confirm lodgement capability

Compliance Officer

Your Compliance Officer (and any nominated delegate) needs to have AUSTRAC Online access set up, tested, and ready before they need it. Finding out that access is not working when you are trying to lodge an SMR is not a position you want to be in.

☐ .....

Document your SMR escalation process end-to-end

Compliance Officer

Who identifies it, who makes the decision, who lodges it, within what timeframe, and what gets recorded. This needs to be documented and communicated before the first real escalation occurs.

☐ .....

Set up the Annual Compliance Report calendar reminder and assign ownership

Compliance Officer

The AUSTRAC Annual Compliance Report is a recurring obligation. Assign ownership and set the reminder before go-live, rather than hoping it gets picked up next year.

☐ .....

PART 2: Additional considerations for medium and large firms

/ Who this part is for

The tasks below are typically only material for firms with the headcount, formal governance, or operational complexity to require them.

Sole practitioners and very small firms (1–5 people) can usually absorb these into another role, address them in a lightweight way, or skip them altogether without compromising compliance.

As a rough guide: Medium = 6–50 people, Large = 50+. Adjust to suit your own structure.

1. Project and change management

Build a dated delivery plan working backwards from 1 July, with a hard freeze two weeks before go-live

Compliance Officer | Project Sponsor

Discovering you're three weeks behind in May is recoverable. Discovering it on 24 June is not. A reverse-engineered timeline with a deliberate freeze period forces dry-run testing before clients arrive.

☐ .....

Plan a post-go-live hypercare period of 4–8 weeks with daily issue triage

Compliance Officer | Project Sponsor

Things will go wrong in the first month. Schedule daily triage with a named owner before go-live, rather than scrambling reactively. The team responds far better to a planned hypercare phase than to chaos.

☐ .....

Appoint a project sponsor (partner / director) and a project manager who is not the AMLCO

Managing Partner

Separation of duties matters once headcount supports it. The AMLCO shouldn't also be the person tracking project actions — different responsibilities, different cadence.

☐ .....

PART 2: Additional considerations for medium and large firms

Establish a cross-functional steering group (Finance, IT, HR, Marketing, Operations)

Project Sponsor

Cross-functional decisions need cross-functional ownership. A monthly steering forum surfaces blockers earlier than a single project manager can.

☐ .....

---

2. Technology, data and IT

Scope and schedule integration work between CDD, PMS, accounting and document storage

IT PMS/IT Vendor

Integration projects are where Tranche 2 timelines go to die. Even when each system has an API, getting them to talk in a way your team can rely on takes weeks of scope, build and test.

☐ .....

Update backup, disaster recovery and cyber incident response plans for the new data footprint

IT Compliance Officer

Your existing plans were written for your existing data. Now you have new categories of PII, and the response to a breach is materially different — particularly the notification obligations.

☐ .....

Automate retention timers and deletion workflows

IT Compliance Officer

Small firms can manage retention manually if volumes are low. Medium and large firms cannot — automation is the only way to keep deletion timely, consistent and auditable.

☐ .....

---

3. Finance, billing and pricing

Forecast the revenue timing impact of extended onboarding (instruction to first invoice lag)

Office Manager Finance Manager

Verification adds time between instruction and first invoice. If your cash flow assumes a 2-day turnaround and it's now 5–7 days, that is a real working-capital question worth modelling.

☐ .....

Update WIP and lock-up reporting to reflect the longer onboarding curve

Office Manager Finance Manager

If you report WIP and lock-up to a board or partnership, those reports need to reflect the longer instruction-to-bill cycle — otherwise you'll be explaining movement that isn't really there.

☐ .....

PART 2: Additional considerations for medium and large firms

4. HR and workforce

Design the AMLCO role (full vs part time), deputy AMLCO, and client onboarding coordinator

Principal HR

Once you have the headcount, separating the AMLCO from the people doing day-to-day CDD makes both roles work better. Role design matters before recruitment starts.

☐ .....

