18 June 2025

General Manager
Policy Development
Policy and Advice Division
APRA Prudential Regulation Authority

To the General Manager,

Thank you for the opportunity to comment on the APRA Governance Review discussion paper and for allowing us additional time to provide this submission. We appreciate the constructive working relationship we have with APRA and look forward to our continued collaboration together in the pursuit of better governance in the public interest.

We commend your initiative in this area to improve the core governance within standards applicable to APRA regulated entities. We note the following standards are under review:

Scope	Objectives	Desired outcome
CPS 510 Governance SPS 510 Governance CPS 520 Fit and Proper SPS 520 Fit and Proper SPS 521 Conflicts of Interest Associated prudential practice guides	Update minimum governance standards. Apply proportionality and reduce compliance burden where possible. Strengthen APRA's capacity to address remaining areas of poor governance practice.	Stronger governance practices improve risk management and reduce potential for misconduct, loss and failure.

The Institute of Internal Auditors Australia (IIA-Australia) has been actively representing the internal audit, risk and assurance profession, making critical submissions and appearances to elevate the visibility and value of internal auditing and the Three Lines Model as a key part of corporate governance.

Overall, our members **support APRA's proposals** in this consultation paper as "taking a step in the right direction" to improve governance across APRA regulated entities. Our feedback has been raised from members in our financial services demographic.

Part 1 - High Level Feedback

Opportunity for entities to document their Corporate Governance Framework

With APRA's aim to raise governance standards for value creation, our first comment for consideration is that APRA regulated entities should articulate their overall Corporate Governance Framework and have in place a process for regularly reviewing the corporate governance framework.

While this may seem obvious, there is currently no obligation for an organisation to disclose a summary description or overview of their Framework. We believe that disclosing this, in an

easily digested form, ensures organisations of all sizes consider their governance as a whole, rather than complying with particular elements of the Standards.

A summary of the Corporate Governance Framework brings all these pieces together at a higher level and allows the reader to understand the "*rules, relationships, systems and processes within and by which authority is exercised and controlled within corporations".* It also provides stakeholders with this important guide to the measures in place to create value.

Our Recommendation: APRA regulated entities to document and publish their Corporate Governance Framework for transparency and oversight.

Inclusion of the Three Lines Model

Good governance can be further enhanced for APRA regulated entities by formally adopting the Three Lines Model, which is a valuable example of how to bring about governance improvements for performance.

IIA-Australia actively promotes the Three Lines Model as a mechanism for establishing internal structures that support good governance. It allows for responsibilities regarding processes, controls and risk management to be clearly delineated between business areas. This Model should be incorporated into the relevant APRA Governance Standards (*not the Risk Management Standard*) to encourage entities to enhance their control environment and risk management and effectively utilise the independent third line of internal audit.

> *The model applies to all organisations and is optimised by:*
>
> • *Adopting a principles-based approach and adapting the model to suit organisational objectives and circumstances.*
>
> • *Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defense" and protecting value.*
>
> • *Clearly understanding the* ***roles and responsibilities*** *represented in the model and the relationships among them.*
>
> • *Implementing measures to ensure activities and objectives are aligned with the prioritised interests of stakeholders.*

Additionally, ISO 37000:2021 *Governance of organizations – Guidance* provides principles for effective corporate governance and these are complementary to the 3 Lines Model. We hold this ISO standard in high regard as a reference point for corporate governance models.

Our Recommendation: APRA regulated entities are required to adopt the Three Lines Model as a basis for their corporate governance and that this be articulated in the APRA Governance Standards.

Internal Audit inclusions in CPS 510 – Governance:

Whilst APRA is performing the Governance Review and updates to the relevant standards, we see an opportunity to enhance the inclusions regarding the internal audit function.

