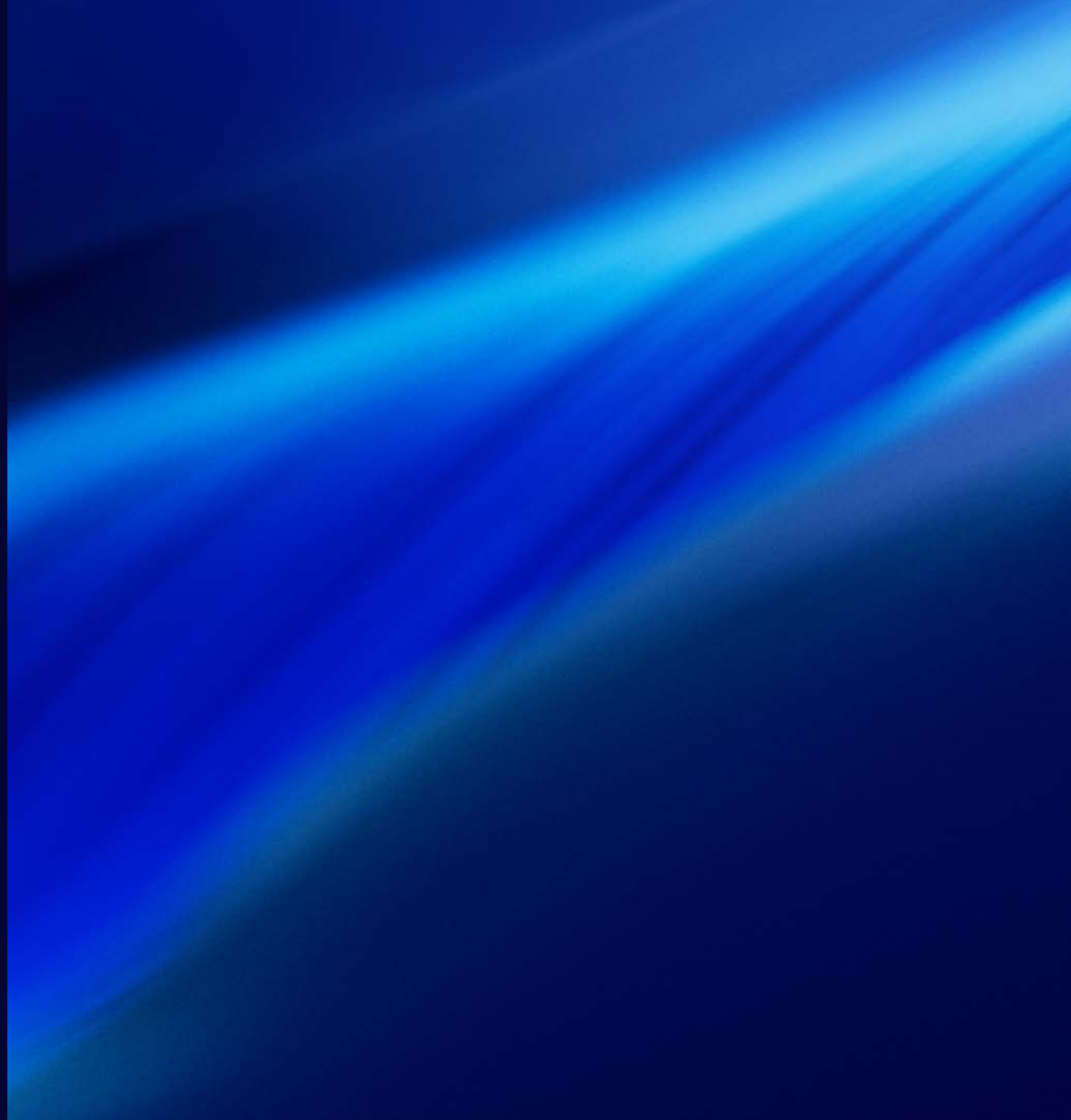
WHITEPAPER

Digital Trust Agenda for Wealth & Super · Part 1 of 5

The Quiet Reordering of Trust

Why the next decade of Australian wealth and superannuation will be defined by the regulatory and trust agenda — not by returns alone.

