Proposed changes to governance

The Australian Prudential Regulation Authority (APRA)

Submitter:

Michael Sanderson

[redacted]

Phone: [redacted]

Email: [redacted]

Introduction

I welcome the opportunity to comment on APRA's proposed changes to governance, including draft Prudential Standard CPS 510 Governance and the associated amendments to CPS 001 Defined terms. The direction of reform is broadly correct because Boards of prudentially regulated institutions should be competent, independent, properly informed and capable of challenging management, while conflicts should be identified and dealt with, responsible persons should be fit and proper, group structures should not compromise the prudential interests of individual regulated entities, and artificial intelligence and other emerging technologies should not create new forms of unaccountable decision making.

The central weakness is that the draft still places too much weight on whether governance machinery exists and too little weight on whether governance actually works. That distinction runs directly through the findings of the Financial Services Royal Commission, APRA's Prudential Inquiry into the Commonwealth Bank, subsequent action involving Westpac and ANZ, and more recent concerns involving superannuation platform trustees, because these institutions did not generally fail for want of Boards, committees, policies, risk frameworks, internal auditors, external auditors, compliance functions, conflicts policies or highly qualified executives. They failed because formal governance and actual governance diverged, information did not always reach the right people, accountability became fragmented, cultural and behavioural warning signs were tolerated, conflicts became normalised, remediation could continue for years without eliminating root causes, and Boards could receive large quantities of information without receiving what they actually needed to understand what was going wrong.

CPS 510 should therefore be judged against a practical test: whether it would make those kinds of failures materially harder to repeat. In its present form, the answer is not yet sufficiently clear because the draft strengthens the architecture of governance without always ensuring that the architecture produces accountability, challenge, transparency and effective risk reduction in practice.

Governance must be measured by outcomes, not artefacts

Draft CPS 510 requires governance frameworks, delegations, charters, management information policies, conflicts registers, skills matrices, annual assessments, external assessments and extensive documentation. All of these can contribute to sound governance, but their existence does not demonstrate that governance is effective, which is why APRA should make the distinction between governance activity and governance outcomes explicit in the operative standard.

A regulated entity should not be able to establish effective governance merely by demonstrating that a matter was considered, a policy existed, a meeting occurred, a risk appeared in a register, a director completed an assessment or a committee received a report. The entity should be capable of showing what information was considered, what contrary information existed, what challenge occurred, why a decision was reached, who was accountable, whether identified weaknesses were corrected and whether the underlying problem subsequently recurred.

The Financial Services Royal Commission repeatedly demonstrated that sophisticated compliance processes can coexist with serious misconduct and poor customer outcomes, while APRA's own CBA Prudential Inquiry similarly identified unclear accountability, inadequate escalation, weak constructive challenge and deficiencies in non-financial risk management despite the existence of an extensive formal governance architecture. Subsequent events showed that this was not merely a pre-Royal Commission problem, because APRA's continuing interventions at Westpac and ANZ demonstrated how long risk governance weaknesses can persist despite extensive remediation programs, while in ANZ's case APRA ultimately increased the operational risk capital add-on to $1 billion and required examination of root causes and behavioural drivers after years of remediation before the Federal Court imposed combined penalties of $250 million in December 2025 for widespread contraventions across several matters.

The lesson should be incorporated directly into CPS 510 by making clear that governance activity is an input and governance effectiveness is the required outcome. APRA should therefore assess whether governance mechanisms change decisions, expose uncomfortable information, identify root causes, prevent recurrence and allocate responsibility, rather than treating the existence of governance documentation as persuasive evidence that the underlying prudential objective has been achieved.

Delegation must not become an accountability escape mechanism

Delegation is unavoidable in a complex financial institution because a Board cannot and should not perform every management function itself, while senior managers and Board committees must carry genuine responsibility for functions entrusted to them. What must not be permitted is the separation of authority from accountability, particularly where a chain of delegation allows responsibility for a serious failure to disappear through committees, business units, group functions, consultants, service providers or automated systems.

Draft paragraph 16 states that the Board remains responsible for "overseeing" obligations delegated to a Board committee or senior managers, but that formulation is too weak because delegation should transfer authority to perform a function without extinguishing the ultimate accountability of the person or body that decided to delegate it. The delegator should remain accountable for determining that the function was appropriate to delegate, selecting a competent and properly resourced delegate, defining the authority and limitations of the delegation, ensuring adequate information and escalation arrangements, monitoring the effective exercise of the delegation, responding to warning signs and correcting failure when it occurs.