We note that CPS 510 – Governance includes the following requirements related to internal audit:

> *56. The responsibilities of the Board Audit Committee must include oversight of…* d) internal and external audit… e) *the **appointment and removal** of that institution's auditor and Head of Internal Audit.*
>
> *57. The Board Audit Committee is required to provide prior endorsement for the **appointment or removal** of the institution's auditor and Head of Internal Audit. If the auditor or Head of Internal Audit is removed from their position, the reasons for removal must be discussed with APRA as soon as practicable, and no more than 10 business days, after the Committee's endorsement is agreed upon.*
>
> *60. The Board Audit Committee must regularly review the **internal** and external **audit plans**, ensuring that they cover all material risks and financial reporting requirements of the institution. It must also regularly review the findings of audits, and ensure that issues are being managed and rectified in an appropriate and timely manner.*
>
> *61. The Board Audit Committee must ensure the **adequacy and independence** of both the internal and external audit functions.*
>
> *62. The members of the Board Audit Committee must, at all times, have **free and unfettered access** to senior management, the internal auditor, the heads of all risk management functions, the auditor and the Appointed Actuary, as applicable, and vice versa.*
>
> *66. The internal auditor must have a reporting line and unfettered access to the Board Audit Committee.*
>
> *68. An APRA-regulated institution must have an **independent and adequately resourced** internal audit function for the institution. If an APRA-regulated institution does not believe it is necessary to have a dedicated internal audit function, it must apply to APRA to seek an **exemption** from this requirement, setting out reasons why it believes it should be exempt. APRA may approve alternative arrangements for an institution where APRA is satisfied that they will achieve the same objectives.*
>
> *69. The objectives of the internal audit function must include evaluation of the adequacy and effectiveness of the **financial and risk management framework** of the institution. To fulfil its functions, the internal auditor must, at all times, have **unfettered access to the institution's business lines and support functions**.*

These requirements are valuable in protecting the independence of the internal auditor, and ensuring they have adequate access to people, systems and information to perform their role. In reviewing Governance requirements, and CPS 510, we believe there is an opportunity to amend the commentary included regarding internal audit.

Our Recommendation: We recommend that the internal audit function of an APRA regulated entity be aligned with the International Professional Practices Framework, including the 'Global Internal Audit Standards'.

This will elevate internal audit practice across APRA regulated entities by ensuring the requirements across ethics and professionalism, governance and management of the internal audit function, and quality of internal audit services is upheld to the expectations set for

internal auditors globally. These Standards have enhanced the requirements for internal auditors to Understand Governance, Risk Management, and Control Processes (Standard 9.1) as part of their audit practice and Communicate the Acceptance of Risks (Standard 11.5), highlighting where management has accepted risks outside of the organisations risk appetite or risk tolerance. These standards have been effective since January 2025. They will further support APRA's initiative to improve governance across their regulated entities.

Part 2 - Detailed Feedback on each Proposal

Proposal 1 – Skills and capabilities

"Require regulated entities to:

a) identify and document the skills and capabilities necessary for the board overall, and for each individual director

b) evaluate existing skills and capabilities of boards and individual directors

c) take active steps to address gaps through professional development, succession planning and appointments."

We recommend additional wording to be added to this proposal to highlight the specific skills of the audit and risk committee in regards to risk management and internal audit to provide appropriate oversight. Particularly when it comes to internal audit, appropriate skills and capability of the audit committee is critical for enabling the success of the internal audit function and to support the chief audit executive.

Our Recommendation is to include the following wording (changes in blue):

"Require regulated entities to:

1. Identify and document the skills and capabilities necessary for the board overall, and minimum skills and capabilities for individual directors.
2. Identify and document the skills and capabilities necessary for the chair and members of audit and risk committees.
3. Evaluate existing skills and capabilities of boards and individual directors.
4. Take active steps to address gaps through professional development, succession planning and appointments.
5. When filing a vacancy document the skills and capabilities assessment undertaken to determine the successful candidate(s)".

Proposal 2 – Fitness and propriety

"Require regulated entities to meet higher minimum requirements to ensure fitness and propriety of their responsible persons.

Require SFIs, and non-SFIs under heightened supervision, to engage proactively with APRA on potential appointments."