Chetna Bedi
General Manager, Wealth & Superannuation



THE ARGUMENT AT A GLANCE

Trust must now be proven, not asserted

For trustees, that means demonstrating evidence across four dimensions — identity, data, operations and supply-chain assurance. This paper sets the strategic context: how the industry arrived here, what is changing now, and what boards should weigh for the decade ahead. The map below is the whole argument on one page.

THE PRESENT—SIX THEMES

01	Compliance posture ≠ operational reality. Artefacts exist; tested capability does not yet.
02	Provider concentration is visible to APRA. The MSP register exposed the system pattern.
03	Identity has moved to the centre. Credential-led attack is now dominant.
04	Member protection is its own subject. ASIC has made it an enforcement priority.
05	Personal accountability changed the room. FAR made security a named-person risk.
06	The agenda is now multi-regulator. APRA, ASIC, ATO, Home Affairs, OAIC.

THE FUTURE—SIX FORCES

01	The 1 July 2026 compression. Five mandates land in one quarter.
02	From compliance to digital trust. Trust becomes an acquisition asset.
03	Active rebalancing of concentration. Market share shifts over 3–5 years.
04	AI moves to a live supervisory issue. Four planes of AI risk, plus post-quantum.
05	The personalisation of accountability. The 2030 accountable person differs.
06	One integrated, evidence-based view. One evidence base for every regulator.

Compliance documentation is no longer the deliverable. Tested capability is.

THE THROUGH-LINE OF THIS PAPER

FOREWORD

Risk management used to be a board paper. Now it is the board agenda.

For most of the last twenty years, the conversation in our industry was dominated by investment performance, scale and consolidation. Funds grew into national institutions; members became beneficiaries of the largest pool of retirement capital in the OECD outside North America. The strategic question was how to deliver competitive net returns at increasing scale. Operational resilience and information security mattered, but they were back-office disciplines.

That world is gone. What has replaced it is more demanding, and arguably more interesting. The contest for member trust — measured not in marketing surveys but in regulatory posture, supervisory standing, member protection and the durability of the operating environment members never see — has moved from the periphery of the strategic agenda to its centre.

APRA has rewritten the operational-risk framework through CPS 230 and, with the 30 April 2026 final amendments confirmed, set the contractual reset at 1 July 2026. Cyber and information security have shifted to a board, FAR-accountable-person and member-trust conversation through CPS 234 and the events of April 2025. APRA's 30 April 2026 letter put AI risk on the same trajectory; ASIC's 8 May 2026 open letter framed cyber resilience as a core licensing obligation; ASIC's February 2026 anti-scam review found super funds behind the major banks on member-facing protections. Payday Super and SuperStream 3.0, also from 1 July 2026, compress the operating cycle.

Underneath all of it: trust is now a measurable strategic asset, and the infrastructure that produces it is a board-level concern. This paper is not about compliance. It articulates why the regulatory and trust agenda has become the defining strategic conversation for the next ten years, what is changing beneath the standards, and what trustees might consider. I write as a practitioner with two decades inside the industry, working alongside NRI's cyber and digital trust specialists. What follows is what I hear, what I observe, and where I think the industry is going.

Chetna Bedi
General Manager, Wealth & Superannuation

SECTION 01 · THE PAST

How the trust agenda emerged

Australian superannuation was built on devolution. Trustees outsourced administration, custody, investment management, insurance and increasingly technology. It was rational: specialisation produced efficiency, and efficiency produced lower fees and better net returns.

By the late 2010s, large funds operated with many material service providers — contributions, claims, unit pricing. The trustee held the licence and the fiduciary duty; almost everything else lived elsewhere.

The framework grew piece by piece over twenty years — SPS 231, SPS 232, SPS 220, and CPS 234 (2019) — each added without redesigning the whole. Operational risk migrated outside the trustee while accountability stayed inside it. The asymmetry was tolerable while incidents were rare. Then three pressures changed the calculus.