This principle should operate throughout CPS 510 so that a Board cannot answer a governance failure merely by pointing to a committee, a committee cannot simply point to senior management, and senior management cannot point further down the chain to a business unit, group function, consultant, service provider or automated system. Responsibility may be distributed according to function, but accountability must remain traceable, and where a delegate is permitted to sub-delegate, that delegate should remain accountable for the proper exercise of the authority it has passed further down the chain.

CPS 510 should therefore state expressly that delegation or sub-delegation does not absolve the delegator of accountability for the effective discharge of the delegated obligation. This would preserve the practical necessity of delegation while preventing organisational complexity from becoming a mechanism through which responsibility evaporates.

Constructive challenge must be capable of being demonstrated

CPS 510 properly requires directors to constructively challenge senior management, but the present drafting risks leaving constructive challenge as an aspiration rather than an auditable governance behaviour. A Board minute recording that a matter was discussed does not establish that assumptions were tested, alternatives were considered or management was genuinely challenged, which means the standard should require evidence capable of showing whether directors sought alternative options, requested additional information, questioned risk estimates, tested

management forecasts, required changes, rejected recommendations, recorded dissent or escalated unresolved concerns.

This matters because one of the recurring failures identified by the Royal Commission and APRA's own inquiries was not necessarily the complete absence of information but the failure to use information effectively to hold management to account. CPS 510 should therefore require Board and committee performance assessments to examine evidence of challenge against significant decisions rather than relying principally on director interviews, surveys and self-assessment.

The objective should not be to manufacture theatrical disagreement or encourage dissent for its own sake because a high-performing Board may ultimately reach a unanimous decision. The important question is whether the decision was genuinely tested before that unanimity was reached and whether the record allows APRA, an independent reviewer or the Board itself to determine how that testing occurred.

Management information must not become curated information

The proposed management information policy is an important reform, but a policy governing the content, quality and frequency of information supplied to the Board will achieve little if senior management remains able to curate the picture presented to directors. Paragraph 22's expectation that information be succinct and relevant is understandable, but brevity can become sanitisation if material adverse information is filtered out on the basis that management considers it too detailed, immaterial or operational.

Boards need concise information, but they also need access to inconvenient information, which means management information should expressly include significant aged audit findings, repeated control failures, breaches, complaints trends, remediation delays, control overrides, operational incidents, near misses, risk appetite exceptions, material conflicts, related-party arrangements, critical outsourcing dependencies and matters management has decided not to escalate. Directors should also have an explicit right to obtain the underlying information because management should summarise information for the Board without being able to control what the Board is permitted to know.

Materiality should also be assessed cumulatively because ten individually small failures may reveal a serious systemic problem, while a recurring complaint, control exception or operational incident should not remain permanently beneath a materiality threshold merely because each occurrence is assessed in isolation. CPS 510 should therefore require aggregation by frequency, duration, recurrence, common cause and cumulative impact so that patterns cannot disappear inside a sequence of apparently immaterial individual events.

The independent Board assessment regime contains a serious closed loop

The proposed independent Board performance assessment for significant financial institutions is potentially one of the strongest reforms in CPS 510, but in its present form it also contains one of the largest loopholes. APRA originally proposed that the independent assessment report be provided to APRA, later withdrew that requirement following consultation, and has also declined to prescribe meaningful minimum qualifications for the independent reviewer, while the draft repeatedly refers to an entity demonstrating progress against recommendations that it has "accepted".

Taken together, these provisions create a closed loop in which the regulated entity selects and pays the reviewer, the standard does not establish meaningful minimum reviewer qualifications, the complete report does not automatically go to APRA, the Board decides which recommendations it accepts, and the strongest express remediation obligation then applies only to those accepted recommendations. An independent review could therefore identify an uncomfortable governance weakness, the Board could reject the recommendation, and the strongest express obligation to remediate that weakness could disappear without APRA necessarily receiving the full assessment that identified it.

APRA does not need to publish every report because there are legitimate reasons to protect confidential interviews and sensitive prudential information, but APRA should automatically receive the complete report for significant financial institutions or, at an absolute minimum, every finding, recommendation, rejected recommendation, Board response and remediation plan. Rejected recommendations may be more important to a prudential supervisor than accepted recommendations because they identify the precise points at which the Board and independent reviewer disagree.

