INFORMATION PAPER

Authorised deposit-taking institutions: guide for directors

November 2022

AUSTRALIAN PRUDENTIAL REGULATION AUTHORITY | WWW.APRA.GOV.AU

Disclaimer Text

This Guide is not legal advice and users are encouraged to obtain professional advice about the application of any legislation or prudential standard relevant to their particular circumstances and to exercise their own skill and care in relation to any material contained in this Guide.

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

Contents

Introduction

This information paper assists directors of authorised deposit-taking institutions (ADIs) in understanding their obligations under APRA's prudential framework. It brings together, in one place, material requirements and guidance for ADI boards from APRA's prudential standards and prudential practice guides (PPGs).

It includes:

- The role of directors at an ADI: Overarching guidance for directors to assist Boards in providing effective oversight of an ADI. This guidance is derived from APRA's Aid for Directors, which was originally published in 2014.
- Specific obligations: A comprehensive list of material requirements and guidance for Boards currently contained in APRA's prudential standards and PPGs.

This Guide does not introduce new requirements or guidance, beyond those that have already been published. It is confined to prudential requirements that have been established by APRA, and excludes obligations that come from primary legislation.[1]

This Guide is intended for information purposes only and does not take the place of any APRA prudential standard or guidance or establish any formal requirements beyond those already set in the prudential standards. For the purposes of understanding the detailed requirements, refer to the prudential standards and guidance directly.

The Guide for ADI Directors is presented in an integrated manner, with enforceable requirements from prudential standards at the start of each section in blue boxes followed by the relevant accompanying guidance below.

Version: 30 September 2022

This version of the Guide is based on prudential standards that were in force at 30 September 2022. It also includes prudential standards that have been recently finalised, which are due to come into effect in 2023.[2] Requirements that are still subject to consultation have not been included.

APRA will regularly update this Guide as changes are made to the prudential framework, so that the compilation remains current. Broader context surrounding the particular obligations included in this Guide can be found in the underlying prudential standards and PPGs.

---

[1] For example, it excludes obligations that are in the *Banking Act 1959* (Banking Act), *Financial Sector (Collection of Data) Act 2001* (FSCOD Act), *the Financial Sector (Shareholdings) Act 1998*, or the *Corporations Act 2001* (Corporations Act).

[2] This includes: *Prudential Standard CPS 511 Remuneration; Prudential Standard APS 113 Capital Adequacy: Internal Ratings-based Approach to Credit Risk*; and those listed at ADI capital reforms: Consequential amendments | APRA

Figure 1: Summary of APRA requirements

Theme	Summary
Financial resilience	**Capital adequacy**: The Board must ensure the ADI maintains an appropriate level and quality of capital commensurate with the type, amount and concentration of risks to which the ADI is exposed. **Liquidity:** An ADI must maintain an adequate level of liquidity to meet its obligations as they fall due across a wide range of operating circumstances.
Risk management	**Risk management**: An ADI must maintain a risk management framework that is appropriate to the size, business mix and complexity of the institution or group.
Governance	**Governance**: It is essential that an APRA-regulated institution and group has a sound governance framework and conducts its affairs with a high degree of integrity. **Accountability**: The accountability obligations of an ADI are to take reasonable steps to conduct its business with honesty and integrity, and with due skill, care and diligence. An ADI must also deal with APRA in an open, constructive and cooperative way (Banking Act, s.37C). **Disclosure**: An ADI must meet minimum requirements for the public disclosure of key information so as to contribute to the transparency of financial markets and to enhance market discipline.
Resolution	**Recovery and exit planning**: An ADI must be adequately prepared for scenarios that may impact the financial viability of their business. (draft requirement) **Resolution planning**: An ADI that is a significant financial institution (SFI), or provides critical functions, must support APRA in the development and implementation of a resolution plan. (draft requirement)

Chapter 1 - The role of directors at an ADI

This chapter provides general guidance to assist directors in providing effective oversight of an ADI. Content is based on APRA's Aid for Directors, which is a general guide first published in 2014.

Aid for Directors

APRA's approach to supervision is built on the premise that the board and management of an APRA-regulated entity are primarily responsible for the entity's financial soundness and prudent risk management.

With this in mind, APRA imposes various requirements and duties on boards, in addition to those that apply to all entities under the Corporations Act and other legislation. APRA's requirements form part of a framework which is designed to protect the interests of depositors within a stable, efficient and competitive financial system.

The additional obligations imposed under APRA's prudential framework, while substantial, can be readily met by a well-functioning board that has an appropriate mix of skills and experience amongst its directors and strong support from management.

This chapter is intended to help directors of the board of an ADI understand the additional responsibility placed on them under APRA's prudential framework. It assumes that the director is otherwise an experienced board practitioner, and familiar with directors' duties more generally.

What is the purpose of APRA regulation?

ADIs are subject to the governance requirements that apply to any other company, including the Corporations Act. For those companies that are publicly listed, the Australian Securities Exchange Corporate Governance Council's Corporate Governance Principles and Recommendations are also relevant.[3]

Beyond the general obligations that apply to all corporations, ADIs are also subject to prudential regulation by APRA. There are two primary purposes that prudential regulation seeks to fulfil:

- To protect the interests of depositors: The efficient functioning of the financial system is dependent on the promises to depositors being met in full and on time. It is also critical that depositors have confidence in the safety of future payments due to them. Yet many lack the capacity, due to the nature of their interests and the complexity of banking businesses, to make informed judgements about the financial soundness and longer-

[3] A working knowledge of general directors' duties set out in the Corporations Act and, for directors of listed companies, the Australian Securities Exchange Corporate Governance Council's Corporate Governance Principles and Recommendations is assumed. See ASX Corporate Governance Council.

term viability of the financial institutions with which they deal. Through setting appropriate standards and undertaking active supervision, prudential regulation seeks to instil confidence in the community that regulated institutions are operating in a safe and sound manner.

- To promote financial stability: The cost of, and potential disruption from, the failure of a financial institution may be significantly greater than that of a normal commercial enterprise – beyond the impact on its own depositors or other creditors. This is because the failure of one financial institution may have flow-on impacts on other financial institutions through direct inter-linkages or as a result of loss of consumer confidence. By setting minimum standards, prudential regulation seeks to ensure that the risks of financial instability, and the wider costs to the community of such instability, are adequately taken into account in the way in which financial institutions operate.

Further, there can be inherent conflicts between the interests of shareholders, management and depositors, and these need to be managed fairly. APRA's prudential framework therefore holds ADIs to high standards in terms of governance and prudent management. Boards play a critical role in ensuring those standards are met.

What is the legal basis of the prudential framework?

The prudential framework for ADIs is set out in a three-tiered framework of legislation, prudential standards and PPGs.

There are three foundational pieces of legislation on which APRA's activities are based:

- the *Australian Prudential Regulation Authority Act 1998* (APRA Act) sets out APRA's broad objectives and powers;
- the Banking Act provides for prudential supervision of ADIs by APRA, and establishes that APRA must exercise its powers and functions for the protection of depositors and for the promotion of financial system stability; and
- the FSCOD Act deals specifically with APRA's powers to collect a range of financial and other data from regulated institutions.

Under the APRA Act, APRA's purposes include regulating bodies in the financial sector where the law provides for their prudential regulation. The Act requires APRA to do so while balancing the objectives of financial safety and efficiency, competition, contestability and competitive neutrality, and in balancing those objectives, to promote financial system stability.

Under the APRA Act, APRA has the power to make prudential standards. Prudential standards are a form of regulation that has the force of law and are used by APRA to establish certain minimum financial and operational requirements which ADIs must comply with.

In some areas, APRA has introduced cross-industry prudential standards, including for governance and risk management, where the fundamental principles that regulated

institutions must adhere do not materially vary by industry. Prudential standards that apply on a cross-industry basis can be identified by the prefix 'CPS'.

Some prudential standards, on the other hand, are applicable only to a particular industry sector, reflecting the inherent differences between the respective industries. For example, minimum capital requirements are set out in separate industry-based capital standards, given the different nature of the risks faced by different types of institutions. Prudential standards that apply to ADIs only can be identified by the prefix 'APS'.

To ensure prudential requirements are proportionately applied, there are some provisions in the prudential standards that only apply to SFIs (i.e. larger, more complex organisations). In the case of ADIs, an SFI means an ADI that is either:

- not a foreign ADI and has total assets in excess of AUD $20 billion; or
- determined as such by APRA, having regard to matters such as complexity in its operations or its membership of a group.

Finally, APRA also develops PPGs to support implementation of the prudential standards. As the name implies, these provide guidance only and do not have the force of law. PPGs are intended to outline APRA's view of how prudential requirements could be met and provide information on good practice within the industry. Regulated institutions are not obliged to adopt the guidance and are free to demonstrate that the requirements of the prudential standards are otherwise met. Nevertheless, the PPGs may provide institutions (and their boards) with helpful information on how to meet prudential requirements.

What role does a board need to play in ensuring compliance with the prudential framework?

The role of a board in meeting APRA's prudential requirements is no different to that of a board in meeting other legal obligations that are placed upon it and the institution for which the board is responsible.

APRA does not expect directors to have a detailed knowledge of each of the relevant laws and prudential standards. It is important, however, that the board satisfies itself that the institution and its management have effective processes and procedures in place to meet APRA's prudential requirements, including those that are specific to the board. It is also important that the board satisfies itself that any breaches of the requirements will be promptly identified and reported to it, and to regulators such as APRA, as appropriate.

Meeting these requirements will, as well as ensuring compliance with the prudential standards, also aid directors in meeting their obligations under the Banking Executive Accountability Regime.

The prudential standards will sometimes set down quite particular responsibilities for the board. For example, the board may be assigned specific responsibility for a matter. This means that the board is expected to be ultimately accountable, and to remain in a position where it can justify the actions and decisions of the institution in relation to that matter. In other cases, the standards may require the board to ensure that a particular matter is

addressed or action is taken. This means that the board should take all reasonable steps and make all appropriate enquiries so that the board can determine, to the best of its knowledge, that the stated matter has been properly addressed. At other times, the standards may require the board to set, approve or review a policy or oversee particular work undertaken by management.

What are the key areas where APRA's prudential standards impose requirements on boards?

Adequate financial strength, robust risk management and sound governance are critical to ensuring the promises made to depositors are met within a safe, efficient and competitive financial system.

Robust risk management, which incorporates both a framework for risk measurement and controls and a healthy risk culture, helps reduce the likelihood of a damaging incident or an ill-conceived business strategy that might impair the financial health of a regulated institution. Adequate financial strength ensures that, when unexpected losses are incurred, the institution has the financial capacity and resilience to continue without its ability to meet its promises to depositors being compromised. Sound governance provides oversight of these critical aspects of an institution's operations, and ensures they are maintained in the face of ever-changing strategic, competitive and environmental pressures.

APRA's general philosophy is to allow regulated institutions the freedom to conduct their affairs as they see fit, provided they can demonstrate sound governance arrangements, robust risk management capabilities and adequate financial strength. Unsurprisingly, therefore, the prudential standards give considerable attention to governance, risk management and financial resilience and in particular the role of the board in each of these areas.

Financial resilience

Adequate financial resilience and sound financial management are fundamental to the ongoing health of an ADI. In particular, it is vital that adequate capital is maintained against the risks associated with its activities and that the minimum requirements in this respect as set down in the prudential standards are met. The board is responsible for ensuring that appropriate financial and capital management policies are established, and for effective oversight of management's implementation of these policies.

As an example, under the prudential standards capital is managed in a formal sense through the Internal Capital Adequacy Assessment Process (ICAAP). Through the ICAAP, the board sets the capital management strategy and key capital targets. In doing this, the board is expected to satisfy itself that the institution's capital targets are consistent with its risk appetite, including its tolerance for potential breaches of regulatory capital requirements, and to have a robust understanding of how the institution's balance sheet would respond to various stresses.

The board is expected to be actively engaged in the development, finalisation and review of the ICAAP and to be in a position to robustly challenge the assumptions and methodologies behind the ICAAP and the associated documentation. However, management – supported by

external advice if needed - would normally provide all the analysis and support needed by the board.

An institution's ICAAP must be approved by the board whenever significant changes are made. The board is also expected to oversee the ongoing implementation of the ICAAP and satisfy itself that the necessary supporting processes are established and operating effectively.

Governance

Good governance is critical to the long-term viability of any company. APRA's prudential standards require that ADIs have a rigorous governance framework, founded on the premise that a well-governed institution is an important source of protection for the interests of depositors. Prudential standards cover the following in particular:

- composition of the board (including board renewal);
- conflicts of interest;
- fitness and propriety; and
- remuneration of senior management and other key staff.

They also cover matters such as board committee composition and board performance.

Within a group of companies, there can be more than one APRA-regulated institution. Sometimes these will be in the same industry segment e.g. a domestic bank owned by an overseas parent bank and sometimes they will straddle more than one industry segment (e.g. banking and life insurance). In such cases, a subsidiary within a financial group is often asked to work with group policies and align themselves with other operational processes, from their parent company. APRA acknowledges this can be entirely appropriate and indeed may add strength to the oversight and control framework. However, the board of an APRA-regulated institution that is asked to adopt a group policy cannot abrogate its regulatory responsibilities. It must still satisfy itself that the group's policy is 'fit for purpose', i.e. it is appropriate for the institution and will meet all regulatory requirements for that institution.

Risk management

Significant financial and other risks are inherent in the business models of financial institutions. Robust risk management therefore lies at the heart of the prudent management of an APRA-regulated institution. APRA's prudential standards expect that the nature of all the institution's material activities and risks are known and well-understood, and that there are robust structures for the management and reporting of those risks.

The prudential standards make it clear that the board must oversee, and is ultimately responsible for, the establishment and maintenance of an effective risk management framework.[4] The board is expected to provide clear direction and leadership for the institution

[4] APRA defines the risk management framework as 'the totality of systems, structures, policies, processes and people within an APRA-regulated institution that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk'.

in its approach to risk management. Amongst other things, this includes setting a clearly articulated risk appetite so that the boundaries within which management may operate are clear.[5] It also involves overseeing the implementation and ongoing operation of a robust and effective risk management strategy that seeks to ensure the institution remains within that appetite.

No control framework will be truly effective if an institution's culture is not appropriately aligned to it. The board therefore has a very important task in this respect: it needs to form a view of the risk culture in the institution[6], and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes.

What sort of engagement does APRA expect to have with boards?

APRA interacts with regulated institutions at various levels and with varying frequencies. For many institutions, APRA will look to meet with the board at least once a year. For larger institutions, this will often be supplemented with additional discussions with the chair of the board and/or the chairs of the audit and risk committees. These meetings provide an opportunity for directors to hear directly from APRA about its views on the risk profile of the institution and for APRA to better understand the board's thinking, priorities and approach. They also afford the board an opportunity to raise matters directly with APRA.

APRA seeks to have an open and constructive relationship with the board. It also seeks the board's assistance in ensuring management maintain an open and candid relationship with APRA and that information of prudential concern is promptly communicated. Certain individuals (such as auditors and actuaries) also have statutory obligations to report information to APRA in some circumstances.

APRA seeks to work with the boards and management of institutions as they take appropriate steps to address issues. Accordingly, when APRA makes supervisory interventions, they are proportionate to the outcomes desired and may range from making recommendations or suggestions through to imposing requirements or taking enforcement action when issues are more serious or not being adequately addressed in a timely manner.

As APRA undertakes its prudential activities – particularly those that involve having supervisors spending time on-site within a regulated institution – it will often send a written report outlining the findings of the review to the institution. Depending on the nature of the findings these may be sent to the Chair or the Chief Executive, but regardless it is expected that the reports would be tabled at the next available board meeting so that the board is aware of the issues raised. The board should pay particular attention to any requirements set down by APRA in these reports. There typically will be various other formal communications

[5] The risk appetite is captured in a formal risk appetite statement. Amongst other things, this must convey the degree of risk that the institution is prepared to accept in pursuit of its strategic objectives and business plan, giving consideration to the interests of depositors and/or policyholders.

[6] Risk culture refers to 'the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risks.' Institute of International Finance (2009) "Reform in the Financial Services Industry: Strengthening Practices for a More Stable System".

with an institution, and the Chief Executive Officer is expected to exercise discretion in deciding which of these will be referred to the board.

As with legal requirements more generally, boards are expected to satisfy themselves that appropriate processes are in place to respond to issues raised by APRA, and that where remedial action is needed it is undertaken in a timely manner.

Chapter 2 - Financial resilience

Financial resilience

This chapter sets out the specific obligations that apply to directors in respect to financial resilience. In simple terms, the key requirements are:

- Capital adequacy: The Board must ensure the ADI maintains an appropriate level and quality of capital commensurate with the type, amount and concentration of risks to which the ADI is exposed.
- Liquidity: An ADI must maintain an adequate level of liquidity to meet its obligations as they fall due across a wide range of operating circumstances.

2.1 APS 110 Capital Adequacy (2023)

Board oversight[7]

12. The Board of an ADI must ensure that the ADI maintains a level and quality of capital commensurate with the type, amount and concentration of risks to which the ADI is exposed from its activities.[8] In doing so, the Board must have regard to any prospective changes in the ADI's risk profile and capital holdings. (APS 110, paragraph 12)

13. An ADI that is a member of a group may be exposed to risks, including reputational and contagion risk, through its association with other members of the group. Problems arising in other group members may compromise the financial and operational position of the ADI. The Board, in determining the capital adequacy of the ADI at Level 1, must have regard to:

    (a) risks posed to the ADI by other members of the group, including the impact on the ability of the ADI to raise funding and additional capital should the need arise;

    (b) obligations, both direct and indirect, arising from the ADI's association with group members that could give rise to a call on the capital of the ADI; and

    (c) the ability to freely transfer capital (including situations where the group is under financial or other forms of stress) from members of the group to recapitalise the ADI or other members of the group. This includes consideration of:

[7] Ensure when used in relation to a responsibility of the Board, means to take all reasonable steps and make all reasonable enquiries as are appropriate for a board so that the board can determine, to the best of its knowledge, that the stated matter has been properly addressed (*Prudential Standard APS 001 Definitions*).