PRESSURE 01 · SCALE

Scale created systemic significance

As FUM passed $4 trillion, funds and their providers became too important to fail. The same administrators, custodians and cloud providers underpin many funds — a single failure could affect millions at once. The TelstraSuper transfer into Aware Super (30 April 2026; ~1.3m members, >$235bn) shows the consolidation trajectory.

PRESSURE 02 · THREAT

The threat landscape changed

Optus and Medibank (2022) reset expectations of institutional durability. Then came credential stuffing: in April 2025 several of the largest funds were hit in a coordinated wave, with 20,000+ accounts accessed. AustralianSuper confirmed 10 members lost a combined A$750,000, fully reimbursed — contained in dollars, damaging for sector trust.

PRESSURE 03 · REDESIGN

The architecture was redesigned

CPS 230 (final 2023; effect 1 July 2025; amendments 30 April 2026, commencing 1 July 2026) consolidated five standards into one framework and changed the paradigm: an end-to-end view of critical operations, board-approved tolerances, scenario testing, and an MSP register making concentration visible to APRA. Compliance documentation is no longer the deliverable — tested capability is.

The current state of digital trust

Most funds have stood up CPS 230 programs, filed an MSP register, mapped critical operations, set tolerances, responded to APRA's June 2025 letter and named a FAR accountable person. The artefacts exist. Beneath them, six themes define the moment.

01

Compliance posture and operational reality have not yet converged

Setting tolerances in a workshop is one thing; testing them under realistic disruption and finding they hold is another. The next two years are about moving from compliance posture to operational truth — controls that do what they say, tolerances that bite, evidence that survives scrutiny. Most funds know this; few have a path through it without external capability they do not hold.

02

Service-provider concentration is no longer hidden from APRA

The MSP register has given APRA a clearer cross-sector view of dependency than the industry itself has had. A handful of administrators, custodians and cloud providers underpin a large share of the system. What to do about that concentration — tolerate, diversify, or build alternatives — is among the largest strategic questions trustees face this decade, and one no single fund can solve alone.

03

Identity has moved to the centre, but the industry has not caught up

For a generation the threat model was a perimeter event. April 2025 made that secondary. The dominant threat is credential-led — reused credentials plus an architecture that fails to stop them at the front door. Passwords-plus-SMS are inadequate, MFA is the floor, phishing-resistant authentication is the trajectory, and recovery flows are the most exploited weakness. The member experience tension can no longer be the excuse.

04

Member protection is a regulatory subject in its own right

ASIC's February 2026 review across 47 funds was a turning point: funds scored 40–60% of criteria against 80%+ for the major banks, with ~A$22m in super-related scam losses in 2025. ASIC views the gap as inadequate and has made member-services failures a 2026 enforcement priority. The trust agenda is now also member communications, reporting pathways, fraud response and victim support.

05

Personal accountability has changed the conversation

The Financial Accountability Regime, in force for RSE licensees since March 2025, has had an effect the industry under-anticipated. When APRA's June 2025 letter required boards to name the FAR accountable person for information security, it turned security from a function-level matter into a personal one. That accountability is proving a powerful catalyst for capability investment.

06

Regulatory expectations now extend beyond APRA

Tolerance for known, unremediated weaknesses has declined, and the perimeter has widened. APRA's June 2025 and April 2026 letters were unusually direct; ASIC's 8 May 2026 open letter (Commissioner Simone Constant) made cyber resilience a licensing obligation and told boards to evidence, not assert. Boards that noted a letter without commissioning uplift now risk a finding of inadequate response — independent of any incident.

INTERLUDE · FROM TOKYO

A view from Japan

This trajectory is not unique to Australia. NRI's colleagues in Tokyo have watched Japan's Financial Services Agency drive a near-identical conversation across banks, insurers and pension institutions for several years — a forward view of where parts of this agenda lead.

NRI also operates one of Japan's largest defined contribution pension administration platforms, handling record-keeping and administration at scale. Running critical retirement infrastructure — not only advising on it — has taught us where the real difficulty lies: not the technology, but achieving management visibility over critical operations and dependencies before they surface as customer or regulatory problems.