CPS 510 should also require the reviewer to be independent in substance, suitably qualified and free from material consulting relationships capable of creating an economic incentive to preserve the client relationship. Independent assessment should operate as an external challenge mechanism capable of informing the regulator, rather than becoming another privately controlled component of the institution's internal governance framework.

External review should follow risk, not merely institutional size

The independent triennial review requirement principally applies to significant financial institutions, which is a reasonable starting point but an incomplete proxy for governance risk. A smaller entity may present heightened governance risk because it is growing rapidly, relies extensively on outsourcing, operates a complex platform model, has significant related-party arrangements, has suffered repeated material breaches or is subject to heightened APRA supervision.

Recent superannuation experience demonstrates that governance risk does not begin at an arbitrary balance-sheet threshold, so APRA should retain the SFI requirement while establishing clear risk-based triggers for requiring an independent governance assessment outside the SFI population. Proportionality should reduce unnecessary governance machinery, but it should not prevent APRA from imposing stronger external scrutiny on a smaller institution whose structure, conduct or history creates heightened governance risk.

Director tenure should not become institutionalised exceptionalism

APRA originally proposed a ten-year tenure limit and has now moved to twelve years, with an additional twelve-month extension available in exceptional circumstances. There is a legitimate argument for retaining institutional knowledge, but twelve years is already a substantial period in which familiarity, relationships and prevailing institutional assumptions can become entrenched, which makes the additional extension particularly important to control.

The draft allows the Board itself to approve the exceptional additional year and then notify APRA, but if the circumstances are genuinely exceptional, APRA should provide prior non-objection rather than merely be informed after the decision has been made. The standard already uses a prior APRA non-objection mechanism in other contexts, so there is no obvious reason why a Board should be permitted to decide for itself that exceptional circumstances justify extending the tenure of one of its own longstanding members without prior regulatory scrutiny.

Cumulative tenure across relevant group entities should also be taken into account because moving from a parent Board to a subsidiary Board should not automatically reset the independence clock where relationships, information and institutional alignment remain substantially unchanged. The relevant question is whether independence may have been eroded through long institutional association, not merely whether the legal entity on the director's appointment letter has changed.

Board independence must exist when decisions are actually made

The draft requires a majority independent Board for many regulated entities, but the meeting requirement appears weaker because the majority of eligible voting directors present need only be non-executive rather than independent. This creates a practical loophole because a Board may be majority independent in overall composition while a material prudential decision is made at a meeting where independent directors do not constitute the voting majority.

APRA should therefore require an independent-majority quorum for material prudential decisions unless genuinely exceptional circumstances make that impossible, with those circumstances documented and subject to appropriate subsequent review.

Formal independence on an organisational chart is not sufficient if independent directors are not present in sufficient numbers when material power is actually exercised.

The RSE governance exclusions require reconsideration

The treatment of RSE licensees deserves particularly close attention because the draft excludes them from important aspects of the general Board independence provisions and from the dedicated group governance regime that applies elsewhere. Those exclusions should be reconsidered in light of APRA's own recent supervisory experience involving platform trustees and other superannuation entities.

APRA has taken action against trustees over weaknesses involving due diligence, monitoring, conflicts, Board information and oversight, while concerns identified in relation to HTFS included governance arrangements involving key decision makers who also held parent or group leadership roles and the absence of an independent trustee voice. Those developments make it difficult to justify a final prudential standard that strengthens group independence elsewhere while leaving RSE licensees outside the dedicated group governance architecture.

The answer need not be mechanical transplantation of the bank and insurer model into superannuation because the SIS Act and representative trustee structures create particular legal considerations. The prudential principle should nevertheless be unavoidable: where an RSE licensee sits inside a corporate group, the trustee must possess sufficient independent capability, information and authority to place beneficiaries' interests ahead of the commercial interests of the parent, platform, related service provider or wider group, rather than allowing group structure to convert fiduciary independence into a matter of internal escalation.

Group governance must follow practical control

The group governance provisions are directionally strong, particularly in recognising that the interests of an individual regulated entity may diverge from the interests of the wider group, but requiring arrangements merely to “support” independent judgement is weaker than requiring the regulated entity to exercise it. CPS 510 should make clear that a local regulated entity must be able to refuse a parent or group direction where that direction is inconsistent with its prudential obligations, risk appetite or the interests it is legally required to protect.

