



PROGRAMME MANAGEMENT

CASESTUDY

Small bank, big compliance:
Mastering a tsunami with
precision and pace.

Background

A regional community bank in Australia (“the Client”) serves 55 000 retail and SME customers through 19 branches and a mobile-first app. With assets of only AUD 2.7 billion and a lean risk staff of seven, the bank suddenly faced a regulatory tsunami:

- APRA CPS 230 (go-live 1 Jul 2025) merging op-risk, continuity and third-party oversight.
- FAR (effective 15 Mar 2024) extending personal liability to directors and executives.
- ASIC RG 277 mandating data-driven, customer-centred remediation.
- Draft AML/CTF reform replacing prescriptive rules with a risk-based regime.
- National Anti-Scam “Scam-Safe Accord” imposing real-time scam detection and mandatory reimbursements.

Introduction

Enigma advised on a 12 month engagement that:

- Integrated five new rule-sets into one obligation library and control framework.
- Built an Agile Remediation Office (ARO) that could evidence 30-day action plans to both APRA and ASIC.
- Embedded data-driven harm discovery and customer-first refund engines.
- Gave the board real-time dashboards to track personal Financial Accountability Regime (FAR) accountabilities and CPS 230 outage tolerances.

Importantly with four concurrent supervisors (APRA, ASIC, AUSTRAC, ACCC) and limited budget, the board feared “death-by-remediation” and hence asked for a single, sustainable compliance programme.

Challenges Faced

Challenge	Impact on a Small Bank
Reg-change overload – 220 new obligations across five regulators	Risk team capacity exceeded; conflicting deadlines
Personal liability under FAR	Directors demanded daily line-of-sight on open issues
Siloed tooling – separate sheets for op-risk, AML, scam disputes	Duplicate evidence, audit gaps
Legacy incident process – manual emails, no outage metrics	Couldn't prove CPS 230 “tolerable outage” thresholds
Scam reimbursement exposure	Forecast payout 3× fraud-loss budget



PROGRAMME MANAGEMENT

CASESTUDY

Small bank, big compliance:
Mastering a tsunami with
precision and pace.

Results and Impact

- 100% regulatory obligations mapped; duplicate controls cut by 37%.
- First CPS 230 self-assessment submitted three months early; APRA issued no material findings.
- FAR accountability map & heat-dash live in board packs; action-plan cycle-time fell from 90 to 28 days.
- Consumer remediation throughput ↑ 65%; AUD 2.1m refunds processed with zero ASIC escalation.
- Scam-loss ratio -40% after deploying real-time mule-account and confirmation-of-payee checks.
- Audit prep effort -50% thanks to automated evidence vault—praised by external auditors.

Solutions Implemented

a. Unified Regulatory Obligation Library

- Merged CPS 230, FAR, RG 277, draft AML/CTF bill and Scam-Safe Accord into 142 atomic obligations tagged to owners, due-dates and evidence types.
- Policy-as-Code Git repo pushes control text straight into Confluence and Jira.

b. Agile Remediation Office (ARO)

- Two-week sprints triage breaches, assign FAR accountable exec, and auto-generate 30-day remediation plans.
- Jira workflows feed a “Reg Radar” dashboard for APRA/ASIC status calls.

c. CPS 230 Resilience Suite

- Defined impact tolerances (payments ≤ 4 h; core banking ≤ 8 h).
- Built an incident-clock bot that starts the SLA timer, surfaces KRI breaches, and triggers board SMS alerts.

d. RG 277 Customer-Centred Remediation Engine

- Python rules calculate refund plus interest; generates customer letters and public progress metrics.
- Data-link to core ledger ensures proactive harm discovery instead of complaint-led fixes.

e. Risk-Based AML/CTF Upgrade

- Re-segmented customers with a Random-Forest risk score; tuned TM scenarios to cut false positives 45%.
- Beneficial-ownership checker calls ASIC, OFAC and ABR APIs in one pass.

f. Scam-Safe Controls

- Real-time AI mule-account scoring on outbound payments.
- Confirmation-of-payee API integrated; positive-pay mismatch auto-holds.
- Dedicated compensation queue to meet 48-hour reimbursement pledge.

g. FAR Accountability & Culture

- RACI heat-map links each obligation to a single accountable person plus two deputies.
- Quarterly “accountability clinics” rehearse board testimony scenarios

Conclusion

By turning five disparate regulatory shocks into one cohesive, sprint-driven change programme, the community bank moved from chronic remediation fire-drills to audit-ready, regulator-praised compliance—all without expanding headcount. The board now steers with a real-time view of operational resilience, customer harm and personal FAR liabilities, proving that scale is no excuse for poor governance.