Start AMLCO recruitment early if hiring externally

Principal HR

The Tranche 2 AMLCO market is tight. If you are hiring externally, expect a long lead time and competitive pricing — and start the search well before you think you need to.

☐ .....

Review incentive and bonus structures so speed-to-bill does not conflict with CDD discipline

Principal HR

If staff are paid on speed of billing, the CDD process is something they'll try to short-cut. Realign incentives before the conflict shows up in audit findings.

☐ .....

Plan staff wellbeing and change-fatigue support through the transition

HR

Material operational change is tiring. Plan for it explicitly — particularly for client-facing staff who will absorb most of the friction.

☐ .....

Update the new-hire induction and onboarding process

HR Compliance Officer

Every new starter after 1 July needs AML training before they can act on a matter. Your standard induction should already cover this — don't leave it for HR to figure out per-hire.

☐ .....

---

5. Client experience

Design a VIP / top-client handling approach so they are not treated like a walk-in

Principal BDM

Your top-tier clients should not feel like walk-ins when they encounter your new process. A deliberate VIP handling approach — without compromising CDD — is worth designing.

☐ .....

PART 2: Additional considerations for medium and large firms

Complete a Privacy Impact Assessment for the chosen CDD provider

Compliance Officer

A formal PIA documents how privacy risks have been considered and mitigated. Larger firms are expected to do this; smaller firms can use a lightweight template.

☐ .....

6. Insurance and risk

Review cyber insurance cover, sub-limits and premium for increased PII volume

Principal Insurance Broker

You are now processing considerably more PII. The policy's sub-limits — for breach response, regulatory fines, and third-party claims — should be tested against this new exposure. Expect some premium movement.

☐ .....

Add operational AML risks to the enterprise risk register with owner and mitigation

Compliance Officer

If you maintain a risk register, AML operational risks belong on it — with named owners and tested mitigations, not just descriptions.

☐ .....

Review D&O implications for the governing body under the new personal accountability regime

Board Insurance Broker

Directors and officers carry personal accountability under the AML/CTF Act. D&O cover should be tested against this expanded exposure.

☐ .....

7. Communications and marketing

Build an internal comms plan (all-staff, partner, client-facing staff briefings)

Compliance Officer Marketing

Larger firms need a deliberate internal comms cadence — what is said, when, and by whom — rather than relying on word-of-mouth.

☐ .....

Prepare a holding statement for public complaints or reviews during transition

Principal Marketing

Public complaints land on Google, social media and review sites. A pre-prepared holding statement means you respond in hours, not days.

☐ .....

PART 2: Additional considerations for medium and large firms

Update proposal and tender documents for RFP responses on AML posture

Compliance Officer BDM

Corporate and government tenders are likely to now ask about AML posture. If you bid for that kind of work, your standard response needs an AML section ready to go.

☐ .....

8. Business continuity

Document AMLCO unavailability delegation and sign-off authority

Principal Compliance Officer

Firms with larger teams should ensure the delegation is documented internally — including the systems access that goes with it.

☐ .....

/ What this means for your timeline

If you start these tasks in the final 4–6 weeks before the deadline, you run risk they won't be completable in time.

Employment contract updates and privacy policy review both require external parties and typically take 3–6 weeks each.

PMS changes, CDD integration work and insurer notifications all involve external parties — and as vendors face similar requests from many Tranche 2 firms simultaneously, timelines stretch in mid-2026.

The existing client audit and communication is proportional to practice size — for a firm with 200+ active matters, it is a multi-week undertaking. Training completion for 5–15 people around existing workloads could take 1–2 weeks of lead time.

easyAML is designed to be fast to implement. The bottleneck is almost never the platform. It is the business processes around it.

** Principal - the partner, director, CEO, licensee or principal of the firm with authority to make the relevant decision. Title varies by sector and business structure.*

easyAML

Ready to get started?

Visit easyAML.com

easyAML handles the compliance engine. Start the operational work now, and you'll be in front of your obligations — not racing to catch up.