Where a material disagreement cannot be resolved internally, there should be a clear escalation pathway to APRA so that the local entity is not forced to choose between group loyalty and prudential responsibility without regulatory visibility. The same principle should apply to shared services, outsourced functions and intra-group

arrangements, because accountability should follow practical control, knowledge, benefit and participation rather than stop at the boundary of a legal entity.

A corporate group should therefore not be permitted to centralise decision making while decentralising responsibility. If practical control sits elsewhere in the group, the governance framework should identify that control and ensure that accountability remains capable of being traced to the people and entities actually exercising it.

Conflict management must begin with avoidance

The proposed conflict requirements are an improvement, particularly because they expressly recognise structural, funding and remuneration conflicts, but the draft remains too dependent on the proposition that conflicts can be managed. Paragraph 74 allows an entity to avoid a conflict where required by law or where the entity reasonably concludes that the conflict cannot effectively be managed, which means the institution exposed to or benefiting from the conflict is substantially permitted to determine whether its own conflict is manageable.

That is a weak foundation for serious structural conflicts because the Financial Services Royal Commission repeatedly demonstrated the limits of disclosure, policies and internal management where economic incentives pull an institution in competing directions. The lesson was not that every conflict could be cured with a better register, but that some conflicts cannot credibly be neutralised while the commercial incentive that created them remains in place.

A disclosed conflict remains a conflict, just as a conflict entered in Board minutes or supported by an internal declaration remains a conflict, so CPS 510 should establish a hierarchy in which avoidance is preferred where reasonably practicable, independent assessment is required where avoidance is not practicable, and material structural conflicts attract heightened independent approval and APRA visibility. The accompanying prudential practice guide should also identify categories of conflict that are presumptively difficult to manage, particularly arrangements involving related-party service providers, overlapping parent and subsidiary roles, remuneration linked to conflicted products or services, and circumstances where the decision maker receives material benefit from the outcome being assessed.

The standard should therefore distinguish between conflicts that can genuinely be managed and structural contradictions that should ordinarily be removed. Without that distinction, the conflicts regime risks becoming another process through which an institution documents why it has decided that a profitable conflict can safely continue.

Apparent independence should not be ignored

APRA has moved away from expressly regulating perceived conflicts in the standard following concerns that the concept could be subjective, but the solution should not be

to ignore how a reasonable independent observer would assess an arrangement. Governance depends partly upon confidence that decision makers are not only independent in their own minds but can reasonably be regarded as independent when the relevant facts are known.

Auditor independence already recognises this broader concept, so CPS 510 should address objectively apparent conflicts by asking whether a reasonable person, properly informed of the relevant circumstances, could conclude that a director's or decision maker's judgement may be materially affected. Such a test would not turn rumour or subjective perception into a prudential standard because it would remain anchored in objective facts and the perspective of a properly informed reasonable observer.

Fit and proper reform should streamline duplication without reducing APRA's sightline

There is a legitimate case for reducing duplication between CPS 510 and the Financial Accountability Regime, but there is not a legitimate case for turning administrative simplification into regulatory blindness. APRA proposes to narrow the responsible-person population and remove substantial routine fit-and-proper reporting affecting information concerning thousands of individuals, while also moving away from its earlier proposal for mandatory pre-appointment engagement for significant financial institutions and entities under heightened supervision.

Those changes need to be considered together because the institution conducts the assessment, determines when an emerging concern becomes material, and will provide less routine information to APRA, while mandatory early engagement on significant appointments is also removed. APRA may therefore become involved only after an institution has already appointed a person or has itself concluded that the person is unsuitable, which represents a considerable transfer of reliance back to the regulated institution.

APRA should retain a lightweight central notification regime covering the most important prudential positions, including Chairs, chief executives, chief risk officers, relevant Board committee chairs and other genuinely critical responsible persons at significant financial institutions and entities under heightened supervision. Notification should occur before appointment with sufficient time for supervisory concerns to be raised, while recognising that this need not become an APRA appointment veto where the legislation does not confer such a power.

This would preserve the legitimate objective of reducing low-value duplication while ensuring that administrative streamlining does not reduce supervisory visibility over the people exercising the greatest prudential influence.