[8] Unless otherwise indicated, a reference to the Board of an ADI in this Prudential Standard is also a reference, where relevant, to the Board of the entity that heads the Level 2 group.

(i) the integration of business operations within the group;

(ii) the importance of members of the group to the group;

(iii) the impact of cross-border jurisdictional issues;

(iv) differences in legislative and regulatory requirements that may apply to group members; and

(v) the impact of taxation and other factors on the ability to realise investments in, or transfer surplus capital from, group members. (APS 110, paragraph 13)

APG 110

1. APS 110 sets out APRA's requirements for capital adequacy for ADIs. Under APS 110, ADIs must maintain adequate capital for the risks associated with their activities. The ultimate responsibility for the prudent management of capital rests with the ADI's Board. (APG 110, paragraph 1)

30. A prudent ADI would, however, adopt a cautious approach to capital distributions during a period of stress even if it is operating above these levels. The Board of a prudent ADI would typically consider moderating dividend payout ratios, and considering the use of dividend reinvestment plans and other capital management initiatives to reinforce capital positions.[9] (APG 110, paragraph 30)

CPG 110

1. Under the capital standards, the Board of a regulated institution has primary responsibility for the capital management of that institution. This obligation goes beyond the need to ensure compliance with regulatory capital requirements and requires the Board to ensure that each regulated institution holds capital resources commensurate with its risk profile. (CPG 110, paragraph 1)

3. While the ICAAP may be developed by the regulated institution's senior management with input from relevant areas and experts across the organisation (including the Appointed Actuary where relevant), the capital standards require the Board to be actively engaged in the development and finalisation of the ICAAP and the oversight of its implementation on an ongoing basis. (CPG 110, paragraph 3)

4. APRA expects the Board to robustly challenge the assumptions and methodologies behind the ICAAP and the associated documentation. APRA expects the Board to understand and to be able to explain the key aspects of the ICAAP and why it is considered appropriate for the institution. (CPG 110, paragraph 4)

6. The Board is responsible for the risk appetite of a regulated institution and for ensuring that the institution has an appropriate risk management framework. Risk appetite is a

[9] APRA may impose restrictions on capital distributions even where an ADI's CET 1 ratio is above the buffer range, under APS 110 (Attachment B, paragraph 4).

fundamental part of both risk management and capital management. (CPG 110, paragraph 6)

13. Under the capital standards, the ICAAP of a regulated institution must be appropriate for its size, business mix and complexity. Each institution's ICAAP will be tailored to the circumstances of the institution. For more complex institutions, appropriately sophisticated processes are expected; for simpler institutions with limited product offerings and simple investment structures, simplified approaches may suffice. The complexity or otherwise of an institution's ICAAP will be expected to reflect the Board's and senior management's view of the institution's functional complexity. (CPG 110, paragraph 13)

20. APRA expects that the Board will satisfy itself that the capital targets are in line with the risk appetite. This will include consideration of the Board's appetite for potential breaches of regulatory capital requirements. (CPG 110, paragraph 20)

25. To avert capital falling below target operating levels and, in the most severe case, breaching regulatory requirements, an institution is required under the capital standards to have capital triggers in place. These triggers are intended to serve as early warning indicators and thereby provide the Board and senior management with time to rectify problems and restore capital while the institution continues to operate. (CPG 110, paragraph 25)

41. An ICAAP summary statement is a high-level document that describes and summarises the capital assessment and management processes of the regulated institution. It serves as a roadmap to the ICAAP that allows the Board and APRA to understand the capital management processes of the institution. APRA anticipates that the ICAAP summary statement will refer to other policies and procedures, but will be relatively self-contained. (CPG 110, paragraph 41)

Board approval

14. An ADI must have an Internal Capital Adequacy Assessment Process (ICAAP) that must be:

    (a) adequately documented, with the documentation made available to APRA on request; and

    (b) approved by the ADI's Board initially, and when significant changes are made. (APS 110, paragraph 14)[10]

16. An ADI that is part of a group may rely on the ICAAP of the group provided that the Board of the ADI is satisfied that the group ICAAP meets the criteria in paragraph 17 of this Prudential Standard in respect of the ADI (APS 110, paragraph 16).

[10] Minimum requirements for the ICAAP are set out at APS 110 paragraph 17.

22. The ICAAP report submitted to APRA by the ADI must be accompanied by a declaration approved by the Board and signed by the Chief Executive Officer (CEO) stating whether:

    (a) capital management has been undertaken by the ADI in accordance with the ICAAP over the period and, if not, a description of, and explanation for, deviations;

    (b) the ADI has assessed the capital targets contained in its ICAAP to be adequate given the size, business mix and complexity of its operations and, at Level 2, given the location of operations of group members and the complexity of the group structure; and

    (c) the information included in the ICAAP report is accurate in all material respects. (APS 110, paragraph 22)[11]

APG 110

24. An ADI that is operating with capital ratios in the regulatory capital buffer range, or that expects to do so, would agree a capital restoration path back out of the range with APRA. To support this, a prudent ADI would provide capital projections, based on a range of scenarios and approved by the Board, to APRA. (APG 110, paragraph 24)

CPG 110

2. Consistent with that overarching responsibility, the capital standards require each regulated institution to have an ICAAP that has been approved by its Board. (CPG 110, paragraph 2)

16. Under the capital standards, a regulated institution may make use of a group ICAAP or components of that ICAAP. In doing so, the Board of each regulated institution in the group is still required to ensure that the ICAAP is appropriate and meets the requirements of the capital standards in relation to the institution. (CPG 110, paragraph 16)

Information for the Board

17. The ICAAP must include at a minimum: processes for reporting on the ICAAP and its outcomes to the Board and senior management of the ADI, and for ensuring that the ICAAP is taken into account in making business decisions. (APS 110, paragraph 17(e))

18. The ICAAP summary statement is a high-level document that describes and summarises the capital assessment and management processes of the ADI. It must address the aspects of the ICAAP listed in paragraphs 17(a) to 17(f) of this Prudential Standard, and also include: a summary of the ADI's policy for reviewing its ICAAP, including who is responsible for the review, details of the frequency and scope of the review, and mechanisms for reporting on the review and its outcomes to the Board and senior management. (APS 110, paragraph 18(d))

[11] Under APS 110, paragraph 20, An ADI must, on an annual basis, prepare a report on the implementation of its ICAAP (ICAAP report). A copy of the ICAAP report must be provided to APRA no later than three months from the end of the period covered by that report.

CPG 110

17. A regulated institution's ICAAP will include a range of processes and systems for assessing capital requirements relative to the risks to which the institution is exposed, setting target capital levels, projecting and monitoring the capital position, taking action if capital levels fall below target levels, and reporting on the process and its outcomes to the Board. These underlying processes will ordinarily be documented in various policies and procedural documents. (CPG 110, paragraph 17)

33. The capital standards require a regulated institution to include stress testing and scenario analysis in its ICAAP. Stress testing and scenario analysis can assist in the formulation of capital targets and trigger levels by: being readily understandable to the Board and senior management. (CPG 110, paragraph 33(f))

40. APRA expects that a regulated institution will have in place processes to report the outcomes of the review to the Board and senior management, as well as processes to assess and respond to any recommendations for change arising out of the review. (CPG 110, paragraph 40)

2.2 APS 111 Measurement of Capital (2023)

Board approval

B.1. To be classified as paid-up ordinary shares in Common Equity Tier 1 Capital, an instrument must satisfy the following criteria: the instrument is only issued with the approval of the owners of the issuer, either given directly by the owners or, if permitted by applicable law, given by the Board or by other persons duly authorised by the owners. (APS 111, Attachment B, paragraph 1(m))

Information for the Board

A.5. An ADI's systems and controls used for valuation purposes must: provide for the Board to receive reports from senior management on the valuation oversight and valuation performance issues that are notified to senior management for resolution, as well as all significant changes in valuation policies, methodologies and adjustments; and explicitly assess valuation uncertainties and ensure that assessments of material valuation uncertainties are included in the information provided to the Board and senior management. (APS 111, Attachment A, paragraphs 5(c) and 5(i))

2.3 APS 113 Capital Adequacy: Internal Ratings-based Approach to Credit Risk (2023)

Board oversight

APG 113

D.1. APRA expects an ADI seeking approval to use an internal ratings-based (IRB) approach for regulatory capital purposes to demonstrate that the:

(a) use of risk-based capital and associated risk-adjusted performance measurement permeates the management of its business; and

(b) Board and senior management are willing and able to incorporate the quantification of risk into management processes and decision-making.[12] (APG 113, Attachment D.1)

Board approval

20. All material aspects of an ADI's rating and estimation processes must be approved by the ADI's Board, or relevant Board committee, and senior management. Those parties must possess a general understanding of the ADI's rating systems and a detailed understanding of the associated management reports. Senior management must notify the Board, or Board committee, of material changes or exceptions from established policies that could have a material impact on the ADI's rating systems. (APS 113, paragraph 20)

23. An ADI must have documented policies that detail sound rating system development, validation, implementation, governance and control processes. These policies must: be approved and actively discussed by the ADI's Board or a delegated committee. (APS 113, paragraph 23(a))

Information for the Board

22. Internal ratings must be an essential part of the reporting to the Board and senior management. Reporting must include:

    (a) risk profile by grade;

    (b) migration across borrower grades;

    (c) quantitative estimates of the relevant parameters for each borrower grade and, where relevant, facility grade; and

    (d) comparison of realised default rates (and, where relevant, realised loss given default (LGD) and exposure at default (EAD) rates) against expectations.

    Reporting frequencies may vary with the significance and type of information and the level of the recipients. (APS 113, paragraph 22)

APG 113

3. APS 113 (paragraphs 20-23) details requirements relating to the role of the Board in the governance and oversight of an ADI's rating systems and risk estimates. Information provided to the Board for this purpose should be sufficient to enable directors to actively discuss and confirm, at least annually, the continuing appropriateness, effectiveness

[12] See also: APG 113, Attachment D, Table 10. Elements of a qualifying management system

and integrity of the rating systems and risk estimates. Such information would generally include reporting from risk management as well as internal audit. (APG 113, paragraph 3)

9. On an annual basis, the internal audit function would usually collate audit findings relevant to APS 113 to provide a holistic view of the effectiveness of the ADI's rating systems and risk estimates for relevant stakeholders, including the Board and senior management. This would include a summary of audit reviews, action plans and the status of audit findings. APRA expects that material issues would be promptly escalated by internal audit and rectified by the ADI. (APG 113, paragraph 9)

D.4. APRA expects an ADI's formal application for IRB approval to contain the information in Table 11. To the extent possible, supporting documentation contained in an ADI's formal IRB application would have been developed for internal purposes rather than IRB approval. Any summary documents requested by APRA are intended to be tools aimed at guiding APRA to the appropriate source documents such as policies, internal reports and Board briefing material. APRA expects the ADI to use cross-referencing extensively to avoid undue repetition or duplication in the documentation.[13] (APG 113, Attachment D.4.)

2.4 APS 116 Capital Adequacy: Market Risk (2023)

Board oversight

A.2. In particular, the Board, or a Board committee, must ensure that the ADI has in place adequate systems to identify, measure and manage market risk, including identifying responsibilities, providing adequate separation of duties and avoiding conflicts of interest. An ADI must inform APRA of all significant changes in these systems and in its market risk profile and must ensure that market risk capital requirements are met on a continuous basis and that intra-day exposures are not excessive. (APS 116, Attachment A, paragraph 2)

C.11. The Board, or a Board committee, and senior management of an ADI must be actively involved in the risk control process and must treat risk control as an essential aspect of the business, to which significant resources need to be devoted. The daily reports prepared by the independent risk control unit must be reviewed by a level of management with sufficient seniority and authority to enforce both reductions of positions taken by individual traders and reductions in the ADI's overall risk exposure. (APS 116, Attachment C, paragraph 11)

Board approval

A.1. An ADI's Board is responsible for approving strategies and policies with respect to market risk and ensuring that senior management takes the steps necessary to monitor and control these risks. (APS 116, Attachment A, paragraph 1)

[13] See also: APG 113, Attachment D, Table 11. IRB application documentation.

Information for the Board

C.14. An ADI must have a routine and robust program of stress testing as a supplement to the risk analysis based on the day-to-day output of the risk measurement model. The results of stress testing exercises must be used in the internal assessment of capital adequacy and reflected in the policies and limits set by management and the Board, or Board committee. The results of stress testing must be routinely communicated to senior management and, periodically, to the ADI's Board, or a Board committee. (APS 116, Attachment C, paragraph 14)

C.40. An ADI must ensure that the results of the stress tests are reviewed periodically by senior management and reflected in the policies and limits set by management and the Board, or Board committee. (APS 116, Attachment C, paragraph 40)

2.5 APS 117 Capital Adequacy: Interest Rate Risk in the Banking Book (Advanced ADIs) (2013)

Board oversight

22. An ADI with internal model approval must have in place an Interest Rate Risk in the Banking Book (IRRBB) management framework that is sufficiently robust to facilitate quantitative estimates of its IRRBB capital requirement that are sound, relevant and verifiable. APRA must be satisfied that the ADI's IRRBB management framework is suitably rigorous and consistent with the complexity of its business. Where industry risk modelling practices evolve and improve over time, the ADI must consider these developments in assessing its own practices. Furthermore, the IRRBB measurement system must play an integral role in the ADI's risk management and decision-making processes and meet the requirements detailed in Attachment A. An ADI must also comply with the requirements relating to the Board and senior management responsibilities in that Attachment. (APS 117, paragraph 22)

A.1. An ADI's Board is responsible for the overall IRRBB profile of the ADI and its IRRBB management framework. Accordingly, the Board must make clear its appetite for this risk, including IRRBB exposure limits. The Board or a Board committee must be actively involved in the oversight of the ADI's approach to managing and measuring IRRBB. (APS 117, Attachment A, paragraph 1)

A.3. To ensure the continued effectiveness of the IRRBB management framework, the Board, or Board committee, must ensure the framework is subject to periodic validation and review (refer to paragraphs 18 and 19 of this Attachment) by a suitable independent party. (APS 117, Attachment A, paragraph 3)

Board approval

A.2. An ADI's IRRBB management framework must be approved by the Board, or a Board committee. In the latter case, the committee must have clearly defined responsibilities, thresholds for reporting to the Board and performance obligations. The approved framework must clearly articulate respective responsibilities and reporting relationships. (APS 117, Attachment A, paragraph 2)

Information for the Board

A.4. An ADI's Board, or Board committee, must review IRRBB management reports (refer to paragraphs 13 to 15 of this Attachment) on a regular basis and satisfy itself that this risk is appropriately managed. (APS 117, Attachment A, paragraph 4)

A.7. Senior management must, in conjunction with the IRRBB management function referred to in paragraph 6 of this Attachment, develop appropriate policies relating to the risk management framework. Management is responsible for translating these policies into specific procedures and processes to facilitate implementation and verification within the ADI's business operations. Senior management must provide notice to the Board, or Board committee, of material changes or exceptions from established policies that could have an impact on the operation of the IRRBB management framework, including the IRRBB capital requirement. (APS 117, Attachment A, paragraph 7)

A.13. An ADI must implement a process to regularly monitor its IRRBB profile. To support the proactive management of this risk, there must be regular reporting of relevant information to the Board, or Board committee, and senior management. (APS 117, Attachment A, paragraph 13)

A.15. An ADI must have in place a process for ensuring that the ADI's Board, or Board committee, and senior management are able to respond appropriately to the information contained in IRRBB management reports. This process must include escalation procedures for key IRRBB issues to facilitate appropriate action between formal reporting cycles. (APS 117, Attachment A, paragraph 15)

B.27. An ADI's policies and limits must reflect the results of stress-testing exercises and these results must be communicated to relevant senior management and the ADI's Board, or Board committee, on a regular basis. (APS 117, Attachment B, paragraph 27)

APG 117

20. Attachment A to APS 117 states that an ADI's Board of directors, or committee thereof, must review on a regular basis IRRBB management reports and satisfy itself that this risk is being appropriately managed. As good practice, APRA envisages that such reviews would occur on at least a quarterly basis. (APG 117, paragraph 20)

2.6 APS 180 Capital Adequacy: Counterparty Credit Risk (2023)

Information for the Board

B.30. An ADI must establish a process for monitoring by, and regular reporting to, senior management of all of its exposures to central counterparties (CCPs), including exposures arising from trading through a CCP and exposures arising from CCP membership obligations such as default fund contributions. An ADI must also establish a process for regular reporting of material exposures to CCPs to the appropriate committee of the Board. (APS 180, Attachment B, paragraph 30)

2.7 APS 210 Liquidity (2023)

Board oversight

15. An ADI's Board is ultimately responsible for the sound and prudent management of the liquidity risk of the ADI. An ADI must maintain a liquidity risk management framework commensurate with the level and extent of liquidity risk to which the ADI is exposed from its activities. In relation to a foreign ADI, the responsibilities of the Board in this Prudential Standard are to be fulfilled by the senior officer outside Australia.[14] (APS 210, paragraph 15)

17. The Board must ensure that:

    (a) senior management and other relevant personnel have the necessary experience to manage liquidity risk; and

    (b) the ADI's liquidity risk management framework and liquidity risk management practices are documented and reviewed at least annually. (APS 210, paragraph 17)

20. Senior management and the Board must be able to demonstrate a thorough understanding of the links between funding liquidity risk (the risk that an ADI may not be able to meet its financial obligations as they fall due) and market liquidity risk (the risk that liquidity in financial markets, such as the market for debt securities, may reduce significantly), as well as how other risks, including credit, market, operational and reputation risks, affect the ADI's overall liquidity risk management strategy. (APS 210, paragraph 20)

23. In setting the liquidity risk tolerance, the Board and senior management must ensure that the risk tolerance allows the ADI to effectively manage its liquidity position in such a way that it is able to withstand a prolonged period of stress. (APS 210, paragraph 23)

APG 210

4. An ADI is expected to take into account its business objectives and strategic direction with the aim of achieving certain budgetary and financial performance outcomes. Critical to this process is the Board's risk tolerance, which informs the acceptability of risks, including liquidity risk, associated with planned business activities. The risk tolerance will generally also reflect the ADI's financial condition and funding capacity as well as its role in the financial system. (APG 210, paragraph 4)

Board approval

16. The liquidity risk management framework must include, at a minimum:

    (a) a statement of the ADI's liquidity risk tolerance, approved by the Board;

[14] As per APS 001, the senior officer outside Australia is the senior nominated officer of a foreign ADI (whether a director or senior executive) outside Australia with delegated authority from the Board to be responsible for overseeing the Australian branch operation.

