Super Consumers Australia

Phone 02 9577 3333
Email enquiries@superconsumers.com.au
Website www.superconsumers.com.au
57 Carrington Road,
Marrickville NSW 2204
ACN 163 636 566 | **ABN** 34 163 636 566

17 June 2025

Policy and Advice Division
Australian Prudential Regulation Authority
GPO Box 9836
Sydney, NSW 2001

Via email: PolicyDevelopment@apra.gov.au

Attention: Ian Beckett, General Manager, Policy Development

Dear Mr. Beckett,

RE: APRA Governance Review - Discussion Paper

Super Consumers Australia welcomes the opportunity to contribute to this consultation. We strongly support APRA's proposed changes to the governance framework for superannuation trustee boards. The proposals are consistent with what should already be standard practice for boards who are responsible for managing approximately $3 trillion of Australians' hard-earned retirement savings. The fact that major governance failures impacting millions of members are still regularly occurring is evidence that these reforms are necessary and that uplift will not occur without APRA's intervention.

While we support all of the proposals in the Discussion Paper related to superannuation trustees, this submission primarily focuses on Proposal 1 - Skills and capabilities. APRA's proposal should be pretty familiar to any Australian who has ever worked: job descriptions, performance evaluations and training/recruitment. If Australians expect these things of the café on the corner, surely it's not too much to ask of a billion dollar super fund.

The importance of strong governance

Strong governance is fundamental to the effective operation of any superannuation fund. Superannuation trustee directors hold our futures in their hands. It is reasonable to expect they would have - individually and collectively - the appropriate skills to do their jobs - just like any other Australian. Being a director of such a systemically important Australian institution is a privilege - not a right - and directors must continually earn that privilege in order for the superannuation system to maintain the public's trust.

We agree that trustee boards have a central role to play in ensuring good governance as they are responsible for setting the strategic direction, culture and risk appetite of their funds, and for holding management to account.

Cyber security failures

In April 2025, at least five superannuation funds (Australian Super, Australian Retirement Trust, Hostplus, Insignia and Rest) were the subject of credential stuffing attacks that resulted in losses to members of over $750,000 (AFR, 27 May 2025). These attacks were not unprecedented - indeed, they should have been *expected* given the frequency of cyber incidents and outages in the past few years. However, if reading the news were not sufficient to alert trustees to the risks:

- following consultation, APRA introduced CPS234 Information Security and CPG 234 Information Security effective from 2019;
- ASIC successfully took enforcement action in 2022 against RI Advice (owned by Insignia Financial) for failing to have adequate risk management systems to manage its cybersecurity risks;
- APRA specifically told trustees about the importance of multi-factor authentication in 2023;
- APRA undertook an IT Resilience Review in April 2024;
- APRA wrote to all its regulated entities in August 2024 outlining cyber resilience weaknesses it had identified;
- ASIC wrote to all trustees in January 2025 outlining its observations of poor scams and fraud mitigation practices.

It is no surprise then that not one of the directors of the five trustees involved in the attacks has any cybersecurity or information technology (IT) expertise according to the fund's website disclosures.

Job descriptions

We support the proposal to require trustees to identify and document the skills and capabilities necessary for the board as a whole and each director individually. Particularly given the fact that regulators have been warning trustees about cyber risk for over six years now, it is a reasonable expectation that trustees would have turned their mind to what skills and capabilities their boards need to have (individually and collectively) in relation to cybersecurity, among other things, and to document them. Members can't wait another six years.

Aside from assisting trustees to ensure that all required skills and capabilities have been acquired, documentation will also assist individual directors to understand their responsibilities (which should assist them to comply with their obligations under the FInancial Accountability Regime).

Performance evaluations

Just like any barista, boards and board members should be evaluated periodically against the needs of the business (proposal 1) as well as their own performance (proposal 5). While we support the proposal to require qualified independent third-party performance assessments every three years, we suggest that individual directors should still be evaluated in some form at least annually in order to ensure that they are meeting basic expectations, such as training and development, compliance and ethics. Where evaluations demonstrate that skills or capabilities are lacking, or performance falls below the expected standard, trustees should be required to develop a documented plan for addressing any gaps or underperformance, and to report progress on the plan at board meetings, or to APRA at its request.

Training and recruitment

In our view, APRA's proposal gives trustees a lot of flexibility in how they fill skills gaps. For example, while it is not reasonable or necessary to expect that every director would have expertise related to cybersecurity, it is reasonable to expect that someone on each board would have enough knowledge of IT to understand the significant risks that exist and to ensure that the trustee prioritises managing them. This knowledge could be acquired through recruitment, training or the retention of expertise: what is important is that someone on the board has the knowledge to ask the right questions and the confidence to hold management to account for how the risk is being managed. The proposal supports this outcome.

Implementation timing

While we appreciate that APRA is undertaking a robust consultation process in relation to the proposed changes, and that the changes to the impacted prudential standards and guidance themselves will take additional time, we encourage APRA to make those changes effective as soon as practicable. The proposals are simple and straightforward - things trustees should already be doing. Trustees should not require significant implementation time and every day delayed puts members at risk.

Please feel free to contact me if you have any questions or would like to discuss this submission further.

Yours truly,

Jessica Spence, Director of Advocacy (Policy)
Super Consumers Australia