THE MIZUHO LESSON

Resilience is a governance capability, not a technology one

After Mizuho Bank suffered eight system failures across 2021, the FSA's business improvement order did not land on the technology. It landed on the board. The finding: management had not treated IT and operational risk as a substantive governance matter, had been insufficiently sensitive to customer impact, and accountability had not kept pace with the operating environment. A chief executive ultimately stepped down. The conclusion APRA is reaching through CPS 230, CPS 234 and FAR is the one the FSA reached the hard way.

Fraud is a customer-trust capability

As fraud, phishing and account takeover grew in Japan, the institutions that pulled ahead were not those with the best detection engines, but those that treated fraud as a customer-trust capability — where detection speed, response coordination and communication mattered as much as the technology. That is precisely the distinction ASIC is now drawing: the differentiator is not only whether fraud is detected, but how fast and how well the institution responds to the member.

What the next decade will reward

Certain trajectories are clear enough to plan against. Six forces will reshape Australian wealth and super where they intersect with the regulatory and trust agenda — the first already dated.

01

The 1 July 2026 compression is now concrete

In one quarter: Payday Super starts; SuperStream 3.0 commences; contributions must be received, allocated or returned within three business days; the CPS 230 contractual transition lands; and APRA's final targeted CPS 230 amendments commence. APRA and the ATO's 25 March 2026 joint letter confirmed contribution processing as a critical operation and warned that many licensees were not on track for SuperStream 3.0. Treat it as one integrated operating-model redesign, not separate projects.

02

The shift from compliance to digital trust

Compliance is the floor; digital trust the ceiling, and the gap becomes the contest. Funds that treat trust as a measurable capability — metrics, board reporting, transparency — will outperform. ASIC's Key Issues Outlook 2026 made the stakes plain: nearly three million Australians become eligible to access their super this decade, and >A$750bn moves to retirement. The funds that earn trust keep those balances.

03

The active rebalancing of provider concentration

The major providers will not lose their position, but active rebalancing is coming. APRA has the data and will use it — through supervisory dialogue, capital expectations, licensing conditions, and ultimately its CPS 230 powers to require concentration to be managed. Some funds diversify proactively; others will be required to. Market share shifts visibly over three to five years.

04

AI has moved from horizon to live supervisory issue

Post-quantum: adversaries harvest encrypted data now, betting on future decryption — for multi-decade member data, cryptographic inventory is a near-term obligation. AI: APRA's 30 April 2026 letter found governance and resilience not keeping pace, flagging gaps in identity for non-human actors, supplier concentration in AI tooling, and frontier models that accelerate attack. Trustees must address AI the fund adopts, AI in providers, AI used by attackers, and board literacy across all three.

05

The personalisation of accountability

FAR is the leading edge of a broader move toward personal accountability for institutional outcomes. Expect the regime to deepen: courts and regulators using it more, boards demanding granular accountability statements, frequent attestations, and tighter linkage to remuneration under CPS 511. The FAR accountable person of 2030 operates to a different standard than the one of 2025.

06

The multi-regulator trust agenda

Through the 2010s, trust was an APRA conversation. No longer. APRA owns prudential resilience; ASIC conduct, member protection and licensing; the ATO contribution integrity; Home Affairs and the National Cyber Security Coordinator the Cyber Security Act 2024 (including ransomware reporting from May 2025); the OAIC privacy. The funds that fare best build one integrated, evidence-based view of trust that satisfies every audience from a single evidence base.

FOR THE BOARDROOM

What boards and executives should consider

Six moves separate funds using this moment to build durable capability from those producing a clean audit and little else. This is the page to table.

01 Treat resilience and digital trust as one capability

CPS 230 and CPS 234 share assets, critical operations, providers, incident response and the board governance trail. Run as one capability — shared rhythm, unified board reporting — they do more with the same resources and produce a more defensible posture. The same logic now extends to AI risk and member protection.

02 Recalibrate authentication as a strategic decision

Authentication is in the critical path of every high-risk transaction, and pressure rises with Payday Super. SMS one-time codes are economically unsustainable at coming volumes and structurally weak. Phishing-resistant authentication is the production-grade standard. The question is how to migrate without breaking the member experience — a board conversation about trust architecture, not an IT project.