(b) the liquidity management strategy and policy of the ADI, approved by the Board;

(c) the ADI's operating standards (e.g. in the form of policies, procedures and controls) for identifying, measuring, monitoring and controlling its liquidity risk in accordance with its liquidity risk tolerance;

(d) the ADI's funding strategy, approved by the Board; and

(e) a contingency funding plan. (APS 210, paragraph 16)

45. The funding strategy must be reviewed and approved by the Board, at least annually, and supported by robust assumptions in line with the ADI's liquidity management strategy and business objectives. (APS 210, paragraph 45)

51. An ADI's contingency funding plan must be reviewed and tested, at least annually, to ensure its effectiveness and operational feasibility. An ADI's Board must review and approve the contingency funding plan, at least annually, or more often as changing business or market circumstances require. (APS 210, paragraph 51)

A.20 In the case of unforeseen changes in circumstances, an ADI may apply to APRA, at any time, for a change in the amount of its Committed Liquidity Facility (CLF) to be recognised for Liquidity Coverage Ratio (LCR) purposes by submitting an updated Board-approved funding and liquidity plan. (APS 210, Attachment A, paragraph 20)

APG 210

1. An ADI's liquidity risk tolerance defines the level of liquidity risk that the ADI is willing to assume. APS 210 requires that the liquidity risk tolerance be set by the Board and that it is documented and appropriate for an ADI's operations and strategy and its role in the financial system. (APG 210, paragraph 1)

2. The Board-approved risk appetite statement will normally include an articulation of liquidity risk appetite and identify its liquidity risk tolerance. (APG 210, paragraph 2)

50. The Board-approved funding strategy will generally include both qualitative and quantitative items, key outcomes and the strategies that will be used to achieve the outcomes. The funding strategy would combine expected funding outcomes with sensitivity analysis. The strategy would include the base-case balance sheet projection, consistent with an ADI's medium-term business plan, that represents the ADI's best estimate of its future funding needs and sources, as well as key sensitivities in the base case. (APG 210, paragraph 50)

Information for the Board

18. The Board must review regular reports on the liquidity position of the ADI and, where necessary, information on new or emerging liquidity risks. (APS 210, paragraph 18)

19. An ADI's senior management must, at a minimum: develop a liquidity management strategy, policies and processes in accordance with the Board-approved liquidity tolerance; establish a set of reporting criteria specifying the scope, manner and frequency of reporting for various recipients (such as the Board, senior management and

the asset/liability committee) including the parties responsible for preparing the reports; and continuously review information on the ADI's liquidity developments and report to the Board on a regular basis. (APS 210, paragraph 19 (a), (f) and (i))

33. An ADI must have adequate policies, procedures and controls in place to ensure that the Board and senior management are informed immediately of new and emerging liquidity concerns. These include increasing funding costs or concentrations, increases in any funding requirements, the lack of availability of alternative sources of liquidity, material and/or persistent breaches of limits, a significant decline in the cushion of unencumbered liquid assets or changes in external market conditions that could signal future difficulties. (APS 210, paragraph 33)

40. An ADI must have a reliable management information system (MIS) that provides the Board, senior management and other appropriate personnel with timely and forward-looking information on the liquidity position of the ADI. (APS 210, paragraph 40)

65. An LCR ADI's stress test scenarios and related assumptions must be well documented and reviewed together with the stress test results. Stress test results and vulnerabilities and any resulting actions must be reported to, and discussed with, the Board and APRA. Results of the stress tests must be integrated into the ADI's strategic planning process and its day-to-day risk management practices. The results of the stress tests must be explicitly considered in the setting of internal limits. (APS 210, paragraph 65)

2.8 APS 120 Securitisation (2023)

Board oversight

16. In a securitisation, an originating ADI must not:

    (d) allow any of the ADI's directors, officers or employees to sit on the Board of an special purpose vehicle (SPV), or on the Board of a trustee of an SPV, unless the Board has at least four members. The ADI, however, may be represented by one director on a Board of four to six directors and by no more than two directors on a Board of seven or more directors; or

    (e) act, or allow any of its directors, officers or employees to act, in any circumstances as a trustee of an SPV, or in any similar role. The trustee must not be part of the group, as defined in Australian Accounting Standards, to which the ADI belongs. (APS 120, paragraph 16(d) and 16(e))

APG 120

60. APS 120 requires that an ADI must not provide, or knowingly allow the perception to arise that it will provide, support to a securitisation in excess of the ADI's explicit contractual obligations. To do so would be to provide implicit support. In addition, the Board of directors and senior management must put policies and procedures in place that outline how the ADI will ensure it is not providing implicit support for a securitisation. (APG 120, paragraph 60)

66. APS 120 provides that, in certain circumstances, APRA may impose quantitative or qualitative limits on an ADI's securitisation activities. Such restrictions could include prohibiting an ADI from undertaking further securitisation activity until the Board of directors and senior management of the ADI can establish they have an appropriate understanding of the ADI's securitisation structures, activities and exposures (APG 120, paragraph 66)

2.9 APS 121 Covered Bonds (2023)

Board oversight

12. The Board and senior management of an issuing ADI must establish and implement policies and procedures relating to:

    (a) decisions to issue covered bonds and the structuring of covered bond issuance;

    (b) the ADI's dealings with covered bond special purpose vehicles (including cover pools); and

    (c) the management of exposures involved in the issuance of covered bonds. (APS 121, paragraph 12)

Chapter 3 - Risk management

Risk management

This chapter sets out the specific obligations that apply to directors in respect to risk management.

- Risk management: An ADI must maintain a risk management framework that is appropriate to the size, business mix and complexity of the institution or group (CPS 220 summary box).

3.1 CPS 220 Risk management (2019)

Board oversight

9. The Board[15] of an APRA-regulated institution is ultimately responsible for the institution's risk management framework and is responsible for the oversight of its operation by management. In particular, the Board must ensure that:

   (a) it sets the risk appetite within which it expects management to operate and approves the institution's risk appetite statement and risk management strategy (RMS);

   (b) it forms a view of the risk culture in the institution, and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensures the institution takes steps to address those changes;

   (c) senior management of the institution monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the Board;

   (d) the operational structure of the institution facilitates effective risk management;

   (e) policies and processes are developed for risk-taking that are consistent with the RMS and the established risk appetite;

   (f) sufficient resources are dedicated to risk management; and

   (g) it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk. (CPS 220, paragraph 9)

[15] A reference to the Board in the case of a foreign ADI, is a reference to the senior officer outside Australia.

10. An APRA-regulated institution that is part of a group or other corporate group may meet requirements of this Prudential Standard using group risk management frameworks, policies, procedures or functions, provided that the Board of the institution is satisfied that the requirements are met in respect of that institution. (CPS 220, paragraph 10)

14. As part of the group risk management framework (see paragraphs 19 to 25), the Head of a group must maintain processes to coordinate the identification, measurement, evaluation, monitoring, reporting, and controlling or mitigation of all material risks across the group, in normal times and periods of stress. The Head of a group must ensure its Board has a comprehensive group-wide view of all material risks, including an understanding of the roles and relationships of subsidiaries to one another and to the Head of a group. (CPS 220, paragraph 14)

19. An APRA-regulated institution must maintain a risk management framework for the institution that enables it to appropriately develop and implement strategies, policies, procedures and controls to manage different types of material risks, and provides the Board with a comprehensive institution-wide view of material risks. (CPS 220, paragraph 19)

CPG 220

9. In order to be effective, risk management functions would have:

   (a) adequately experienced staff with relevant technical knowledge who facilitate the development, ongoing review and validation of the risk management framework; and

   (b) appropriate seniority and authority, with access to the responsible board committees. (CPG 220, paragraph 9)

15. Under CPS 220, the Board is ultimately responsible for the risk management framework of the APRA-regulated institution and is responsible for the oversight of its operation by management. An institution must have, at all times, a risk management framework that governs the way the institution manages risks arising in the institution. Together, the Board Risk Committee and Board Audit Committee assist the Board in its oversight of the operation by management of the overall risk management framework. (CPG 220, paragraph 15)

16. The Board Audit Committee assists the Board to fulfil its corporate governance and oversight responsibilities in relation to an entity's financial reporting, internal control system, risk management framework and internal and external audit functions (i.e. independent assurance). (CPG 220, paragraph 16)

19. The Board approval and oversight responsibilities for the risk management framework are unaffected if risk management and business operations are outsourced to a third party or are performed by another part of a group. (CPG 220, paragraph 19)

20. In determining whether the Board has met its responsibilities under CPS 220, APRA will assess the steps taken by the Board to ensure it meets those responsibilities. For example, APRA expects senior management to report on the material risks and escalate material risk issues to the Board or the Board Risk Committee level. The Board and/or Board Risk Committee could also obtain independent views and reports as they deem

appropriate, as well as consider risk issues escalated from the risk management function. APRA expects that the Board would clearly communicate its expectations in respect of the reporting and escalation to be provided by management, the risk management function(s) and internal audit. Where the Board considers that the risk reporting is ineffective or that material risk issues have failed to be escalated, APRA expects the Board to adopt all appropriate measures (including directions for management remedial actions and reports) to identify and address the reasons for the failure. (CPG 220, paragraph 20)

21. CPS 220 requires a Board to ensure that they form a view of the risk culture in the institution and the extent to which that culture supports the ability of the institution to operate consistently within its risk appetite, identify any desirable changes to the risk culture and ensure the institution takes steps to address those changes. APRA's view is that a sound risk culture is a core element of an effective risk management framework. Risk culture refers 'the norms of behaviour for individuals and groups within an organisation that determine the collective ability to identify, understand, openly discuss and act on the organisation's current and future risk'.[16] APRA expects that the Board would have a view of the risk culture that is appropriate for ensuring that the institution operates within the risk appetite. (CPG 220, paragraph 21)

22. An institution's risk culture is strongly influenced by the 'tone at the top'. APRA expects the Board and senior management to demonstrate their commitment to risk management and foster a sound risk management environment in which staff will be actively engaged with risk management processes and outcomes, and a risk management function that is influential and respected. The development of the risk culture is likely to occur through an iterative process involving both the Board and senior management. (CPG 220, paragraph 22)

27. CPS 220 allows an APRA-regulated institution that is part of a group to meet the requirements of the standard on a group basis provided that the Board of the institution is satisfied that the requirements are met in respect to that institution. (CPG 220, paragraph 27)

34. CPS 220 requires the Board to ensure that it recognises uncertainties, limitations and assumptions attached to the measurement of each material risk. In addition to recognition of these matters by the Board, APRA expects that they would be well understood within the institution. (CPG 220, paragraph 34)

36. Stress testing, including both scenario analysis and sensitivity analysis is used to assess a range of potential impacts as a result of different material risks. Stress testing is important in considering potential changes that could occur in the external operating environment, and provides a more forward looking view of an APRA-regulated institution's risk profile. APRA expects that stress testing would be based on a combination of robust modelling and informed expert judgement, with effective senior management engagement and appropriate Board oversight. (CPG 220, paragraph 36)

---

[16] Refer to the Institute of International Finance (2009) "Reform in the financial services industry: Strengthening Practices for a More Stable System".

38. The risk management framework supports the Board and senior management in obtaining an appropriate view of the APRA-regulated institution's overall risk profile. Reporting facilitates decision-making and oversight, taking into consideration the overall structure and nature of the institution's business and different approaches to managing different material risks. In understanding the overall risk profile of the institution, specific consideration would be given to:

    (a) identifying risks throughout the institution that, in combination, may have a material impact on the institution;

    (b) understanding the interaction of material risks throughout the institution. For example, a failure in processes or systems (operational risk) may result in excess claims being paid (underwriting risk); and

    (c) risks of contagion arising from issues identified with related parties (including any non-APRA-regulated activities). (CPG 220, paragraph 38)

46. The risk appetite statement is used to communicate the Board's expectations of how much risk the APRA-regulated institution is willing to accept. APRA notes that, in practice it is likely that the risk appetite and risk appetite statement will be developed through an iterative process involving the Board and management. APRA's view is that a reasonable and easily understood risk appetite statement that aligns to the approaches used to identify, assess and manage material risk is fundamental to risk management. (CPG 220, paragraph 46)

48. The development and review of an APRA-regulated institution's risk appetite statement will generally be performed as part of the strategic and business planning process. The risk appetite statement would provide relevant information on the Board's expectations regarding the risk appetite, and would in turn be updated to reflect any changes as a result of the strategic and business planning process. (CPG 220, paragraph 48)

49. APRA expects that the Board would be actively engaged with management in developing and reviewing the risk appetite statement, and would be able to demonstrate ownership of the statement. APRA considers that this might be achieved, in part, through reporting and communication processes and structures that enable the Board and/or Board Risk Committee to:

    (a) identify the APRA-regulated institution's overall current risk profile and how this compares to its risk appetite and capital strength;

    (b) be satisfied that senior management's interpretation and application of the risk appetite and tolerances is appropriate; and

    (c) appropriately align risk appetite to the approach adopted in the risk management framework for assessing, monitoring and managing the different material risks. (CPG 220, paragraph 49)

70. CPS 220 sets out requirements for the independence of the Chief Risk Officer (CRO) and specifies roles that cannot also be performed by the CRO. CPS 220 recognises that an APRA-regulated institution may seek approval for alternative arrangements to those

required. This may be where the institution is materially constrained in appointing a CRO who is free from conflicts of interest, or for other reasons particular to that institution. APRA expects these instances normally to be limited to smaller and less complex institutions, but will consider applications from all APRA-regulated institutions, provided the applicant clearly sets out the exceptional circumstances that might warrant APRA considering the alternative proposal. Where an institution seeks an alternative arrangement under CPS 220, the Board is expected to demonstrate to APRA that it has undertaken a process to identify conflicts, has established structural oversight and controls to mitigate the additional risk and is satisfied that the risk management framework will ensure these mitigants are adhered to. APRA will assess the appropriateness of alternative arrangements on a case-by-case basis. APRA expects that the Board would take into account the following controls and other mitigating factors that manage conflicts of interests including, but not limited to:

(a) alternative sources of risk-based challenge to business lines;

(b) the resources allocated to risk management;

(c) executive level engagement in risk issues;

(d) the strength of compliance and audit mechanisms;

(e) oversight from the Board and its committees;

(f) the experience and capabilities of the other risk management function personnel; and

(g) the robustness of the regulated institution's and, where appropriate, the group's risk management framework. (CPG 220, paragraph 70)

Board approval

17. The Head of a group must maintain a Board-approved liquidity management policy for the group to adequately and consistently identify, measure, monitor, and manage its material liquidity risks. The policy must include a strategy that ensures the group has sufficient liquidity to meet its obligations as they fall due, including in stressed conditions, and outline processes to identify existing and potential constraints on the transfer of funds within the group. The Head of a group must submit to APRA a copy of its group liquidity management policy as soon as practicable, and no more than 10 business days, after Board approval. (CPS 220, paragraph 17)

27. An APRA-regulated institution must maintain an appropriate, clear and concise risk appetite statement for the institution that addresses the institution's material risks. The Board is responsible for setting the risk appetite of the institution and must approve the institution's risk appetite statement. (CPS 220, paragraph 27)

29. An APRA-regulated institution must maintain an RMS for the institution that addresses each material risk listed under paragraph 26. The RMS must be approved by the Board. (CPS 220, paragraph 29)

30. The RMS is a document that describes the strategy for managing risk and the key elements of the risk management framework that give effect to this strategy. At a minimum, an RMS must:

    (a) describe each material risk identified, and the approach to managing these risks;

    (b) list the policies and procedures dealing with risk management matters;

    (c) summarise the role and responsibilities of the risk management function;

    (d) describe the risk governance relationship between the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution with respect to the risk management framework; and

    (e) outline the approach to ensuring all persons within the institution have awareness of the risk management framework as it relates to their role and for instilling an appropriate risk culture across the institution. (CPS 220, paragraph 30)

32. The business plan must be a rolling plan of at least three years' duration that is reviewed at least annually, with the results of the review reported to the Board. The business plan must cover the entirety of the institution and be approved by the Board. (CPS 220, paragraph 32) [17]

47. The comprehensive review of the risk management framework must, at a minimum, assess whether:

    (a) the framework is implemented and effective;

    (b) it remains appropriate, taking into account the current business plan;

    (c) it remains consistent with the Board's risk appetite;

    (d) it is supported by adequate resources; and

    (e) the RMS accurately documents the key elements of the risk management framework that give effect to the strategy for managing risk. (CPS 220, paragraph 47) [18]

CPG 220

18. The Board is directly responsible for the broader strategy of the APRA-regulated institution and is required to approve the risk appetite statement, business plan and risk management strategy. Effective design of these documents and related processes by the institution will facilitate their integration, with each process appropriately supporting the others. (CPG 220, paragraph 18)

---

[17] As per, CPS 220, paragraph 31, an APRA-regulated institution must maintain a written plan for the institution that sets out its approach for the implementation of its strategic objectives (business plan).