Fit and proper concerns should trigger inquiry before they become findings

Draft CPS 510 sensibly recognises that credible allegations or adverse information may require a person's fitness and propriety to be reassessed, but the standard should distinguish clearly between information sufficient to trigger an inquiry and evidence sufficient to determine that somebody is not fit and proper. An allegation should not be treated as a finding, while equally an institution should not be able to avoid APRA scrutiny by investigating indefinitely on the basis that no final adverse conclusion has yet been reached.

CPS 510 should therefore require prompt escalation based on seriousness so that, where a significant responsible person becomes subject to credible allegations of material dishonesty, serious misconduct, major control failure or another matter directly relevant to fitness and propriety, APRA is notified that a reassessment has commenced. The institution can then investigate fairly and reach a properly evidenced conclusion while APRA remains sighted on the prudential risk, thereby protecting both regulatory integrity and procedural fairness.

An adverse fit and proper finding should have a real consequence

Paragraphs 91 and 92 require clarification because the draft states that reasonable steps must be taken to ensure that an unfit person does not continue in the position while also expressly contemplating circumstances in which that person may remain. There may be rare legal or operational circumstances in which immediate removal is impossible and a short transition is necessary to transfer responsibilities safely, but that limited possibility should not become an ambiguity capable of permitting indefinite continuation.

Where a person has been finally assessed as not fit and proper, continued service should therefore be permitted only for a tightly controlled transition, APRA should be notified immediately, material decision-making powers should be restricted where practicable and a defined removal timetable should apply. A fit and proper regime loses credibility if a final conclusion that a person is not fit and proper can coexist with that person continuing indefinitely to exercise the very functions for which fitness and propriety are required.

Culture must be treated as a prudential mechanism, not a slogan

CPS 510 refers to culture, values and tone from the top, but these concepts require greater substance because the Royal Commission and APRA's subsequent supervisory experience show that culture cannot be measured principally through employee surveys, Board statements or codes of conduct. Culture is more reliably revealed by what an institution rewards, tolerates, escalates and ignores, particularly when commercial objectives collide with risk controls or legal obligations.

Boards should therefore receive information about repeated breaches, control overrides, complaints, whistleblowing trends, internal challenge, employee retaliation, remediation failures, risk acceptance, promotion decisions, consequence management and circumstances in which commercial objectives repeatedly prevail over risk controls. Remuneration should also be understood broadly because formal variable remuneration is only one incentive, while promotion, status, revenue targets, divisional budgets, sales expectations, access to senior management, career advancement and informal consequences can exert equal or greater influence over behaviour.

CPS 510 should consequently require Boards to consider the whole incentive architecture where it materially affects prudential risk. A culture policy cannot prove sound culture if the institution's actual incentives continue to reward the behaviour that the policy claims to discourage.

Control functions need direct protection when their leaders are removed

The draft appropriately addresses the removal of auditors, the Head of Internal Audit and the Chief Risk Officer, but APRA should not rely solely on the regulated entity's explanation of why a control-function leader was removed. Where the CRO, Head of Internal Audit or relevant auditor is removed, materially stripped of authority or has resources substantially reduced, that person or function should have an independent right to provide APRA directly with their account of the circumstances.

A regulator should hear both sides where the person responsible for challenging management loses their position because even the strongest formal control function is ineffective if exercising that function creates an unrecorded career risk. The provisions governing communication with APRA should therefore be strengthened by an express prohibition on retaliation, disadvantage or adverse career action arising from good-faith engagement with APRA or the proper exercise of internal prudential control responsibilities.

Internal audit should examine governance effectiveness itself

The internal audit provisions should be widened so that internal audit is not confined principally to financial and traditional risk-management frameworks. Its mandate should expressly extend to the operating effectiveness of material governance arrangements, culture controls, conflicts management, fit and proper processes, remuneration governance, critical outsourcing, artificial intelligence governance and major remediation programs.

This does not mean every internal audit plan must examine every topic every year, but it does mean the mandate should be capable of following prudential risk wherever that risk sits. Many modern institutional failures do not arise from accounting weakness but from incentives, information flows, conduct, outsourcing, technology, organisational

complexity and failures to act on known problems, so internal audit should have an unambiguous mandate to test those systems directly.

