Strategies to enhance fraud prevention outcomes

Lata McNulty
Head of Business Risk and Compliance
Member Engagement, Education and Advice

6 May 2026

Problem statement

Australians reported $2.18 billion lost due to fraud and scams in 2025 (7.8% increase)*

- ❑ Combined losses reported to Scamwatch, ReportCyber, IDCARE, AFCX and ASIC
- ❑ Over the last 5 years over $11 billion

Top 5 scam types by losses (combined data)

Year	Investment	Payment redirection	Romance	Phishing	Remote access	Total loss %
2025	⇩ $837.7m	⇧ $166.8m	⇩ $139.9m	⇧ $97.6m	⇩ $69.9m	⇩ 60%
2024	$945.0m	$152.6m	$156.8m	$84.5m	$106.0m	71%

Highlights the complex and adaptive nature of fraud and scams

* National Anti-Scam Centre's 'Targeting Scams Report' released on 30 March 2026

Redefining fraud control

✓ Evolving fraud risks

Increasingly driven by digital channels, AI-enabled social engineering, and organised fraud networks challenging traditional controls.

✓ Demand for measurable outcomes

Clients, Executives and Regulators expect fraud controls to demonstrate loss reduction, faster detection, and efficient resource use with clear metrics.

✓ Cost of Ineffective controls

Manual reviews and high false positives increase costs and customer friction while missing significant fraud cases.

✓ Redefining fraud control success

Success means faster detection of relevant fraud events, preventing losses, and influencing fraudster behaviour beyond just compliance

The case for change

Retrospective Compliance attestations

Compliance looks backward, not assessing current or emerging risk landscape that may impact control effectiveness.

Audit and Assurance alignment and complexity

Focusing on audits over innovation may lead to reduced clarity on the pace and velocity of risks. Find the right balance.

Disconnect on Risk Impact

Compliance statements often fail to convey true financial, reputational, and customer harm risks to leaders.

Shift to Outcome-Based Approach

Evaluating controls by real use cases and scenarios and continuous measurement builds effective fraud resilience.

Strengthening fraud resiliency

Speed in fraud Response

Early detection and rapid intervention reduce fraud losses and prevent cascading effects across payment systems.

Deterrence through controls

Effective controls, knowing when to add friction to client journey, can reduce repeat fraud attacks by influencing fraudster behavior and shifting attack patterns.

Ownership and accountability

Clear responsibility for fraud risks across business units ensures early integration in product design and risk management.

Measurable and adaptive resilience

Balancing prevention, detection, and compliance creates a shared performance language for continuous fraud improvement.

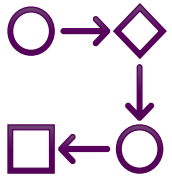
Utilise fraud use cases – test and learn

Generic vs Scenario-based controls

Traditional controls are generic and may lack clear linkage to specific fraud scenarios, limiting effectiveness assessment.

Scenario-based control mapping

Mapping controls to detailed fraud scenarios clarifies their role as preventative, detective, or responsive measures.

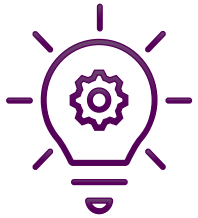


Performance assessment

Scenario linkage enables meaningful evaluation of control timing, alert actionability, and response effectiveness.

Communication and prioritisation

Scenario-based linkage improves understanding and prioritises investment in high-impact fraud controls.



Detection data for performance metrics

Defined metrics should align with business outcomes to reflect fraud detection performance

- ✓ **Trend analysis:** Tracking trends over time reveals improvements, fraudster adaptations, and emerging risks beyond single data points.
- ✓ **Contextual data segmentation:** Segmenting metrics by channel, product, or fraud type uncovers specific issues masked by aggregated data.
- ✓ **Strategic decision support:** Meaningful metrics provide actionable insights supporting prioritisation, accountability, and investment decisions.

Design reporting that drives decisions

Focus on key metrics: Executive dashboards highlight essential fraud indicators, avoiding overwhelming operational details for clarity.

Response-time metrics: Measuring time from alert to action links fraud detection to impact and highlights accountability gaps.

Contextual narratives: Dashboards provide narrative context explaining metric changes, necessary actions, and decision requirements.

Trend visualisation: Visualising trends over time helps executives quickly understand risk progression and emerging threats.

Align reporting to business outcomes

Accountability and action: Assigning metric ownership to leaders provides clear accountability and fosters shared responsibility to integrate fraud management outcomes into business goals.

Operational control maturity: Using control maturity and response metrics in discussions promotes active management and continuous improvement.

Benchmarking fraud metrics:

- ✓ Benchmarking against peers provides context to evaluate performance effectively.
- ✓ Highlights both performance gaps and good practice to inform risk management strategies.
- ✓ Ensure peer organisations in benchmarking is meaningful

Demonstrating ROI & sustainable funding

Quantifying avoided losses

- ✓ Avoided loss estimates use historical data and clear methodology to show impact of controls.

Efficiency gains and cost savings

- ✓ Translate efficiency metrics like fewer manual reviews & lower false positives to cost savings.

Aligning funding with strategy

- ✓ Funding cases tied to strategic goals like digital growth and customer trust.

Shift the focus from cost to value

- ✓ Consistent ROI communication reframes fraud control as value contributor ‘accounts protected’

Thank you.

aware super