[18] As per CPS 220, paragraph 45, a comprehensive review of the risk management framework must be conducted at least every three years by operationally independent, appropriately trained and competent persons.

61. APRA expects that a risk management strategy would contain sufficient information to communicate, in general terms the APRA-regulated institution's approach to risk management. This includes how it identifies, measures, evaluates, monitors, reports and controls or mitigates the material risks of its operations. CPS 220 requires that the risk management strategy list the policies and procedures dealing with risk management matters. Where these policies and procedures require Board approval under other prudential standards, approval of the strategy does not negate the Board's responsibility to approve those individual documents. (CPG 220, paragraph 61)

Information for the Board

25. The MIS must provide the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution with regular, accurate and timely information concerning the institution's risk profile. The MIS must be supported by a robust data framework that enables the aggregation of exposures and risk measures across business lines, prompt reporting of limit breaches, and forward-looking scenario analysis and stress testing. Data quality must be adequate for timely and accurate measurement, assessment and reporting on all material risks across the institution and must provide a sound basis for making decisions. (CPS 220, paragraph 25)

37. An APRA-regulated institution must have a designated risk management function for the institution that, at a minimum:

    (a) is responsible for assisting the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution to maintain the risk management framework;

    (d) has the necessary authority and reporting lines to the Board of the APRA-regulated institution, board committees of the APRA-regulated institution and senior management of the institution to conduct its risk management activities in an effective and independent manner;

    (g) is required to notify the Board of any significant breach of, or material deviation from, the risk management framework. (CPS 220, paragraph 37(a) 37(d) and 37(g))

40. The CRO must have a direct reporting line to the CEO, and have regular and unfettered access to the Board and the Board Risk Committee. (CPS 220, paragraph 40)

44. An APRA-regulated institution must ensure that compliance with, and the effectiveness of, the risk management framework of the institution is subject to review by internal and/or external audit at least annually. The results of this review must be reported to the institution's Board Audit Committee or the senior officer outside of Australia, as relevant. (CPS 220, paragraph 44)

45. An APRA-regulated institution must, in addition to paragraph 44, ensure that the appropriateness, effectiveness and adequacy of the institution's risk management framework are subject to a comprehensive review by operationally independent, appropriately trained and competent persons (this may include external consultants) at least every three years. The results of this review must be reported to the institution's

Board Risk Committee or the senior officer outside Australia, as relevant. (CPS 220, paragraph 45)

CPG 220

6. A key tenet of the three lines of defence model is that business management cannot abrogate its responsibility for risk management. The first line of defence is responsible for:

   (a) effective implementation of the risk management framework, including reporting and escalation of relevant information to responsible senior management, the second line of defence or as far as the board committees or the Board[19], as necessary; and

   (b) managing risk in a way that is consistent and integrated with the risk management framework. (CPG 220, paragraph 6)

8. The second line of defence comprises the specialist risk management function(s) that are functionally independent of the first line of defence. The second line of defence supports the Board and its committees by:

   (a) developing risk management policies, systems and processes to facilitate a consistent approach to the identification, assessment and management of risks;

   (b) providing specialist advice and training to the Board, board committees and first line of defence on risk-related matters;

   (c) objective review and challenge of:

      (i) the consistent and effective implementation of the risk management framework throughout the APRA-regulated institution; and

      (ii) the data and information captured as part of the risk management framework which are used in the decision-making processes within the business, in particular the completeness and appropriateness of the risk identification and analysis, ongoing effectiveness of risk controls, and prioritisation and management of action plans; and

   (d) oversight of the level of risk in the institution and its relationship to the risk appetite, and any necessary reporting and escalation to the Board or its committees. (CPG 220, paragraph 8)

11. The third line of defence comprises the function(s) that, in accordance with CPS 220, provide to the Board and its committees:

   (a) at least annually, independent assurance that the risk management framework has been complied with and is operating effectively; and

[19] For the purposes of this PPG, a reference to the Board, in the case of a foreign ADI, is a reference to the Senior Officer Outside of Australia (as applicable) as referred to in *Prudential Standard CPS 510 Governance*.

(b) at least every three years, a comprehensive review of the appropriateness, effectiveness and adequacy of the risk management framework. (CPG 220, paragraph 11)

17. Consistent with normal practice, for the purpose of discharging its responsibilities, the Board is able to obtain such recommendations and advice from board committees, external advisers and management as it considers prudent. The Board is entitled to place reasonable reliance on those inputs, provided directors approach their tasks with an enquiring mind and make an independent assessment of the matters for decision. (CPG 220, paragraph 17)

35. Risk can arise from structures that impede transparency, such as special-purpose or related structures. APRA expects that the APRA-regulated institution's operational structure and associated risks would be well understood in the institution, recognised by the Board, taken into account in the risk management framework and reported, as appropriate (including to the Board or its committees where necessary). (CPG 220, paragraph 35)

43. Fundamental to an effective risk management framework is a sound business plan that is consistent and integrated with the risk management strategy and risk appetite statement. APRA expects that the APRA-regulated institution's risk management framework will provide relevant information to senior management and the Board to facilitate their respective roles in the strategy and business planning process (e.g. areas of increased risk, changes in the environment, prioritisation and allocation of resources). APRA also expects that the relevant components of the risk management framework would be reviewed in the context of the institution's strategic and business planning processes. (CPG 220, paragraph 43)

52. An APRA-regulated institution would generally use a variety of approaches and processes to assess different material risks. An institution with the capability to use risk quantification techniques would generally use them in the setting and monitoring of its risk appetite statement. Risk quantification techniques may provide an institution with assurance that the risk does not exceed the institution's risk tolerance and/or risk capacity. These techniques may not be appropriate for all types of risk. APRA expects senior management to assess the appropriateness of such techniques before they are adopted and on an ongoing basis. APRA expects that the results of such analysis and testing would be reported to the Board and/or Board Risk Committee and be taken into account when establishing or reviewing the risk appetite statement. APRA expects the Board and/or Board Risk Committee to recognise the limitations and assumptions relating to any models used to measure components of risk that could materially affect its decision-making. (CPG 220, para 52)

62. A key role of an APRA-regulated institution's risk management function is to provide independent and objective review and challenge, oversight, monitoring and reporting in relation to material risks arising from the institution's operations. An additional responsibility is to provide technical support and assist the Board, relevant committees and senior management to fulfil their respective roles in relation to the risk management framework. (CPG 220, paragraph 62)

63. APRA expects the risk management function would also facilitate the building of risk management capabilities throughout the APRA-regulated institution by providing specialist education, training and advice to directors, senior management and staff of the institution. It would also typically facilitate the development of the Board's view of risk culture. (CPG 220, paragraph 63)

66. APRA expects the risk management function to have sufficient stature, authority and resourcing to support sound risk-based decision-making. This is reflected in the requirement in CPS 220 that the CRO must have authority to provide effective challenge to activities and decisions that may materially affect the institution's risk profile. (CPG 220, paragraph 66)

67. This can be further evidenced by a CRO who is appropriately skilled, unencumbered by conflicts of interest with their risk management role and can speak with candour to the CEO, the Board and relevant committees. Under a three lines of defence model, the role and responsibilities of the CRO are clearly within the second line. (CPG 220, paragraph 67)

71. CPS 220 requires that the risk management function, via a CRO, has direct and unfettered access to the CEO, Board, Board Risk Committee and senior management. CPS 220 also requires the reporting line for the risk management function to be independent from business lines and to directly report to the CEO. Where an APRA-regulated institution is part of a group, including a Level 2 and/or Level 3 group, the CRO of that institution may report to the group CRO as long as the group CRO reports directly to the group CEO. (CPG 220, paragraph 71)

77. APRA expects an APRA-regulated institution's risk management framework to ensure that the Board and senior management receive regular, concise and meaningful assessment of actual risks relative to the institution's risk appetite and the operation and effectiveness of controls. (CPG 220, paragraph 77)

84. APRA will accept annual reviews that explore particular elements of the risk management framework in depth and on a rotational basis. For example, if an institution's risk management framework has six material elements, it may choose to review two of these every year. The structure of such a program of review is at the discretion of the regulated institution. The annual review sign-off would include those reviews conducted during the year since the previous such sign-off. APRA expects that all elements of the risk management framework would be subject to review at least every three years. This review must be reported to the Board Audit Committee or, in the case of a foreign ADI, to the Senior Officer Outside of Australia. (CPG 220, paragraph 84)

86. CPS 220 requires the comprehensive review to be conducted by operationally independent, appropriately trained and competent persons at least every three years. There is no requirement that the comprehensive review must be undertaken by a party external to the institution. This review must be reported to the Board Risk Committee or, in the case of foreign ADIs, to the Senior Officer Outside of Australia. (CPG 220, paragraph 86)

87. APRA expects the comprehensive review to include a comparison of the institution's current practice against any identified better practice. Where any gaps are identified,

APRA expects the review to outline steps to address these differences or identify why changing current practice is not considered appropriate. The review may draw upon the APRA-regulated institution's internal resources, such as internal audit reports, to the extent that the independence of the review is not undermined. This forward-looking review is intended to assist the Board Risk Committee to oversee the implementation and appropriateness of the institution's risk management framework, while any compliance issues identified would be reported to the Board Audit Committee. (CPG 220, paragraph 87)

Risk management declaration, notifications and submissions

49. The Board of an APRA-regulated institution must make an annual declaration to APRA on risk management of the institution (risk management declaration) that must satisfy the requirements set out in Attachment A to this Prudential Standard. The declaration must be signed by the chairperson of the Board and the chairperson of the Board Risk Committee. In the case of a foreign ADI, the risk management declaration must be signed by the senior officer outside Australia. (CPS 220, paragraph 49)

50. The Board of an APRA-regulated institution must qualify the risk management declaration of the institution if there has been any significant breach of, or material deviation from, the risk management framework or the requirements set out in Attachment A to this Prudential Standard. Any qualification must include a description of the cause and circumstances of the qualification and steps taken, or proposed to be taken, to remedy the problem.[20] (CPS 220, paragraph 50)

52. An APRA-regulated institution must on adoption, and following any material revisions, submit to APRA a copy of the institution's:

    (a) risk appetite statement;

    (b) business plan; and

    (c) RMS

    as soon as practicable, and no more than 10 business days, after Board approval. (CPS 220, paragraph 52)

A.1. For the purposes of paragraph 49 of this Prudential Standard, the Board of an APRA-regulated institution must provide APRA with a risk management declaration of the institution stating that, to the best of its knowledge and having made appropriate enquiries, in all material respects:

    (a) the institution has in place systems for ensuring compliance with all prudential requirements;

    (b) the systems and resources that are in place for identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risks, and the risk

[20] Where relevant, any qualification of a risk management declaration must identify where the material deviation has occurred and whether it was on a Level 1/individual APRA-regulated institution basis and/or group basis.

management framework, are appropriate to the institution, having regard to the size, business mix and complexity of the institution;

(c) the risk management and internal control systems in place are operating effectively and are adequate having regard to the risks of the institution they are designed to control;

(d) the institution has a RMS that complies with this Prudential Standard, and the institution has complied with each measure and control described in the RMS;

(e) where it is a general insurer, the institution's Reinsurance Management Strategy complies with Prudential Standard GPS 230 Reinsurance Management, for selecting and monitoring reinsurance programs; and

(f) the APRA-regulated institution is satisfied with the efficacy of the processes and systems surrounding the production of financial information at the institution. (CPS 220, Attachment A1)

CPG 220

93. CPS 220 requires the Board to provide APRA with a risk management declaration on an annual basis. While this declaration does not have to be audited, APRA expects that the Board would have obtained reasonable assurance and, if necessary, considered independent advice on the matters covered by the declaration, prior to the signing of the declaration by the required signatories. The extent of enquiry required prior to making the declaration is a matter for the judgment of each Board of an APRA-regulated institution. The wording of the declaration allows materiality to be taken into account when making the declaration. (CPG 220, paragraph 93)

94. CPS 220 allows an APRA-regulated institution's risk management declaration to be encompassed in the risk management declaration documentation of a Level 2 and/or Level 3 group where applicable. Where a Level 1 institution's declaration is encompassed within the group declaration, the Level 1 institution's Board remains responsible for any qualifications in the declaration that relate to that institution. Where a risk management declaration is made on a Level 2 and/or Level 3 group basis, CPS 220 requires any qualification to identify whether it related to the Level 1 institution or the group's risk management framework. A qualification for the institution may not mean that a group-wide qualification needs to be made, and vice versa. However, where a group's Board has taken the decision that a qualification at the institution level does not result in a group declaration qualification, the reason for this decision would be articulated. (CPG 220, paragraph 94)

100. APRA expects that an APRA-regulated institution would be in regular dialogue with its supervisors about potential material changes to the institution. APRA expects that, at the latest, notification in accordance with the requirements in CPS 220 would be made within 10 business days of the Board becoming aware of a current or proposed material change to the institution's risk profile or business operations. (CPG 220, paragraph 100)

3.2 APS 220 Credit quality (2023)

Board oversight

27. The Board must ensure that senior management of the ADI has the capability and resources to appropriately manage the credit risk activities conducted by the ADI and that such activities operate within the credit risk management strategy, credit risk policies and credit risk appetite. (APS 220, paragraph 27)

B.4. Where the Board or senior management of an ADI believe that the prescribed provisions calculated in accordance with this Prudential Standard do not reasonably address assessed loss outcomes, they must report additional specific provisions. The level of specific provisions required will depend on the type of exposure and term of payments past-due or the period of irregularity in cash flows due on an exposure. (APS 220, Attachment B.4)

APG 220

20. A prudent Board would be alert to pressures on credit standards that could emerge, particularly as competition intensifies or market conditions shift. Ambitious lending growth plans, such as above system targets, can create pressures on credit standards. (APG 220, paragraph 20)

21. It is prudent for the Board to also be alert to emerging signs of credit deterioration, and to hold senior management to account for timely action. This could include having appropriate checks in place to maintain an independent perspective on credit quality and lending practices across the credit portfolio. (APG 220, paragraph 21)

Board approval

25. The Board[21] of an ADI must review and approve, on at least an annual basis, the ADI's credit risk appetite and credit risk management strategy. (APS 220, paragraph 25)

28. Senior management of an ADI must have responsibility for implementing the Board approved credit risk management strategy and for developing and implementing appropriate policies and processes for identifying, measuring, monitoring, reporting and controlling or mitigating credit risk. Such policies and processes must address credit risk in all of the ADI's activities and at both the individual exposure and portfolio levels. (APS 220, paragraph 28)

APG 220

7. APS 220 requires the credit risk appetite statement to be reviewed and approved by the Board on at least an annual basis. This review process would typically be incorporated into, or aligned with, an ADI's strategic and business planning process. (APG 220, paragraph 7)

---

[21] The requirements to be met by the Board must, in the case of a foreign ADI, be read subject to *Prudential Standard CPS 510 Governance* (CPS 510), which requires a foreign ADI to nominate a senior officer (whether a director or senior executive) outside Australia with delegated authority.