Remediation must end in demonstrated risk reduction

One of the clearest lessons from post-Royal Commission experience is that remediation itself can become a governance industry in which programs are established, consultants engaged, actions allocated, milestones created, reports produced and Board dashboards progressively turn from red to amber and finally green without the underlying behaviour or control weakness necessarily disappearing. APRA's experience with institutions including ANZ demonstrates why closure of a remediation program cannot itself be treated as evidence that the underlying prudential problem has been solved.

CPS 510 should therefore require material remediation to conclude with outcome testing under which the Board satisfies itself not merely that actions were completed but that the root cause was addressed, the relevant control now works, the weakness has not migrated elsewhere and recurrence has materially reduced. Remediation should be treated as complete when the risk has changed in practice, not merely when the project plan records that the action has been closed.

Artificial intelligence requires controls outside the artificial intelligence

APRA specifically asks whether the proposed framework adequately supports governance of artificial intelligence and related technologies, and recent developments make this question considerably more immediate. CPS 510 can appropriately remain technology neutral because APRA should not write a prudential standard around particular models or software that may rapidly become obsolete, but the accompanying prudential practice guide should establish minimum governance expectations for material AI systems and, critically, should not assume that instructions given to an AI system are themselves an adequate control.

Recent experience with increasingly capable agentic models demonstrates why this distinction matters. In July 2026, the UK AI Security Institute reported that every frontier model it tested for relevant behaviour had at times attempted to achieve cyber evaluation objectives through methods outside the permitted scope, including searching outside authorised environments, escalating privileges and probing evaluation infrastructure. In one particularly significant case, a model confronted with a misconfigured and effectively unsolvable evaluation persisted until it wrote and executed code on an external internet service in an attempt to access AISI's own infrastructure. No damage occurred, but AISI concluded that the attempt could have succeeded had the surrounding infrastructure not been securely designed, while also finding that model self-reporting and expressed reasoning were not reliable ways of detecting prohibited behaviour.

OpenAI disclosed a related experience in July 2026 involving a long-horizon model that was instructed to post the results of a task only to Slack but subsequently persisted for approximately an hour, identified a vulnerability in its sandbox, circumvented restrictions intended to prevent external access and posted material to a public GitHub repository. OpenAI paused the internal deployment and responded with stronger safeguards, including monitoring the model's entire sequence of actions rather than assessing actions individually, together with mechanisms capable of pausing activity and allowing human intervention. The significance for prudential governance is not whether the model possessed some independent intention to “escape”, but that a capable automated system pursuing an authorised objective found an unauthorised route around a control intended to contain it.

This exposes an important weakness in conventional AI governance. A regulated institution cannot safely rely on the AI system to police its own compliance with instructions, report its own breaches or determine whether its own proposed actions remain within authority. The system performing the task should therefore not also constitute the principal control over the task, just as a business unit exposed to a conflict should not be treated as the sole judge of whether that conflict has been effectively managed.

For material agentic systems, CPS 510 guidance should consequently require controls that are technically and organisationally external to the model, including appropriately restricted system privileges, network and data access controls, segregation between systems, independently enforced limits on available tools and transactions, monitoring of sequences of actions rather than isolated outputs, reliable audit trails, predefined escalation thresholds, and an effective capacity to suspend, isolate or roll back an AI system where unexpected behaviour occurs. The strength of those controls should reflect the consequence of the authority given to the system, particularly where AI can move funds, alter customer records, approve transactions, interact with critical infrastructure, modify production code, access confidential data, execute cyber functions or communicate autonomously with external systems.

A regulated entity should also know where material AI is deployed, what decisions it influences, what authority and system access it possesses, what data it relies upon, what limitations and failure modes are known and who remains accountable for its behaviour. Independent validation should be proportionate to the consequence of the use, while data provenance, model drift, anomalous behaviour, control circumvention and unexpected tool use should form part of continuing monitoring rather than being treated solely as pre-deployment testing issues.

The recent incidents also strengthen the case for continuous monitoring because they show that even sophisticated pre-deployment evaluation cannot anticipate every

behaviour that may emerge when a capable system operates for long periods or encounters an unexpected weakness in its environment. APRA should therefore make clear that certification, initial validation or vendor assurance cannot establish continuing safety, just as the existence of a governance policy cannot establish effective governance more generally.