03 Test what you have designed — and be honest

The key discipline in CPS 230 is scenario testing; in CPS 234, control validation. Both demand the gap between design and reality be surfaced, not concealed. Funds that recalibrate tolerances to pass, or close incidents at the symptom, accumulate risk that surfaces through supervision, audit or the next incident. Governance should rest on evidence — not assurances.

04 Engage actively with the supply chain

Material providers are now inside the regulatory perimeter. The 1 July 2026 contractual transition is a once-in-a-generation chance to reset terms with administrators, custodians, cloud and AI vendors — for capability, not just compliance. APRA's April 2026 AI letter extends this to fourth-party dependencies. Approached as a strategic negotiation, with leverage, it yields materially more.

05 Equip the FAR accountable persons

Accountability is a catalyst only with authority, resources and information. Ask directly: does our FAR accountable person have a real-time view of the posture they are accountable for? The authority to require remediation? Access to advice before signing attestations? Is the same true for member protection and fraud? If any answer is no, the regime is not yet operating as designed.

06 Invest in capability that compounds

Regulatory programs are time-boxed; capability is durable. Invest in what outlasts the moment: a live information- asset register powering CPS 234 and CPS 230; authentication built for Payday Super volumes; security operations that detect credential stuffing and account takeover in time; a third-party assurance model; a member-protection capability. Time-boxed compliance buys a clean audit; compounding capability buys both.

A FINAL REFLECTION

The question is no longer whether trust matters. It is whether the operating model can prove it.

The conversation about what defines a great Australian super fund is shifting away from net returns alone, toward a broader proposition: returns, plus operational resilience, plus information security, plus AI governance, plus member protection, plus the demonstrable ability to keep members' trust through whatever the next decade brings.

This is not a softer agenda — it is a harder one. Net returns are measurable; trust is harder. Performance is a quarterly conversation; resilience, security and member protection are continuous. A great investment team can be built; a great digital-trust capability requires sustained investment across people, technology, partnerships and governance over years. Funds that started early are already pulling away.

The role of advisors is to help trustees navigate a more complex environment than the one most of us trained in — bringing sector depth, delivery capability and an honest external perspective to a conversation now held at the boardroom level. Australian wealth and super deserves to be led with the seriousness that responsibility demands. I would welcome the conversation continuing.

NEXT IN THIS SERIES

02 · Identity Trust
Authentication and access in a credential-led era.

03 · Data Trust
Protecting member information across its lifecycle.

04 · Operational Trust
Detection, response and recovery as tested capability.

05 · Supply-chain Trust
Assuring providers and fourth parties before 1 July 2026.

Primary sources, current as at publication

APRA & ATO, Payday Super Readiness, joint letter to RSE licensees, 25 March 2026.
APRA, Final targeted amendments to CPS 230, CPG 230 and the MSP Register Template, 30 April 2026 (commencement 1 July 2026).
APRA, Letter to Industry on Artificial Intelligence, 30 April 2026.
APRA, Letter to RSE licensees on information security obligations and critical authentication controls, 10 June 2025.
APRA, Corporate Plan 2025–26.
ASIC, Open letter to AFS licensees on AI-accelerated cyber threats (Commissioner Simone Constant), 8 May 2026.
ASIC, Media release 26-014MR, anti-scam and fraud protections, 4 February 2026.
ASIC, Enforcement Priorities 2026 and Key Issues Outlook 2026.
Australian Government, Cyber Security Act 2024 and Cyber Security (Ransomware Payment Reporting) Rules 2025.
Financial Accountability Regime, in force for RSE licensees from March 2025.
Japan FSA, business improvement order re Mizuho Bank system failures, 2021.
Industry reporting on the April 2025 credential-stuffing attacks against multiple RSE licensees, including AustralianSuper's confirmed loss.

This piece reflects the personal views of the author. It draws on published materials from APRA, ASIC, the ATO and other primary sources. It is provided for general information and does not constitute legal, financial or regulatory advice.


NRI
WWW.NRI-ANZ.COM