18. The Board does not have direct day-to-day responsibility for credit risk management. However, APS 220 requires the Board to review and approve the credit risk appetite and credit risk management strategy, and ensure that senior management has the capability and resources to effectively manage credit risk. It is important that the Board clearly set expectations for the monitoring and reporting of the credit risk appetite and management strategy. A prudent Board would also set clear expectations for the timely escalation of credit risk issues by senior management, including findings from internal and external credit risk reviews. (APG 220, paragraph 18)

Information for the Board

26. The Board must regularly challenge, seek assurance and evidence from senior management that the credit risk policies, processes and practices are consistent with the credit risk management strategy (and, in turn, the credit risk appetite) of the ADI. The Board must obtain sufficient information to confirm whether or not the credit risk profile of the ADI is consistent with the credit risk management strategy, and require senior management to take appropriate and timely action if it is not. (APS 220, paragraph 26)

74. Stress testing analyses must include contingency plans regarding actions the Board and senior management may take given certain scenarios. (APS 220, paragraph 74)

75. An ADI's stress testing arrangements must include well-documented and sound policies and processes governing the stress testing program, including the timely communication of information on scenarios, key assumptions, results and capital impacts to the ADI's Board and senior management. (APS 220, paragraph 75)

77. An ADI must establish a system of independent, regular reviews of the ADI's credit risk management processes and practices (refer to paragraph 29(e) of this Prudential Standard) and the results of such reviews must be communicated directly to the Board and senior management. (APS 220, paragraph 77)

86. An ADI's Board must obtain timely and appropriate information on the condition of the ADI's credit portfolio, including the classification of exposures as performing and non-performing and the level of provisions. The information must include, at a minimum, results of the latest credit risk review process, comparative trends in the overall quality of exposures and measurements of existing or anticipated deterioration in asset quality and expected credit losses. (APS 220, paragraph 86)

APG 220

19. While the Board may obtain advice on credit risk issues from Board committees, external advisers and senior management, it is important that the Board does not accept recommendations without due scrutiny and challenge. (APG 220, paragraph 19)

74. Risk grades are useful in tracking the quality of the credit portfolio and help in identifying necessary changes to the credit risk management strategy. Good practice is for the Board and senior management to receive regular reports on trends in risk grades to support their oversight of the credit portfolio. (APG 220, paragraph 74)

81. APS 220 requires an ADI to establish a system of independent, regular reviews of credit risk management processes and practices, with the results communicated directly to the Board and senior management. (APG 220, paragraph 81)

82. It is good practice for internal reviews of credit risk to be conducted by personnel that are independent from the business function. This provides a more objective assessment. Internal reviews can be used to evaluate the overall credit administration process, determine the accuracy of internal credit risk grades (where applicable), and confirm whether policies are being followed in practice. It is good practice for the credit review function to report directly to either the Board, the Risk or Audit committee, or senior management without lending authority, such as senior management within the risk control function. (APG 220, paragraph 82)

3.3 APG 223 Residential Mortgage Lending (2023)

Board oversight

3. Where residential mortgage lending forms a material proportion of an ADI's lending portfolio and therefore a risk that may have a material impact on the ADI, APRA expects that the Board would take reasonable steps to satisfy itself as to the level of risk in the ADI's residential mortgage lending portfolio and the effectiveness of its risk management framework. This would, at the very least, include:

    (a) specifically addressing residential mortgage lending in the ADI's risk appetite, risk management strategy and business plans;

    (b) seeking assurances from senior management that the approved risk appetite is communicated to relevant persons involved in residential mortgage lending and is appropriately reflected in the ADI's policies and procedures; and

    (c) seeking assurances from senior management that there is a robust management information system in place that:

        (i) tracks material risks against risk appetite;

        (ii) provides periodic reporting on compliance with policies and procedures, reasons for significant breaches or material deviations and updates on actions being taken to rectify breaches or deviations; and

        (iii) provides accurate, timely and relevant information on the performance and risk profile of the residential mortgage lending portfolio. (APG 223, paragraph 3)

9. Typically, senior management is responsible for monitoring compliance with material policies, procedures and risk limits and reporting material breaches or overrides to the Board. Further, where risk limits are routinely breached or policies and procedures overridden, senior management and the Board could consider whether this is indicative of a less prudent lending culture than that reflected in its risk appetite and what steps could be necessary to remedy any identified deficiency. (APG 223, paragraph 9)

77. A prudent ADI would monitor exposures by loan-to-valuation ratio (LVR) bands over time. Significant increases in high LVR lending would typically be a trigger for senior management to review risk targets and internal controls over high LVR lending, with Board oversight. APRA has not formally defined 'high LVR lending', but experience shows that LVRs above 90 per cent (including capitalised LMI premium or other fees) clearly expose an ADI to a higher risk of loss. (APG 223, paragraph 77)

Board approval

17. *Prudential Standard CPS 510 Governance* (CPS 510) requires the Board-approved ADI remuneration policy to be aligned with prudent risk-taking. CPS 510 requires the remuneration policy to apply to responsible persons, risk and financial control personnel and all other persons whose activities may affect the financial soundness of the regulated institution. Where the residential mortgage lending portfolio is material, a prudent ADI would apply its remuneration policy to the persons involved in residential mortgage lending. This would include remuneration of third parties, particularly mortgage broker firms, when they are responsible for origination of a material proportion of the residential mortgage loan portfolio. For the avoidance of doubt, the ADI remuneration policy is intended to capture an ADI's engagement with its brokers, not how a broking firm pays its staff. Alternatively, the ADI may address such remuneration arrangements within its risk management framework with appropriate senior management or Board oversight. (APG 223, paragraph 17)

Information for the Board

10. In order to establish robust oversight, the Board and senior management would receive regular, concise and meaningful assessment of actual risks relative to the ADI's risk appetite and of the operation and effectiveness of internal controls. The information would be provided in a timely manner to facilitate early corrective action. (APG 223, paragraph 10)

11. A prudent ADI would have controls in relation to its residential mortgage portfolio that have appropriate regard to the level of risk within the portfolio. Portfolios that have higher inherent risk, for example where the portfolio is usually operating at the higher end of risk limits, would typically be accompanied by stronger controls, including: increased monitoring and more granular reporting to the Board and senior management. (APG 223, paragraph 11(b))

12. Consistent with CPS 220, the aspects of the risk management framework that apply to the residential mortgage lending portfolio would be subject to a comprehensive review by an operationally independent and competent person at least every three years. The person would report the results of reviews to the Board, providing an independent and objective evaluation of the appropriateness, adequacy and effectiveness of the risk management framework with respect to the portfolio. (APG 223, paragraph 12)

15. Further, a prudent ADI would have analytical capability that allows it to monitor, analyse and report key metrics against risk appetite and to assess the residential mortgage portfolio at both the individual loan level and portfolio level. The data, when collectively presented to the Board and senior management, would enable an accurate and meaningful assessment of the residential mortgage portfolio. A history of low defaults

does not justify under-investment in management information systems. (APG 223, paragraph 15)

22. When an ADI is increasing its residential mortgage lending rapidly or at a rate materially faster than its competitors, either across the portfolio or in particular segments or geographical areas, a prudent Board would seek explanation as to why this is the case. Rapid relative growth could be due to an unintended deterioration in the ADI's loan origination practices, in which case APRA expects that an ADI's risk management framework would facilitate rapid and effective measures to mitigate any consequences. (APG 223, paragraph 22)

51. Good practice is for regular override reporting to be provided to senior management and to the Board. Such reporting would include:

    (a) delinquency rates for residential mortgage loans approved as overrides and exceptions;

    (b) tracking against risk tolerance limits for overrides;

    (c) reasons for overrides; and

    (d) distribution of overrides across business units, products, locations, third-party originators and, where relevant, ADI officers associated with a disproportionate number of overrides. (APG 223, paragraph 51)

93. An ADI following good practice would include a carefully considered collections strategy in its credit risk management framework for residential mortgage lending. The framework could include: appropriate reporting to senior management and the Board on delinquencies, including recoveries and cost of collections. (APG 223, paragraph 93 (e))

99. Results from portfolio stress tests enable the Board and senior management to review an ADI's risk appetite, capital adequacy and relevant strategic business decisions in both current and potential environments. For example, stress tests might identify vulnerabilities in certain product or borrower segments that would prompt an ADI to tighten its loan origination criteria or lower risk appetite limits on those products. (APG 223, paragraph 99)

101. Stress testing arrangements include well-documented policies and procedures governing the stress testing program, including timely communication of the stress test results to the Board, senior management and other relevant staff. When reporting results, sufficient information would be provided to enable the Board and senior management to understand and challenge stress test assumptions and conclusions. This includes quantitative information on the scenario, results, capital impact, key assumptions and recommended actions arising from the stress tests. (APG 223, paragraph 101)

3.4 APS 221 Large exposures (2023)

Board oversight[22]

10. The Board of an ADI is ultimately responsible for the oversight of the ADI's large exposures and risk concentrations and for approving policies governing large exposures and risk concentrations of the ADI. The Board must ensure that these policies are reviewed regularly (at least annually) and that they remain adequate and appropriate for the ADI's risk appetite, risk profile, capital and balance sheet size. (APS 221, paragraph 10)

Board approval

12. An ADI's policies on large exposures and risk concentrations must, at a minimum, cover: the circumstances in which the exposure limits may be exceeded and the authority and processes required for approving such excesses (e.g. by the ADI's Board or a board committee). (APS 221, paragraph 12(b))

3.5 APS 222 Associations with Related Entities (2022)

Board oversight

12. The Board of an ADI is ultimately responsible for oversight of the ADI's associations with its related entities and for approving policies governing the ADI's dealings and associations with its related entities. The Board must ensure these policies are reviewed at least annually and that they remain adequate and appropriate for the ADI's risk appetite, risk profile, capital, balance sheet size and the complexity of the ADI's group. (APS 222, paragraph 12)[23], [24]

Board approval

15. An ADI's Board must first approve the terms and conditions agreed to by an ADI in relation to dealings with its related entities that are not consistent with terms and conditions that would be negotiated with an unrelated entity with justifications fully and clearly documented in a register. (APS 222, paragraph 15)

[22] APS 221 paragraph 22 sets out factors that may give rise to control relationships. This includes with respect to the Board.

[23] Attachment B of APS 222 sets out particular requirements, including with respect to the Board, that apply to an ADI's associations with a funds management vehicle that is a related entity of the ADI. Attachment C sets out requirements relating to an Extended Licensed Entity.

[24] As per APS 222, Footnote 1, a reference to the Board in the case of a foreign ADI, is a reference to the senior officer outside Australia.

3.6 CPS 226 Margining and Risk Mitigation for Non-Centrally Cleared Derivatives (2023)

Information for the Board

92. The dispute resolution mechanism or process must include the escalation of material disputes to senior management. The dispute resolution mechanism or process must include escalation to the Board where the dispute is considered material to the APRA covered entity. (CPS 226, paragraph 92)

3.7 CPG 229 Climate Change Financial Risks (2021)

Board oversight

8. Climate change may also give rise to liability risks which have implications for businesses and directors' duties. Liability risks stem from the potential for litigation where institutions and boards do not adequately consider or respond to the impacts of climate change. (CPG 229, paragraph 8)

13. Prudential standards CPS 510 and SPS 510 set out the minimum governance requirements of an APRA-regulated institution. The ultimate responsibility for the sound and prudent management of an APRA-regulated institution's business operations rests with its board of directors[25]. APRA therefore considers it prudent practice for the board to seek to understand and regularly assess the financial risks arising from climate change that affect the institution, now and into the future. (CPG 229, paragraph 13)

14. APRA is of the view that climate risks can and should be managed within an institution's overall business strategy and risk appetite, and a board should be able to evidence its ongoing oversight of these risks. (CPG 229, paragraph 14)

15. The board of an institution may delegate certain functions of the management of climate risks but, as with other risks, needs to maintain mechanisms for monitoring the exercise of this delegated authority. Board-level engagement is important to ensure that work on climate risks holds sufficient standing within an institution, and gives the board the requisite institution-wide insights to strategically respond to the risks. (CPG 229, paragraph 15)

16. In fulfilling its obligations under CPS 510 and SPS 510, a prudent board is, in overseeing the management of climate risks, likely to:

    (a) ensure an appropriate understanding of, and opportunity to discuss, climate risk at the board and sub-committee levels, which may include appropriate training for board members;

[25] For the purposes of this PPG, a reference to the board, in the case of a foreign ADI, is a reference to the Senior Officer Outside of Australia as referred to in *Prudential Standard CPS 510 Governance*.

(b) set clear roles and responsibilities of senior management in the management of climate risks, and hold senior management to account for these responsibilities;

(c) re-evaluate the risks, opportunities and accountabilities arising from climate change on a periodic basis, and consider these risks and opportunities in approving the institution's strategies and business plans;

(d) take both a shorter-term view (consistent with the institution's regular business planning horizon) and longer-term view when assessing the impact of climate risks and opportunities; and

(e) ensure that, where climate risks are found to be material, the institution's risk appetite framework incorporates the risk exposure limits and thresholds for the financial risks that the institution is willing to bear. (CPG 229, paragraph 16)

18. Under CPS 220 and SPS 220, the board of an APRA-regulated institution is ultimately responsible for both the institution's risk management framework, and for the oversight of its operation by management. Senior management of the institution monitor and manage all material risks consistent with the strategic objectives, risk appetite statement and policies approved by the board. APRA considers it prudent for climate risks to be considered within an institution's existing framework, including the board-approved risk appetite statement, risk management strategy and business plan. (CPG 229, paragraph 18)

Information for the Board

17. In light of the board responsibilities set out in Paragraph 16, an institution's senior management would typically be responsible for:

(a) applying an institution's risk management framework to assess and manage climate risk exposures on an ongoing basis, including developing and implementing appropriate policies;

(b) regularly reviewing the effectiveness of the framework, policies, tools, and metrics and targets, and making appropriate revisions;

(c) providing recommendations to the board on the institution's objectives, plans, strategic options and policies as they relate to climate risks that are assessed to be material. This may include the establishment and use of relevant tools, models, and metrics and targets to monitor exposures to climate risks so as to enable the board to make informed decisions in a timely manner; and

(d) ensuring that adequate resources, skills and expertise are allocated to the management of climate risks, including thorough training and capacity building amongst relevant staff. (CPG 229, paragraph 17)

20. APRA considers that prudent practice would be for an institution to evidence the management of climate risks within its written risk management policies, management information, and board risk reports. Where climate risks are material, this may require updating existing risk management policies and procedures. (CPG 229, paragraph 20)

31. Given the evolving understanding of climate change, a prudent institution would ensure that climate risk data, metrics and targets were updated regularly to support decision-making by the institution's board and senior management. It would also consider the circumstances which might trigger a review of its strategy or engagement with customers and counterparties. (CPG 229, paragraph 31)

35. To facilitate well-informed decision-making, APRA expects that a prudent institution would establish procedures to routinely provide relevant information on its material climate risk exposures, including monitoring and mitigation actions, to the board and senior management. This information would allow the board and senior management to understand and review the activities, and to make decisions consistent with the institution's overall risk appetite and risk management approach. (CPG 229, paragraph 35)

46. A prudent institution would maintain appropriate documentation of the method and results of its climate risk scenario analysis and stress testing, including an assessment of the limitations of the analysis for assessing the climate risks faced by the institution. Material results should be communicated to the institution's board and senior management, and used to inform business planning and strategy setting, as well as setting and reviewing the institution's overall climate risk management approach. (CPG 229, paragraph 46)

3.8 CPS 231 Outsourcing (2017)

Board oversight

22. The Board is ultimately responsible for oversight of any outsourcing of a material business activity undertaken by an APRA-regulated institution. Although outsourcing may result in the service provider having day-to-day managerial responsibility for a business activity, the APRA-regulated institution is responsible for complying with all prudential requirements that relate to the outsourced business activity. (CPS 231, paragraph 22)

24. The Board of an APRA-regulated institution must ensure that outsourcing risks and controls are taken into account as part of the institution's risk management strategy and when completing a risk management declaration required to be provided to APRA.[26] (CPS 231, paragraph 24)

Board approval

5. Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group policy used by a related body corporate,[27] provided that the

[26] For details of the risk management framework for regulated institutions refer to *Prudential Standard CPS 220 Risk Management*.

[27] Related body corporate has the meaning given in section 50 of the *Corporations Act 2001*.

policy has been approved by the Board[28] and meets the requirements of this Prudential Standard. (CPS 231, paragraph 5)

23. The Board of an APRA-regulated institution must approve the institution's outsourcing policy, which must set out the approach to outsourcing of material business activities, including a detailed framework for managing all such outsourcing arrangements. (CPS 231, paragraph 23)

26. An APRA-regulated institution must be able to demonstrate to APRA that, in assessing the options for outsourcing a material business activity to a 'third party',[29] it has: involved the Board of the APRA-regulated institution, Board committee of the APRA-regulated institution, or senior manager of the institution with delegated authority from the Board, in approving the agreement. (CPS 231, paragraph 26(d))

CPG 231

7. When a regulated institution decides to enter into an outsourcing agreement, there are a number of factors that may be appropriate for the Board to consider in addition to those outlined in the Prudential Standards.[30]

Information for the Board

18. The group internal audit function must review any proposed outsourcing of a material business activity of the group, except where the internal audit function of an APRA-regulated institution within the group has reviewed the proposed outsourcing. The group internal audit function must regularly review and report to the Board of the Head of the group or group Board Audit Committee on compliance with the group outsourcing policy. (CPS 231, paragraph 18)

44. An institution's internal audit function must review any proposed outsourcing of a material business activity and regularly review and report to the Board or Board Audit Committee on compliance with the institution's outsourcing policy. Where APRA has exempted an institution from having a dedicated internal audit function, or approved alternative arrangements under *Prudential Standard CPS 510 Governance*, APRA may also vary the requirements of this paragraph. (CPS 231, paragraph 44)

CPG 231

21. When assessing options for outsourcing material business activities, it is good practice to establish an outsourcing team consisting of individuals from the relevant business area(s) and others with the necessary skills to assess the risks involved in outsourcing. They may include specialists in the relevant risk areas and external experts. This team would ensure that the outsourcing policy is followed at all times, including assessment of the initial tender and due diligence processes, evaluation of the outsourcing options,

---

[28] A reference to the Board in the case of a foreign ADI is a reference to the senior officer outside Australia.

[29] For the purposes of this Prudential Standard, 'third party' is a reference to an institution that is not the APRA-regulated institution or a related body corporate of the APRA-regulated institution.