Our Recommendation: The explanatory requirements should expressly include self-regulated professional body sanctions / membership with commitment to ethical standards. For example, those who are members of the IIA-Australia are required to uphold the International Professional Practices Framework including the Global Internal Audit Standards, and relevant ethical behaviour requirements within. Code of conduct breaches have professional repercussions.

Proposal 5 – Board Performance Review

"Require SFIs to commission a qualified independent third-party performance assessment at least every three years which covers the board, committees and individual directors."

Our Recommendation: This work needs to be undertaken by a qualified governance, risk and assurance professional familiar with independent organisational reviews that go well beyond financial statements and look to delivering insights and foresight for value creation for the organisation.

This is an area IIA-Australia and its members are experts. We recommend that the mechanism for this be an External Board Governance & Performance Assessment performed by an independent, qualified External Quality Assessment practitioner. As there are Standards for these practitioners, IIA-Australia could maintain a Register of such practitioners from large firms to independent contractors. We would welcome the opportunity to discuss this further.

Proposal 6 – Role Clarity

"Define APRA's core expectations of the board, the chair and senior management. Provide additional guidance on which APRA requirements may be delegated to board committees and senior management."

Our Recommendation: Consistent with the recommendations of ISO 37000:2021 *Governance of organizations – Guidance* we suggest that in addition to contact between assurance functions and designated board committees (such as the Audit Committee or the Risk Committee) the board have direct (unmediated) contact with the compliance manager, the risk manager and the chief audit executive (internal auditor) at least once a year.

Board members also need to be aware that while they may delegate some activities, they cannot absolve themselves of their accountabilities outlined in the Three Lines Model:

> *The Governing body*
>
> • *Accepts accountability to stakeholders for oversight of the organization.*
>
> • *Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.*
>
> • *Nurtures a culture promoting ethical behaviour and accountability.*

- *Establishes structures and processes for governance, including auxiliary committees as required.*
- *Delegates responsibility and provides resources to management for achieving the objectives of the organization.*
- *Determines organizational appetite for risk and exercises oversight of risk management (including controls).*
- *Maintains oversight of compliance with legal, regulatory, and ethical expectations.*
- *Establishes and oversees an independent, objective, and competent internal audit function.*

Proposal 7 – Board Committees

"Extend the current requirement for bank and insurer boards to have separate risk and audit committees, to apply to SFI RSE licensees as well. Repeal this requirement for non-SFI banks and insurers, allowing flexibility for smaller entities. Mandate that only full board members can be voting members of APRA-required board committees."

Our Recommendation: Although the separation of risk committees and audit committees is common practice for some entities, we have observed that it makes it difficult for internal audit to be sufficiently across the risk management issues of the organisation and to be party to the relevant discussions. Internal auditors are sometimes left out of the relevant risk committee information and discussion, given that their direct reporting line is only to the audit committee. We recommend that there be a requirement developed for the Chief Audit Executive to attend the risk committee meetings (if they are held separately from the audit committee) and be heard.

Additionally separation of risk committees and audit committees creates other difficulties, such as both being adequately across integrated assurance activities in first, second and third line functions. We recommend that there be a requirement developed for these committees to effectively communicate on such topics.

Proposal 8 – Director Tenure and Board Renewal

"Impose a lifetime default tenure limit of 10 years for non-executive directors at a regulated entity. Require regulated entities to establish a robust, forward-looking process for board renewal."

We commend APRA for taking a bold stance in regard to Board member tenure. We acknowledge that this is being proposed to ensure turnover of board members over time to bring impartial judgement and refresh the Board thinking. There are positives to the approach, but we are aware of some negatives impacts to be managed, such as board members swapping across various boards within their networks and not being truly suitable for their appointment.

Our Recommendation: Strengthening the requirements of Proposal 1 as recommended will help with this. We also recommend that you consider the government pre-qualification

schemes available, such as the IIA-Australia Audit Committee prequalification scheme for renewal outside of current networks.

Thank you for our opportunity to comment and provide feedback. If you have any questions regarding our submission, please do not hesitate to contact us.

Yours sincerely

[redacted]

[redacted]

Chief Executive Officer