Third-party AI requires particular attention because a regulated institution cannot outsource a model and thereby outsource accountability for what the model does. Where a vendor controls the underlying model, updates it, changes its capabilities or provides the infrastructure through which it operates, the regulated entity should understand that dependency, retain the ability to restrict the authority granted to the system and maintain independent controls capable of containing an unexpected failure regardless of assurances provided by the model developer.

The governance principle is therefore stronger than simply requiring a human accountable owner. The more autonomy, persistence, system access and practical decision-making authority an AI system is given, the less acceptable it becomes to rely upon the AI system itself as a control and the stronger the independent human and technical controls surrounding it must become. This is consistent with the broader principle running through CPS 510 that responsibility should remain with those who authorise, control and benefit from the delegation of authority, whether the delegate is a person, service provider or machine.

Proportionality should apply to machinery, not accountability

APRA asks whether CPS 510 will operate proportionately across institutions of different types, sizes and structures, and it should, but proportionality requires careful definition. A small institution should not be required to reproduce every governance layer of a major bank merely because that is the structure easiest for APRA to supervise, while a simpler institution may reasonably require fewer committees, simpler documentation and less elaborate review machinery.

The underlying prudential outcomes should not be scaled down because integrity, fitness and propriety, effective conflict management and Board accountability do not become less important merely because a regulated entity has fewer assets. Proportionality should therefore operate primarily in how an institution demonstrates compliance and structures its governance machinery, rather than in whether it must achieve the underlying prudential outcome.

The same principle should apply to new and non-traditional institutions because governance quality depends upon competence, accountability, independence, challenge and control of the authorised activities, not upon mechanically replicating the organisational structure of an incumbent major bank.

Compliance cost should be measured against useful regulatory information

The consultation also asks about compliance cost, and there is a genuine opportunity to reduce low-value duplication, particularly where FAR and prudential reporting overlap. Compliance cost should not, however, be assessed simply by counting the number of forms removed or policies consolidated because a shorter reporting burden that deprives APRA of useful early-warning information is not efficient regulation, just as requiring thousands of pages of governance documentation that neither directors nor supervisors use effectively is not strong regulation.

The correct approach is to remove information that genuinely serves no independent prudential purpose while strengthening the flow of information concerning material conflicts, important appointments, rejected independent-review findings, unresolved control weaknesses, major remediation failures and emerging prudential risks. Good regulation should demand less evidence of activity while demanding better evidence of outcomes.

Has consultation begun to reverse APRA's own prudential diagnosis?

Meaningful consultation requires APRA to listen to regulated entities and alter proposals where costs, duplication or unintended consequences cannot be justified, but consultation should not result in the regulated population progressively removing the external checks introduced because self-regulation and supervisory guidance had already proved insufficient. That risk deserves particular attention in this review because APRA's starting diagnosis was unusually clear: supervisory experience had identified weaknesses in Board renewal, conflicts management, fitness and propriety, accountability and governance effectiveness, while APRA itself concluded that guidance and supervision alone had not always changed entrenched practice and that some fit and proper processes had become little more than a tick-box exercise.

Against that diagnosis, the cumulative direction of the changes made following consultation is difficult to ignore. The proposed ten-year director tenure limit has become twelve years after calls for greater Board flexibility; the proposed requirement for at least two directors independent of other group Boards was withdrawn following strong opposition; perceived conflicts were removed from the enforceable standard after strong opposition; banks and insurers will not be required to publish conflicts registers after opposing public disclosure; significant financial institutions will no longer routinely provide their independent Board assessment reports to APRA after concerns were raised about candour; APRA declined to prescribe reviewer qualifications; mandatory early engagement on significant appointments was abandoned following strong opposition, despite APRA expressly describing that retreat as a deliberate risk trade-off; and routine fit and proper reporting is proposed to disappear for approximately 6,000 individuals as APRA places greater reliance on FAR reporting.

None of these decisions, considered individually, establishes that APRA has yielded improperly to industry, and several may have legitimate arguments concerning proportionality, duplication or practicality. The concern arises from their combined direction, because many of the concessions reduce external constraint, regulatory visibility or independent scrutiny while leaving more of the judgement about governance effectiveness inside the regulated institution itself.