[30] Refer to CPG 231, paragraphs 8-21

and making recommendations to senior management and the Board on the outsourcing proposal. (CPG 231, paragraph 21)

3.9 CPS 234 Information Security (2019)

Board oversight

13. The Board of an APRA-regulated entity (Board) is ultimately responsible for the information security of the entity. The Board must ensure that the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity.[31] (CPS 234, paragraph 13)

14. An APRA-regulated entity must clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and individuals with responsibility for decision-making, approval, oversight, operations and other information security functions.[32] (CPS 234, paragraph 14)

CPG 234

8. Under CPS 234, the Board of an APRA-regulated entity is ultimately responsible for the information security of the entity. In order for a Board to be able to more effectively discharge its responsibilities (including oversight, seeking assurance and, as appropriate, challenging management), it could consider the following:

   (a) roles and responsibilities – clearly outline for management how the Board expects to be engaged, including delegation of responsibilities, escalation of risks, issues and reporting requirements (including schedule, format, scope and content). Refer to Attachment H for common examples of the types of information that the Board might find useful to effectively fulfil its role and discharge its responsibilities;

   (b) information security capability – consider the sufficiency of the regulated entity's information security capability in relation to vulnerabilities and threats; ensure sufficiency of investment to support the information security capability; and review progress with respect to execution of the information security strategy;

   (c) policy framework - whether information security policies reflect Board expectations;

   (d) implementation of controls - regularly seek assurance from and, as appropriate, challenge management on reporting regarding the effectiveness of the information security control environment and the overall health of the entity's information assets;

[31] A reference to the Board in the case of a foreign ADI, is a reference to the senior officer outside Australia.

[32] For the purposes of this Prudential Standard, governing bodies and individuals includes committees, working groups and forums.

(e) testing control effectiveness - regularly seek assurance from and, as appropriate, challenge management on the sufficiency of testing coverage across the control environment; form a view as to the effectiveness of the information security controls based on the results of the testing conducted; and

(f) internal audit - consider the sufficiency of internal audit's coverage, skills, capacity and capabilities with respect to the provision of independent assurance that information security is maintained; form a view as to the effectiveness of information security controls based on audit conclusions; and consider where further assurance, including through expert opinion or other means, is warranted. (CPG 234, paragraph 8)

9. In considering the above, the Board would normally take into account the use of third parties and related parties (including group functions) by the APRA-regulated entity. (CPG 234, paragraph 9)

10. APRA does not seek to impose restrictions on a Board's ability to delegate information security roles and responsibilities to Board sub-committees, management committees or individuals. However, APRA expects that a Board would clearly outline how it expects to be engaged with respect to information security, including escalation of risks, issues and reporting. Refer to Attachment H for common examples of the types of information that the Board might find useful in this regard. (CPG 234, paragraph 10)

11. Definition of information security-related roles and responsibilities is typically achieved through a combination of role statements, policy statements, reporting lines and charters of governing bodies. Common governing bodies and individuals with decision-making, approval, oversight, operations and other information security roles and responsibilities typically include:

(a) information security steering/oversight committee;

(b) risk management committee (Board and management level);

(c) Board audit committee;

(d) executive management/executive management committee;

(e) chief information officer /IT manager;

(f) chief information security officer/IT security manager;

(g) information security operations/administration; and

(h) management (business and IT). (CPG 234, paragraph 11)

20. Under CPS 234, an APRA-regulated entity must actively maintain an information security capability with respect to changes in vulnerabilities and threats. Accordingly, an entity would typically adopt an adaptive and forward-looking approach to maintaining its information security capability, including ongoing investment in resources, skills and controls. This would commonly be achieved through the execution of an information security strategy which responds to the changing environment throughout the year. The

strategy could be informed by existing and emerging information security vulnerabilities and threats, contemporary industry practices, information security incidents, both internal and external, and known information security issues. Oversight of execution of the strategy is normally the responsibility of the Board or a delegated governing body with representation from across the organisation. (CPG 234, paragraph 20)

83. Internal audit is an important vehicle by which the Board can gain assurance that information security is maintained. This assurance would typically be achieved through the inclusion of information security within the APRA-regulated entity's internal audit plan. The Board could also choose to gain assurance through expert opinion or other means to complement the assurance provided by the internal audit function. This typically occurs where the required skills do not reside within the internal audit function or the area subject to audit pertains to third parties or related parties. (CPG 234, paragraph 83)

Information for the Board

25. An APRA-regulated entity's information security response plans must include the mechanisms in place for: escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate. (CPS 234, paragraph 25(b))

29. An APRA-regulated entity must escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner. (CPS 234, paragraph 29)

CPG 234

13. The Board, governing bodies and individuals would typically define their information requirements (e.g. schedule, format, scope and content) to ensure they are provided with sufficient and timely information to effectively discharge their information security roles and responsibilities. Reporting to governing bodies would normally be supported by defined escalation paths and thresholds. An APRA-regulated entity could benefit from implementing processes for periodic review of audience relevance and fitness for use. (CPG 234, paragraph 13)

71. An APRA-regulated entity would typically have clear accountability and communication strategies to limit the impact of information security incidents. Under CPS 234, this includes escalation and reporting of information security incidents to the Board, other governing bodies and individuals responsible for information security incident management and oversight, as appropriate. A regulated entity could also include customer communication as part of any such communication strategy where appropriate. Incident response plans would also typically assist in compliance with regulatory notification requirements. (CPG 234, paragraph 71)

86. Under CPS 234, an APRA-regulated entity's internal audit function must assess the information security control assurance provided by a third party or related party in certain circumstances. Where that assessment identifies material deficiencies in the information security control assurance provided by the third party or related party, or no

assurance is available, this would typically be highlighted in reporting to the Board. (CPG 234, paragraph 86)

3.10 CPG 235 Managing Data Risk (2013)

Board oversight

5. As with any process, governance is vital to ensure that data risk management and related business processes are properly designed and operating effectively to meet the needs of the regulated entity. In APRA's view, effective governance of data risk management would be aligned to the broader corporate governance frameworks and involve the clear articulation of Board and senior management responsibilities and expectations, formally delegated powers of authority and regular oversight. (CPG 235, paragraph 5)

20. In order to ensure that data risk management is not conducted in an ad hoc and fragmented manner, a regulated entity would typically adopt a systematic and formalised approach that ensures data risk is taken into consideration as part of its change management and business-as-usual processes. This could be encapsulated in a formally approved data risk management framework outlining the entity's approach to managing data risk that: includes the expectations of the Board and senior management. (CPG 235, paragraph 20(c))

Board approval

50. In APRA's view, the following would normally be applied to the assessment and ongoing management of outsourced/offshored data management responsibilities: Board/senior management's understanding, acceptance and approval of the resulting risk profile. (CPG 235, paragraph 50 (f))

Information for the Board

61. Subject to the nature of the data, a regulated entity would: have clear accountability and communication strategies to limit the impact of data issues. This would typically include defined mechanisms and thresholds for escalation and reporting to the Board and senior management, and customer communication where appropriate. Issue management strategies would also typically assist in compliance with regulatory and legal requirements. (CPG 235, paragraph 61(a))

3.11 CPS 232 Business Continuity Management (2017)

Board oversight

13. The Board of the Head of a group must:

    (a) ensure that the group's Business Continuity Management (BCM) is appropriate to the nature and scale of its operations and is consistent with the group's risk management strategy and risk management framework;

    (b) oversee the appropriateness of BCM across the group; and

(c) ensure that the group's business continuity plan (BCP) is reviewed at least annually by responsible senior management of the Head of the group. (CPS 232, paragraph 13)

18. The Board is ultimately responsible for the business continuity of the institution. The Board remains ultimately responsible for BCM of the institution whether or not business operations are outsourced or are part of a corporate group.[33] (CPS 232, paragraph 18)

19. The Board must ensure that the business continuity risks and controls are taken into account as part of the institution's risk management strategy and when completing a risk management declaration required to be provided to APRA.[34] (CPS 232, paragraph 19)

Board approval

6. Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group policy used by a related body corporate, provided that the policy has been approved by the Board[35] of the regulated institution and meets the requirements of this Prudential Standard (CPS 232, paragraph 6)

23. The Board must approve the institution's BCM policy. (CPS 232, paragraph 23)

Information for the Board

15. The group internal audit function, or an appropriate external expert, must periodically review the group BCP and provide an assurance to the Board of the Head of the group, or delegated management, on the matters in paragraph 38 on a group basis. (CPS 232, paragraph 15)

34. An APRA-regulated institution must review and test the institution's BCP at least annually, or more frequently if there are material changes to business operations, to ensure that the BCP can meet the BCM objectives. The results of the testing must be formally reported to the Board or to delegated management.[36] (CPS 232, paragraph 34)

38. An institution's internal audit function, or an appropriate external expert, must periodically review the BCP and provide an assurance to the Board or to delegated management that:

(a) the BCP is in accordance with the institution's BCM policy and addresses the risks it is designed to control; and

---

[33] Refer to *Prudential Standard CPS 231 Outsourcing* (CPS 231) for further information on requirements relating to outsourcing.

[34] For details of the risk management framework for regulated institutions refer to *Prudential Standard CPS 220 Risk Management*.

[35] A reference to the Board in the case of a foreign ADI is a reference to the senior officer outside Australia.

[36] A material change to business operations includes a change in a material outsourcing arrangement. Refer to CPS 231 for further information on outsourcing.

(b) testing procedures are adequate and have been conducted satisfactorily. (CPS 232, paragraph 38)

Chapter 4 - Governance

Governance

This chapter sets out the specific obligations that apply to directors in respect to governance. In summary:

- Governance: It is essential that an APRA-regulated institution and group has a sound governance framework and conducts its affairs with a high degree of integrity (CPS 510 summary box)
- Accountability: The accountability obligations of an ADI are to take reasonable steps to conduct its business with honesty and integrity, and with due skill, care and diligence. An ADI must also deal with APRA in an open, constructive and cooperative way (Banking Act, s.37C)
- Disclosure: An ADI must meet minimum requirements for the public disclosure of key information so as to contribute to the transparency of financial markets and to enhance market discipline (APS 330 summary box).

4.1 CPS 510 Governance (2019)[37]

Board oversight

13. The Board of the Head of a group is ultimately responsible for oversight of the sound and prudent management of the group and must have the following committees for the group:

    (b) a group Board Audit Committee that meets the requirements of paragraphs 74 to 89 and that assists the Board by providing an objective non-executive review of the effectiveness of the group's financial reporting and group risk management framework; and

    (c) a group Board Risk Committee that meets the requirements of paragraphs 102 to 109 and that assists the Board by providing an objective non-executive oversight of the implementation and operation of the group risk management framework. (CPS 510, paragraphs 13(b) & 13(c))

14. The Board of a Head of a group must ensure that directors and senior management of the group, collectively, have the full range of skills needed for the effective oversight and

[37] CPS 510 requirements relating to remuneration have not been included (paragraphs 12, 13(a), 52, 56, 58, 62, 65-72), given APRA's intention to retire these once CPS 511 comes into force, refer to: https://www.apra.gov.au/sites/default/files/2021-08/Response%20paper%20-%20Strengthening%20prudential%20requirements%20for%20remuneration.pdf

prudent management, respectively, of the group. This does not lessen the responsibility of each of the individual Boards of the institutions within the group for their institutions. (CPS 510, paragraph 14)

16. The Board of a locally-incorporated APRA-regulated institution is ultimately responsible for oversight of the sound and prudent management of that institution. (CPS 510, paragraph 16)

17. The Board must have a formal charter that sets out the roles and responsibilities of the Board. (CPS 510, paragraph 17)

18. The Board, in fulfilling its functions, may delegate authority to management to act on behalf of the Board with respect to certain matters, as decided by the Board. This delegation of authority must be clearly set out and documented. The Board must have mechanisms in place for monitoring the exercise of delegated authority. The Board cannot abrogate its responsibility for oversight of the functions delegated to management. (CPS 510, paragraph 18)

19. The Board must ensure that directors and senior management of the institution collectively have the full range of skills needed for the effective and prudent operation of the institution, and that each director has skills that allow them to make an effective contribution to Board deliberations and processes. This includes the requirement for directors, collectively, to have the necessary skills, knowledge and experience to understand the risks of the institution, including its legal and prudential obligations, and to ensure that the institution is managed in an appropriate way taking into account these risks. This does not preclude the Board from supplementing its skills and knowledge by engaging external consultants and experts. (CPS 510, paragraph 19)

21. Directors and senior management of a locally incorporated APRA-regulated institution must be available to meet with APRA on request. (CPS 510, paragraph 21)

22. The Board must provide the auditor and the Appointed Actuary of the institution, as relevant, with the opportunity to raise matters directly with the Board. (CPS 510, paragraph 22)

44. The Board of a locally incorporated APRA-regulated institution must have procedures for assessing, at least annually, the Board's performance relative to its objectives. It must also have in place a procedure for assessing, at least annually, the performance of individual directors. (CPS 510, paragraph 44)

45. The Board of a locally incorporated APRA-regulated institution must have in place a formal policy on Board renewal. This policy must provide details of how the Board intends to renew itself in order to ensure it remains open to new ideas and independent thinking, while retaining adequate expertise. The policy must give consideration to whether directors have served on the Board for a period that could, or could reasonably be perceived to, materially interfere with their ability to act in the best interests of the institution. The policy must include the process for appointing and removing directors, including the factors that will determine when an existing director will be re-appointed. (CPS 510, paragraph 45)

46. As in the case of locally incorporated APRA-regulated institutions, the ultimate responsibility for the safety and soundness of a foreign ADI resides with its Board. Foreign ADIs must nominate a senior officer (whether a director or senior executive) outside Australia with delegated authority from the Board (senior officer outside Australia) who will be responsible for overseeing the Australian branch operation. (CPS 510, paragraph 46)

93. The Board of the APRA-regulated institution or the senior officer outside Australia, as relevant, must, to the extent practical, undertake steps to satisfy itself that the auditor, who undertakes work for the APRA-regulated institution in relation to the Prudential Acts, prudential standards or reporting standards, is independent of the institution,[38] and that there is no conflict of interest situation that could compromise, or be seen to compromise, the independence of the auditor. (CPS 510, paragraph 93)

Board approval

42. Where a locally incorporated APRA-regulated institution is part of a group or any other corporate group, and the APRA-regulated institution utilises group policies or functions, the Board of the APRA-regulated institution must approve the use of group policies and functions and must ensure that these policies and functions give appropriate regard to the APRA-regulated institution's business and its specific requirements. (CPS 510, paragraph 42)

Board committees, composition and representation

Board composition

26. The Board of a locally incorporated APRA-regulated institution must have a minimum of five directors at all times. (CPS 510, paragraph 26)

27. The Board must have a majority of independent directors at all times. For a locally incorporated APRA-regulated institution that is a subsidiary[39] of another APRA-regulated institution or overseas equivalent,[40] exceptions may apply as set out at paragraphs 37 to 39. For a locally incorporated APRA-regulated institution that is a subsidiary of a parent company that is not prudentially regulated, exceptions may apply as set out at paragraph 40. (CPS 510, paragraph 27)

28. The chairperson of the Board must be an independent director of the APRA-regulated institution. (CPS 510, paragraph 28)

29. A majority of directors present and eligible to vote at all Board meetings must be non-executive directors. (CPS 510, paragraph 29)

---

[38] Independent of the APRA-regulated entity means that the auditor has been assessed as independent in terms of paragraph 80 of this Prudential Standard.

[39] 'Subsidiary' means a subsidiary within the meaning of the *Corporations Act 2001* (Corporations Act).

[40] An 'overseas equivalent' is an entity which is not authorised in Australia but is authorised and subject to prudential regulation in a foreign country.

30. The chairperson of the Board cannot have been the CEO of the APRA-regulated institution at any time during the previous three years. If the position of the CEO is unexpectedly vacated, the chairperson may serve as an interim CEO. After a period of 90 days, approval must be sought from APRA to allow this arrangement to continue. (CPS 510, paragraph 30)

31. The chairperson must be available to meet with APRA on request. (CPS 510, paragraph 31)

32. For a locally owned and incorporated APRA-regulated institution, a majority of directors must be ordinarily resident in Australia. (CPS 510, paragraph 32)

33. For a foreign-owned, locally incorporated APRA-regulated institution, at least two of the directors must be ordinarily resident in Australia, at least one of whom must also be independent. (CPS 510, paragraph 33)

37. For a locally incorporated APRA-regulated institution that is a subsidiary of another APRA-regulated institution or an overseas equivalent, the Board must have a majority of non-executive directors, but these non-executive directors need not all be independent. (CPS 510, paragraph 37)

38. An institution to which paragraph 37 applies will be required to have, at a minimum, two independent directors, in addition to an independent chairperson, where the Board has up to seven members. Where the Board has more than seven members, the institution will be required to have at least three independent directors, in addition to an independent chairperson. (CPS 510, paragraph 38)

39. For the purposes of meeting the requirements in paragraph 38, the independent directors on the Board of the parent company or its other subsidiaries may also sit as independent directors on the Board of the institution. (CPS 510, paragraph 39)

40. For a locally incorporated APRA-regulated institution that is a subsidiary of another entity not covered by the arrangements in paragraphs 37 to 39 of this Prudential Standard, the Board must have a majority of independent directors. However, independent directors on the Board of the parent company or its other subsidiaries may also sit as independent directors on the Board of the institution. (CPS 510, paragraph 40)

41. For the purposes of this Prudential Standard, a locally incorporated APRA-regulated institution that operates as a joint venture can be considered as part of the group of each parent entity. Independent directors of a parent may sit as independent directors on the Board of the joint venture entity. However, the general concessions available to subsidiaries in paragraphs 37 to 39 are not available to joint ventures. (CPS 510, paragraph 41)

43. The board composition and representation requirements in paragraphs 26 to 36 that apply to a locally incorporated APRA-regulated institution do not apply to an entity within the group that is not an APRA-regulated institution. (CPS 510, paragraph 43)

96. A person who was a member of an audit firm or a director of an audit company and who served in a professional capacity in the audit of an APRA-regulated institution in relation

to the Prudential Acts, prudential standards or reporting standards, cannot be appointed to the role of director or senior manager of that APRA-regulated institution until at least two years have passed since they served in that professional capacity. (CPS 510, paragraph 96)

97. A person who was an employee of an audit company, other than a director of that company, and who acted as the lead auditor[41] or review auditor[42] in the audit of an APRA-regulated institution in relation to the Prudential Acts, prudential standards or reporting standards, cannot be appointed to the role of director or senior manager of that APRA-regulated institution until at least two years have passed since they acted as the lead auditor or review auditor. (CPS 510, paragraph 97)

98. A person cannot be appointed as a director or senior manager of an APRA-regulated institution if:

    (a) the person was, or is, a director of the audit company or a member of the audit firm that was, or is, responsible for the audit of the APRA-regulated institution in relation to the Prudential Acts, prudential standards or reporting standards; and

    (b) there is already another person employed as a director or senior manager of the APRA-regulated institution who was a director of the audit company or a member of the audit firm, at a time when the audit company or audit firm undertook an audit of the APRA-regulated institution at any time during the previous two years. (CPS 510, paragraph 98)

Director independence, and definition of non-executive director

23. For the purposes of this Prudential Standard, an 'independent director' is a non-executive director who is free from any business or other association - including those arising out of a substantial shareholding, involvement in past management or as a supplier, customer or adviser - that could materially interfere with the exercise of their independent judgement. The circumstances that will not meet this test of independence include, but are not limited to, those set out in Attachment A. (CPS 510, paragraph 23)

24. If the Board of a locally incorporated APRA-regulated institution is in doubt about a director's independence for the purposes of this Prudential Standard, the APRA-regulated institution may refer the matter to APRA for guidance. (CPS 510, paragraph 24)

25. For the purposes of this Prudential Standard, a reference to a 'non-executive director' is interpreted as meaning a reference to a director who is not a member of the APRA-regulated institution's management. Non-executive directors may include Board members or senior managers of the parent company of the locally incorporated APRA-

[41] Lead auditor means the registered company auditor who is primarily responsible to the audit firm or the audit company for the conduct of audit work conducted in relation to the Prudential Acts, prudential standards or reporting standards.

[42] Review auditor means the registered company auditor (if any) who is primarily responsible to the individual auditor, audit firm or audit company for reviewing audit work conducted in relation to the Prudential Acts, prudential standards or reporting standards.

regulated institution or of the parent company's subsidiaries, but not executives of the APRA-regulated institution or its subsidiaries. (CPS 510, paragraph 25)

Attachment A. A director is not independent if the director:

1. is a substantial shareholder[43] of the APRA-regulated institution or an officer of, or otherwise associated directly with, a substantial shareholder of the institution;

2. is employed, or has previously been employed in an executive capacity by the APRA-regulated institution or another member of the group, and there has not been a period of at least three years between ceasing such employment and serving on the Board;

3. has within the last three years been a principal of a material professional adviser or a material consultant to the APRA-regulated institution or another member of the group, or an employee materially associated with the service provided;

4. is a material supplier or customer of the APRA-regulated institution or another member of the group, or an officer of or otherwise associated directly or indirectly with a material supplier or customer; or

5. has a material contractual relationship with the APRA-regulated institution or another member of the group other than as a director. (CPS 510, Attachment A)

Board representation

34. Board representation must be consistent with a locally incorporated APRA-regulated institution's shareholding. Where a shareholding constitutes not more than 15 per cent of the APRA-regulated institution's voting shares, there should not be more than one Board member who is an associate of the shareholder where the Board has up to six directors, and not more than two Board members who are associates of the shareholder where the Board has seven or more directors. A director is taken to be an associate of a shareholder for the purposes of this Prudential Standard if the director is an associate of the shareholder, or the shareholder is an associate of the director, according to the definition of associate in clause 4 of Schedule 1 of the *Financial Sector (Shareholdings) Act 1998* (Financial Sector (Shareholdings) Act). That definition is to be applied for the purposes of this Prudential Standard as if subparagraph (1)(l) of that definition were omitted. (CPS 510, paragraph 34)

35. Where an individual shareholding is greater than 15 per cent, as approved under the Financial Sector (Shareholdings) Act, the Board representation of that shareholding may be greater than allowed in paragraph 34, although it must still be broadly proportionate to the shareholding concerned.[44] (CPS 510, paragraph 35)

[43] For the purpose of this Attachment, a 'substantial shareholder' is a person with a substantial holding as defined in section 9 of the Corporations Act.

[44] Note that, where the proportionate shareholding does not equate to a whole number, it may be rounded to the nearest whole number.

36. For a locally incorporated ADI that operates as a special service provider, the ADI may apply to APRA for approval for alternative Board composition arrangements that meet the objectives of this Prudential Standard. APRA may approve alternative arrangements for the ADI if satisfied that those arrangements will, in APRA's opinion, achieve the objectives of this Prudential Standard. (CPS 510, paragraph 36)

Board Audit Committee

73. An APRA-regulated institution (excluding foreign ADIs) must have a Board Audit Committee, which assists the Board by providing an objective non-executive review of the effectiveness of the institution's financial reporting and risk management framework. (CPS 510, paragraph 73)

74. The Board Audit Committee must have sufficient powers to enable it to obtain all information necessary for the performance of its functions. (CPS 510, paragraph 74)

75. The Board Audit Committee must have at least three members. All members of the Committee must be non-executive directors of the APRA-regulated institution. A majority of the members of the Committee must be independent. (CPS 510, paragraph 75)

76. The chairperson of the Board Audit Committee must be an independent director of the APRA-regulated institution. (CPS 510, paragraph 76)

77. The chairperson of the Board may be a member of the Board Audit Committee, but may not chair the Committee. (CPS 510, paragraph 77)

78. The Board Audit Committee must have a written charter that outlines its roles, responsibilities and terms of operation. The responsibilities of the Committee must include oversight of:

    (a) all APRA statutory reporting requirements;

    (b) other financial reporting requirements;

    (c) professional accounting requirements;

    (d) internal and external audit; and

    (e) the appointment and removal of that institution's auditor and Head of Internal Audit. (CPS 510, paragraph 78)

79. 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. (CPS 510, paragraph 79)

80. The Board Audit Committee must review the engagement of the auditor at least annually, including making an assessment of whether the auditor meets the Audit

Independence tests set out in APES 110 Code of Ethics for Professional Accountants,[45] as well as the additional auditor independence requirements set out in this Prudential Standard. (CPS 510, paragraph 80)

81. For a foreign ADI, the assessment referred to in paragraph 80 is the responsibility of the senior officer outside Australia. (CPS 510, paragraph 81)

82. 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. (CPS 510, paragraph 82)

83. The Board Audit Committee must ensure the adequacy and independence of both the internal and external audit functions. (CPS 510, paragraph 83)

84. 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. (CPS 510, paragraph 84)

85. The Board Audit Committee must ensure that the APRA-regulated institution maintains policies and procedures for employees of the institution to submit, confidentially, information about accounting, internal control, compliance, audit, and other matters about which the employee has concerns. The Committee must also ensure that the APRA-regulated institution has a process for ensuring employees are aware of these policies and for dealing with matters raised by employees under these policies. (CPS 510, paragraph 85)

86. Members of the Board Audit Committee must be available to meet with APRA on request. (CPS 510, paragraph 86)

87. The Board Audit Committee must invite the auditor and the Appointed Actuary, as applicable, to meetings of the Committee. (CPS 510, paragraph 87)

88. The internal auditor must have a reporting line and unfettered access to the Board Audit Committee. (CPS 510, paragraph 88)

Board Risk Committee

101. The Board of an APRA-regulated institution (excluding foreign ADIs) must have a Board Risk Committee, which assists the Board by providing an objective non-executive oversight of the implementation and operation of the institution's risk management framework. (CPS 510, paragraph 101)

102. The Board Risk Committee must be provided with the powers necessary to enable it to perform its functions. (CPS 510, paragraph 102)

[45] APES 110 Code of Ethics for Professional Accountants was issued by the Accounting Professional and Ethical Standards Board in December 2010.

103. The chairperson of the Board Risk Committee must be an independent director of the APRA-regulated institution. (CPS 510, paragraph 103)

104. The chairperson of the Board may be a member of the Board Risk Committee, but may not chair the Committee. The chair of the Board Audit Committee may also chair the Board Risk Committee. (CPS 510, paragraph 104)

105. The Board Risk Committee must have at least three members. All members of the Committee must be non-executive directors of the APRA-regulated institution. A majority of the members of the Committee must be independent. (CPS 510, paragraph 105)

106. The Board Risk Committee must have a written charter that outlines its roles, responsibilities and terms of operation. The responsibilities of the Committee must include:

    (a) advising the Board on the institution's overall current and future risk appetite and risk management strategy;

    (b) oversight of an institution-wide view of the institution's current and future risk position relative to its risk appetite and capital strength;

    (c) oversight of senior management's implementation of the risk management strategy;

    (d) constructive challenge of senior management's proposals and decisions on all aspects of risk management arising from the institution's activities;

    (e) reviewing the performance and setting the objectives of the institution's CRO,[46] and ensuring the CRO has unfettered access to the Board and the Committee; and

    (f) oversight of the appointment and removal of the CRO. (CPS 510, paragraph 106)

107. The Board Risk Committee is required to provide prior endorsement for the appointment or removal of the institution's CRO. If the CRO 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. (CPS 510, paragraph 107)

108. The Board Risk Committee must have free and unfettered access to senior management, risk and financial control personnel, and other parties (internal and external) in carrying out its duties. (CPS 510, paragraph 108)

109. The Board Risk Committee must invite the CRO to attend all relevant sections of meetings of the Committee. (CPS 510, paragraph 109)

[46] Refer to CPS 220.

4.2 CPS 511 Remuneration (2023)

Board oversight

21. The Board, or relevant oversight function, of an APRA-regulated entity is ultimately responsible for the entity's remuneration framework and its effective application. (CPS 511, paragraphs 21 (SFI) and 63 (non-SFI))

23. The Board must establish a Board Remuneration Committee that:

    (a) oversees the design, operation and monitoring of the remuneration framework;

    (b) is appropriately composed to enable it to exercise competent and independent judgment when fulfilling requirements under paragraph 23(a) above; and

    (c) has the powers necessary to perform its functions. (CPS 511, paragraph 23 (SFIs only))

31. An APRA-regulated entity must design all variable remuneration arrangements to align with paragraph 19 of this Prudential Standard and must incorporate in its variable remuneration arrangements:

    (c) appropriate variable remuneration adjustment tools, that include but are not limited to overriding board discretion at each decision point, in-period adjustments, malus and, where appropriate, clawback, which are supported by a downward-adjustments process:

        (i) with clearly identified triggers to make a downward-adjustment;

        (ii) that determines the appropriate adjustment tools to use; and

        (iii) that determines the amount of downward-adjustment, proportionate to the severity of risk and conduct outcomes, to nil if appropriate. (CPS 511, paragraphs 31(c) (SFI) and 65(c) (non-SFI))

CPG 511

6. SFI specific requirements include establishing a Board Remuneration Committee, applying a material weight to non-financial measures in variable remuneration arrangements, applying minimum deferral periods and clawback arrangements, and periodically reviewing the remuneration framework. (CPG 511, paragraph 6, (SFIs only))

8. Under CPS 511, the Board, or relevant oversight function, is ultimately responsible for the entity's remuneration framework and its effective application.[47] (CPG 511, paragraph 8)

[47] Relevant oversight function is defined in CPS 511. It is only applicable to foreign ADIs. Consistent with CPS 511 requirements, references to the Board and Board Remuneration Committee in this guidance refer to the relevant oversight function, where appropriate.

9. APRA expects Boards to ensure that remuneration practices are well supported by broader frameworks and policies that influence behaviour, beyond financial rewards. This includes clear accountabilities and expectations for risk management, effective consequence management and a strong tone from the top on risk culture. (CPG 511, paragraph 9)

10. In providing oversight of remuneration, other prudential standards and guidance are also applicable, in particular requirements on governance and risk management. Broader regulatory requirements and expectations, including guidance provided by the Australian Securities and Investments Commission (ASIC), are also relevant for the Board.[48] (CPG 511, paragraph 10)

17. There may be occasions where the Board would need to exercise its discretion to challenge and override remuneration recommendations, and make downward adjustments for individuals, cohorts or all personnel. (CPG 511, paragraph 17)

27. Specified roles are defined in CPS 511 and are intended to capture those individuals and cohorts who can have a material influence on the performance and risk profile of the entity, in both the short and long-term. Specified roles comprise senior managers, executive directors, material risk-takers (including highly-paid material risk-takers) and all risk and financial control personnel. (CPG 511, paragraph 27)

34. A prudent Board would closely monitor the remuneration of risk and financial control personnel as a cohort, to ensure arrangements are adequate to attract and retain suitably qualified, skilled and experienced staff.[49] (CPG 511, paragraph 34)

60. In assessing whether material weight[50] is being applied effectively in the design and determination of variable remuneration outcomes, a prudent Board would consider whether the weighting:

    (a) is a sufficient incentive to influence an individual's behaviour, priorities and decisions;

    (b) is robust and cannot be overshadowed or diminished by performance or outperformance on financial measures;

    (c) is applied to measures over which the individual has a reasonable degree of control and influence;

    (d) is applied to measures that effectively support the objectives of the remuneration framework, including risk management; and

---

[48] This would include ASIC guidance in Information Sheet 245 Board oversight of executive variable pay decisions, the Australian Securities Exchange's (ASX) Corporate Governance Council's Corporate Governance Principles and Recommendations, and the Financial Stability Board's (FSB) Principles of Sound Compensation Practices.

[49] Risk and financial control personnel are defined in CPS 511 as persons whose primary role is in risk management, compliance, internal audit, financial control or actuarial control.

[50] As per CPS 511, paragraph 32(a) [SFIs only], in determining each component of a person's variable remuneration, material weight must be given to non-financial measures where the remuneration is performance related.

(e) has been demonstrated to work in practice to incentivise prudent outcomes over time, where this is possible to determine. (CPG 511, paragraph 60, SFIs only)

62. A prudent Board would establish clear guidelines to ensure appropriate weight is applied to non-financial measures in the determination of variable remuneration. This could include a minimum level or range. Good practice would be for the Board to review these guidelines on an annual basis to ensure it is operating as intended in driving expected behaviours. (CPG 511, paragraph 62, SFIs only)

63. To assess whether the weighting for non-financial measures is driving intended behaviours and outcomes in practice, a prudent Board would consider how effectively risk and conduct is managed. Reporting on non-financial measures for the entity as a whole, as well as aggregate information on risk adjustments, would support this assessment. Entities with a high reliance on downward adjustments for adverse risk and conduct outcomes would investigate root causes and, where appropriate, consider if the weighting to non-financial measures needs to be increased or the design improved. (CPG 511, paragraph 63, SFIs only)

82. In gauging the severity of a case[51], a prudent entity would consider a range of factors. This would include the expected or actual impact on the entity's reputation, customers or beneficiaries and prudential standing, as well as any financial loss. An individual's contribution to circumstances which led to the adverse outcome would also be considered, potentially including inaction. Good practice would be to develop a severity scale, with example cases and any precedents, to guide decision-making on the level of severity and indicative remuneration impacts that would be expected to result. This scale would support a Board in applying proportionate downward-adjustments to variable remuneration, and in applying consistency across different cases. (CPG 511, paragraph 82)

88. The scope of the triennial review would encompass the role of the Board, the design of remuneration arrangements, and the effectiveness of risk and conduct adjustments. This would include any key design features, such as the definition of material risk-takers and the application of non-financial measures. The review would also assess the appropriateness of any remuneration adjustments made, to ensure that triggers and criteria for downward adjustments are prudently calibrated. (CPG 511, paragraph 88, SFIs only)

89. CPS 511 requires the triennial review to be conducted by operationally independent, appropriately experienced and competent persons. A prudent entity may consider the use of external expertise to meet this requirement. Where internal staff conduct the review, a prudent Board would gain assurance that they are operationally independent and are able to provide an objective review, with the requisite skills, experience and expertise. (CPG 511, paragraph 89, SFIs only)

[51] As per, CPS 511 paragraphs 36 and 68, an APRA-regulated entity must take reasonable steps to appropriately adjust variable remuneration downwards when, as a minimum, any of the criteria specified in paragraph 35 (or 67) are satisfied.