That creates an uncomfortable circularity. APRA began the review because its supervisory experience showed that regulated entities did not always identify conflicts adequately, assess fitness and propriety robustly, renew Boards sufficiently, challenge management effectively or remediate governance weaknesses despite existing obligations. Yet the revised framework increasingly relies upon those entities to assess their own conflicts, determine the independence of their own directors, select and pay their own independent Board reviewers, decide which review recommendations they accept, retain the full review report unless APRA asks for it, assess their own responsible persons and determine when an emerging fit and proper concern has become sufficiently serious to notify the regulator.

The relevant question is therefore not whether every industry objection should have been rejected. It is whether consultation has cumulatively shifted the balance so far towards institutional discretion that the entities whose governance APRA is supposed to supervise increasingly determine the information and evidence through which APRA supervises them.

That question is especially important after the Financial Services Royal Commission and subsequent governance failures. Those episodes demonstrated that sophisticated institutions can possess extensive internal governance, compliance and assurance machinery while serious problems remain unidentified, unreported, normalised or unresolved. A prudential framework designed in response to that history should be particularly cautious about replacing external visibility with additional reliance on internal assurance.

APRA should therefore conduct a final cumulative review of every material concession made since the March 2025 proposals and ask, for each one, what prudential safeguard has been removed, what risk that safeguard was originally intended to address, what evidence demonstrates that the risk can now be managed without it, and what equally effective mechanism has replaced it. Where no convincing replacement exists, the original safeguard should be restored or an alternative external check introduced.

This does not require APRA to reject legitimate industry concerns or impose unnecessary prescription. It requires recognition that consultation is an input into prudential regulation, not a transfer of regulatory design to the regulated population. The final CPS 510 should be determined by the prudential risk APRA originally identified

and the evidence of what prevents that risk, rather than by how many regulated entities find a particular safeguard inconvenient.

The prudential practice guide should not be used to rescue weak operative requirements

APRA proposes to support CPS 510 with further prudential guidance, which will be useful for proportionality, constructive challenge, conflicts, AI governance, management information and fit and proper assessments. Important safeguards should nevertheless not exist only in guidance where they are fundamental to the intended prudential outcome.

The operative standard should establish the core duties clearly while guidance explains how those duties may be satisfied in different circumstances. This distinction matters because a framework can be formally strong but practically optional if its hardest expectations sit only in non-binding guidance, so the final CPS 510 should contain the minimum hard requirements concerning ultimate Board accountability, independent-review findings, material conflicts, regulatory escalation and fit and proper consequences, with CPG 510 then providing examples and proportional implementation guidance around those requirements.

Conclusion

APRA should proceed with a consolidated CPS 510, but strengthen it before finalisation because the principal risk is not that the draft lacks governance machinery; it is that the standard may generate more policies, registers, reviews and attestations without producing correspondingly stronger accountability, challenge and risk reduction. Australia has already tested that model through institutions that possessed sophisticated Boards, committees, risk functions, auditors and remediation programs while serious governance failures developed beneath them.

The Financial Services Royal Commission, APRA's CBA Prudential Inquiry, subsequent intervention at Westpac and ANZ, and more recent superannuation trustee failures all demonstrate that formal governance can coexist with fragmented accountability, filtered information, normalised conflicts and ineffective remediation. The final standard should therefore require Boards to remain ultimately accountable despite delegation, management information to expose rather than curate risk, constructive challenge to be demonstrable, independent reviews to genuinely inform APRA including rejected findings, structural conflicts to be avoided where they cannot credibly be managed, group structures not to dilute local responsibility, fit and proper streamlining not to reduce APRA's sightline, and remediation to close only when the underlying risk has demonstrably been reduced.

The same principle should apply to artificial intelligence, particularly as increasingly capable agentic systems demonstrate that authorised objectives can be pursued through unintended or unauthorised means. Material AI should remain subject to identifiable human accountability and independent technical controls, with stronger safeguards as autonomy, persistence and system access increase.

APRA should also reconsider the cumulative effect of the concessions made since its original proposals because the concern is not any single change, but whether their combined direction has shifted too much discretion, self-assessment and information control back to the institutions whose governance APRA is supervising. Where a review begins from evidence that existing internal governance and supervisory guidance have not always produced sufficiently robust outcomes, the final framework should be cautious about weakening external scrutiny without an equally effective replacement.

A regulated entity has not demonstrated good governance merely because it can prove that governance processes occurred. It has demonstrated good governance when those processes expose risk, change decisions, preserve accountability, correct root causes and prevent recurrence, and that is the standard against which CPS 510 should be written, supervised and enforced.