Board approval

22. The Board, or relevant oversight function, must approve the remuneration policy required under paragraph 20 of this Prudential Standard. (CPS 511, paragraphs 22 (SFI) and 64 (non-SFI))

50. The Board, or relevant oversight function, must approve the variable remuneration outcomes for persons in specified roles as follows:

    (a) individually for senior managers and executive directors;[52] and

    (b) on a cohort basis for highly-paid material risk-takers, other material risk-takers and risk and financial control personnel. (CPS 511, paragraphs 50 (SFI) and 74 (non-SFI))

57. In relation to the requirements for a Board Remuneration Committee and remuneration policy, where an APRA-regulated entity is part of a group, the Board of the APRA-regulated entity may:

    (a) use a group Board Remuneration Committee as the Board Remuneration Committee for the APRA-regulated entity, provided that:

        (i) the requirements set out in this Prudential Standard are met;

        (ii) all members of the group Board Remuneration Committee are non-executive directors of the Head of the group in the context of an ADI; and

        (iii) the Board of the entity has free and unfettered access to the group Board Remuneration Committee; and

    (b) adopt and apply a group remuneration policy that is also used by a related body corporate or a connected entity provided that the group remuneration policy:

        (i) meets the requirements of this Prudential Standard;

        (ii) has been approved by the Board or relevant oversight function; and

        (iii) gives appropriate regard to the entity's business activities, its specific requirements and its remuneration framework. (CPS 511, paragraph 57 (SFIs only))

75. In relation to the requirements for a remuneration policy, where an APRA-regulated entity is part of a group, the Board of the APRA-regulated entity may adopt and apply a group remuneration policy that is also used by a related body corporate or a connected entity provided that the group remuneration policy:

    (a) meets the requirements of this Prudential Standard;

[52] Paragraph 50(a)/74(a) of this Prudential Standard does not apply to a senior manager that is a senior officer outside Australia of a foreign ADI.

(b) has been approved by the Board or relevant oversight function; and

(c) gives appropriate regard to the entity's business activities, its specific requirements and its remuneration framework. (CPS 511, paragraph 75 (non-SFIs only))

CPG 511

18. A prudent Board would be actively engaged in the oversight of key remuneration decisions, providing robust challenge and independent scrutiny. Board oversight and discretion to adjust variable remuneration would be particularly relevant in unusual or exceptional circumstances. These circumstances may include:

    (a) material cases of adverse risk or conduct outcomes, especially where these have impacted the entity's prudential standing or prudential reputation;

    (b) periods of stress in which the entity may be experiencing negative financial performance and erosion of its regulatory capital base; and

    (c) periods of stress in which the entity is provided with exceptional public sector support. (CPG 511, paragraph 18)

19. It is important that the Board uses its discretion in a timely and informed manner, rather than acting only on the basis of realised outcomes. For example, it could be appropriate for a Board to reduce pre-emptively variable remuneration during a period of stress, rather than waiting for losses to be realised.[53] It would not be prudent to act only once risk issues are made public, to adopt management recommendations without challenge, or to excuse poor risk outcomes on the basis of good intent. (CPG 511, paragraph 19)

25. An entity that is part of a wider corporate group may adopt and apply the group remuneration policy, provided that it meets the requirements of CPS 511 and has been approved by the Board. Good practice would be for the entity to assess how the policy complies with each requirement of CPS 511, is appropriate for its specific business activities and risk profile, and meets the spirit and intent of the standard. (CPG 511, paragraph 25)

26. Under CPS 511, the variable remuneration outcomes for persons in specified roles must be approved by the Board, on either an individual or cohort basis. APRA expects the remuneration policy would define the particular specified roles for the entity, and summarise the remuneration arrangements for these roles. (CPG 511, paragraph 26)

29. As set out in CPS 511, the variable remuneration outcomes of all material risk-takers must be approved by the Board on a cohort basis.[54] Good practice is to develop, disclose and keep under review a threshold definition for material risk-takers, including

---

[53] For an ADI, good practice would be to take a forward-looking approach to reductions in discretionary bonus payments to staff, before being formally required to by the constraints imposed by the capital conservation buffer regime as set out in *Prudential Standard APS 110 Capital Adequacy*.

[54] A material risk-taker is defined in CPS 511 as a person whose activities have a material potential impact on the entity's risk profile, performance and long-term soundness.

quantitative indicators and qualitative criteria for the identification of such roles. (CPG 511, paragraph 29)

38. A prudent entity would take reasonable steps to identify which service providers may give rise to material conflicts or risks. This may include a materiality threshold or definition, approved by the Board, which would be used to identify the scale and nature of service providers that are likely to present a material conflict or risk. (CPG 511, paragraph 38)

Information for the Board

CPG 511

20. It is the responsibility of the Board and RemCo to guide management on the reporting it needs to fulfil its role. A prudent Board and RemCo would regularly review the information they are provided with to ensure that reporting is sufficient and insightful. Poor quality, inadequate, incomplete or voluminous reporting can significantly hamper oversight and challenge. (CPG 511, paragraph 20)

77. A prudent Board would consider a wide range of evidence and ensure appropriate mechanisms are in place to escalate issues. Good practice would be to consider, for example, known incidents, findings from audits and regulatory reviews, product failures, trends in conduct or risk incidents. APRA expects that a risk adjustment would be considered, for an individual or cohort, in the event of a breach of a prudential standard or other regulation. (CPG 511, paragraph 77)

Board Remuneration Committee

SFIs only

24. The Board Remuneration Committee must have at least three members and all members must be non-executive directors of the entity. (CPS 511, paragraph 24)

25. For an entity that is not an RSE licensee, a majority of members of the Committee must be independent and the chairperson of the Committee must be an independent director of the entity. (CPS 511, paragraph 25)

27. The Board Remuneration Committee must have a written charter that sets out its roles, responsibilities and terms of operation. (CPS 511, paragraph 27)

28. The Board Remuneration Committee, or relevant oversight function, must consult the Board Risk Committee[55] and CRO or person in a similar role, to enable risk outcomes to be appropriately reflected in remuneration outcomes for persons in specified roles. This consultation must follow a documented process. (CPS 511, paragraph 28)

29. The Board Remuneration Committee, or relevant oversight function, must obtain comprehensive reporting that will allow it to determine whether remuneration outcomes

[55] Consultation with a Board Risk Committee does not apply to a foreign ADI.

of all remuneration arrangements align with paragraph 19 of this Prudential Standard. (CPS 511, paragraph 29)

30. The Board Remuneration Committee, or relevant oversight function, in carrying out its duties must:

    (a) have free and unfettered access to other Board committees;

    (b) have free and unfettered access to risk and financial control personnel and other relevant parties (internal and external); and

    (c) if choosing to engage third-party experts, have the power to do so in a manner that ensures that the engagement, including any advice received, is independent. (CPS 511, paragraph 30)

47. The Board Remuneration Committee, or relevant oversight function, must provide clear guidance to senior management on its expectations in determining the appropriate level and timing of risk adjustment to the variable remuneration outcomes for persons in specified roles. (CPS 511, paragraph 47)

48. The Board Remuneration Committee must make recommendations to the Board annually on the remuneration arrangements and variable remuneration outcomes for persons in specified roles as follows:

    (a) individually for senior managers and executive directors;[56] and

    (b) on a cohort basis for highly-paid material risk-takers, other material risk-takers and risk and financial control personnel. (CPS 511, paragraph 48)

49. When forming its recommendations under paragraph 48 of this Prudential Standard, the Board Remuneration Committee must:

    (a) obtain sufficient information to enable remuneration outcomes to be commensurate with performance and risk outcomes; and

    (b) determine whether the variable remuneration arrangement, individually and on a cohort basis:

        (i) is appropriate to meet its intended purpose and expected remuneration outcomes; and

        (ii) supports the entity's compliance with paragraph 19 of this Prudential Standard. (CPS 511, paragraph 49)

54. An APRA-regulated entity must document and report the results of the reviews required under paragraphs 52 and 53 of this Prudential Standard to the Board Remuneration Committee, or relevant oversight function, in a timely manner. The Board Remuneration

[56] For the avoidance of doubt, paragraph 48(a) of this Prudential Standard applies to a senior manager who is a senior officer outside Australia of a foreign ADI.

Committee, or relevant oversight function, must take appropriate and timely action to ensure the findings of these reviews are adequately considered and addressed. (CPS 511, paragraph 54)

58. An APRA-regulated entity may apply to APRA for approval of alternative Board Remuneration Committee arrangements that meet the objectives of this Prudential Standard. APRA may approve alternative arrangements for the entity if satisfied that those arrangements will, in APRA's opinion, achieve the objectives of this Prudential Standard. (CPS 511, paragraph 58)

CPG 511

11. Under CPS 511, the Board of a SFI is required to establish a Board Remuneration Committee (RemCo) to oversee the design and implementation of the remuneration framework. The RemCo is responsible for making recommendations to the Board annually on the remuneration arrangements and variable remuneration outcomes for persons in specified roles. (CPG 511, paragraph 11)

12. A prudent Board would ensure that the RemCo is composed of members with the appropriate skills, experience and expertise to exercise competent and independent judgment. This includes a clear understanding of what constitutes good risk management. (CPG 511, paragraph 12)

14. In determining the variable remuneration outcomes for individuals and cohorts in specified roles, the assessment of performance and risk is a critical input. It is important for the RemCo to ensure it understands the performance and risk outcomes for persons in specified roles, as well as for the entity overall. (CPG 511, paragraph 14)

15. APRA expects that the assessment of performance and risk would include direct input from senior risk management personnel, and not be based on self-assessments alone. Good practice would be for risk and internal audit executives to present a comprehensive assessment of key risk and audit metrics on at least an annual basis, to inform remuneration decision making and outcomes. (CPG 511, paragraph 15)

16. Under CPS 511, the RemCo must consult the Board Risk Committee and CRO to enable risk outcomes to be appropriately reflected in remuneration outcomes for persons in specified roles. The use of joint meetings with the Board Risk Committee can be an effective mechanism for providing insights into risk considerations for the RemCo. It would not be prudent to rely on cross-membership between the RemCo and the Board Risk Committee as the sole means of providing a view on risk. (CPG 511, paragraph 16)

21. Good practice would be for the RemCo to be provided with formal documented performance and risk assessments for individuals in specified roles, and summaries for relevant cohorts such as risk and financial control personnel. This would include clear qualitative and quantitative assessments for measures that have formed the basis of decisions, including key metrics, and an outline of how assessments have flowed

through to remuneration outcomes.[57] It would not be prudent to rely on verbal discussion and generalised attestations as evidence of performance or risk assessments, or high-level summaries of major incidents. (CPG 511, paragraph 21)

22. Good practice for cohorts would be to assess, on an aggregated basis by business unit or role type, similar information to that which is reviewed for individual remuneration decisions. Additional information may also be useful, such as trends and outliers, summary indicators that show distributions, averages or medians, and other data-driven insights. (CPG 511, paragraph 22)

Non-SFIs

CPG 511

13. While the Board of a non-SFI is not required to establish a RemCo, it must put in place arrangements to meet the requirements of CPS 511 and ensure there is appropriate oversight of the remuneration framework and key remuneration decisions. (CPG 511, paragraph 13)

4.3 APS 330 Public disclosure (2018)

Board oversight

29. An ADI must take reasonable steps to ensure that its prudential disclosures reflect its actual risk profile and are consistent with the manner in which its Board and senior management assess and manage its risks. Where the minimum requirements for prudential disclosures set out in this Prudential Standard do not adequately capture this, the ADI must disclose additional information. (APS 330, paragraph 29)

Board approval

27. An ADI must have a formal policy relating to its prudential disclosures approved by the Board that addresses the ADI's approach to determining the content of its prudential disclosures and the internal controls over the disclosure process. (APS 330, paragraph 27)

4.4 CPS 520 Fit and proper (2019)

Board oversight

A.1 A responsible person of an ADI (other than a foreign ADI) or authorised banking NOHC is any person who is:

(a) a director of the APRA-regulated institution;

(b) a senior manager of the institution;

[57] A prudent Board would challenge any adjustments to quantitative metrics. This would include in particular any adjustments to profit measures that could affect whether hurdles for variable remuneration are met.

(c) an appointed auditor who provides any report in relation to the ADI that is required to be prepared by an auditor under the Banking Act, prudential standards made under the Banking Act or reporting standards under FSCODA;

(d) an appointed auditor who provides any report in relation to the authorised banking NOHC that is required to be prepared by an auditor under the Banking Act, prudential standards made under the Banking Act or reporting standards; or

(e) a person who performs activities for a subsidiary of the APRA-regulated institution where those activities could materially affect the whole, or a substantial part, of the business of the APRA-regulated institution or its financial standing, either directly or indirectly. (CPS 520, Attachment A, paragraph 1)

Board approval

13. The Fit and Proper Policy must be approved by the Board.[58] (CPS 520, paragraph 13)

16. Nothing in this Prudential Standard prevents an APRA-regulated institution from adopting and applying a group Fit and Proper Policy used by a related body corporate[59], provided that the policy has been approved by the Board in accordance with paragraph 13 and meets the requirements of this Prudential Standard. (CPS 520, paragraph 16)

Information for the Board

40. The Fit and Proper Policy must provide that a copy of the Policy is to be given to:

(a) any candidate for election as a director as soon as possible after the candidate is nominated; and

(b) any other person before an assessment of their fitness and propriety is conducted. (CPS 520, paragraph 40)

52. The Fit and Proper Policy must require that all provisions of the Policy encouraging whistleblowing, and the procedures related to whistleblowing, are adequately explained to directors and employees of the APRA-regulated institution and its subsidiaries who are likely to have information relevant to fit and proper assessments. (CPS 520, paragraph 52)

[58] A reference to the Board in the case of a foreign ADI is a reference to the senior officer outside Australia.

[59] Related body corporate has the meaning given in section 50 of the *Corporations Act 2001* (Corporations Act).

4.5 APS 310 Audit (2023)

Information for the Board[60, 61]

23. An ADI must ensure that the appointed auditor has access to all data, information, reports and staff of the ADI that the appointed auditor reasonably believes is necessary to fulfil its role and responsibilities under this Prudential Standard. This includes access to the ADI's Board, Board Committees and internal auditors as required. (APS 310, paragraph 23)

25. An ADI must ensure that the following are provided to its Board or Board Audit Committee (if not already sighted by the Board or Board Audit Committee):

    (a) reports provided by the appointed auditor in accordance with this Prudential Standard, and any associated assessments and other material provided by an appointed auditor to the ADI on request;

    (b) commentary or responses provided by APRA to the ADI on reports provided by the appointed auditor, and any associated assessments and other material; and

    (c) any commentary or response on the reports, associated assessments and other material provided by the appointed auditor that are given to APRA by the ADI. (APS 310, paragraph 25)

35. The responsibilities of the appointed auditor include reporting simultaneously (subject to paragraph 32) to APRA and the ADI's Board (or Board Audit Committee), within three months of the end of the financial year of the ADI[62], on:

    (a) the matters relating to APRA data collections; and

    (b) internal controls at both Level 1 and the Level 2 group;

    as referred to in paragraph 36. For this purpose, APRA data collections means any data collected in accordance with the *Financial Sector (Collection of Data) Act 2001* (FSCODA). (APS 310, paragraph 35)

40. Under the responsibilities of an appointed auditor for a special purpose engagement, the auditor's report must be submitted, within three months of the date of the notice commissioning the report, simultaneously to APRA and to the Board (or Board Audit Committee) of the ADI, unless otherwise determined by APRA, and advised to the ADI, by notice in writing (subject to paragraph 32). (APS 310, paragraph 40)

---

[60] As per APS 310, paragraph 7, in the case of a foreign ADI, a reference to the Board or a Board Committee in this Prudential Standard will be taken to refer to the senior officer outside Australia to whom authority has been delegated in accordance with *Prudential Standard CPS 510 Governance* (CPS 510). For a foreign ADI, a reference to the CEO refers to the senior manager in Australia with overall responsibility for the conduct of the foreign ADI's Australian operations.

[61] APS 310 paragraphs 5, 6 and 21 include additional requirements relating to non-operating holding companies (NOHCs).

[62] For non-disclosing entities the relevant period is four months.

Chapter 5 - Resolution

Resolution

This chapter sets out the specific obligations that apply to directors in respect to recovery, exit and resolution, including the Financial Claims Scheme (FCS). There is one relevant prudential standard included in this Guide, noting draft standards CPS 190 and CPS 900 are not yet in force.

- Recovery and exit planning: An ADI must be adequately prepared for scenarios that may impact the financial viability of their business. (draft CPS 190 summary box).
- Resolution: An ADI that is an SFI, or provides critical functions, is to support APRA in the development and implementation of a resolution plan. (draft CPS 900 summary box).
- FCS: A locally-incorporated ADI must meet minimum requirements to ensure that it is adequately prepared should it become a declared ADI for FCS purposes (APS 910 summary box).

5.1 APS 910 Financial Claims Scheme (2013)

Board oversight

30. It is the responsibility of the Board and senior management of an ADI to ensure that appropriate policies and procedures are in place to ensure the integrity of the operations, internal controls and information required by this Prudential Standard. (APS 910, paragraph 30)

Chapter 6 - For Boards of Level 3 groups and purchased payment facility (PPF) providers

Groups and PPFs

This chapter sets out the specific obligations that apply to directors in respect of Level 3 groups and purchased payment facilities (PPF) providers. As set out in the table below, there are 4 relevant prudential standards, supported by accompanying guidance.

- Level 3 groups: these standards and guidance relate to: obtaining and making available to APRA independent advice from an auditor (Audit and related matters); and ensuring that aggregate risk exposure, and associations and dealings, do not expose APRA-regulated entities within the group to excessive risk (Aggregate risk exposures; and Intra-group transactions, respectively) (*3PS 310, 3PS 221, 3PS 222, Objective and key requirements*).
- PPF: ADIs that have obtained an authority to provide PPFs are required to meet prudential requirements commensurate with their risk profile (*APS 610, Objective and key requirements*).

6.1 3PS 310 Audit (2017)

Information for the Board

15. A Level 3 Head must ensure that the Appointed Auditor has access to all data, information, reports and staff of the Level 3 group that the Appointed Auditor reasonably believes is necessary to fulfil its role and responsibilities under this Prudential Standard. This includes access to the Board and Board Audit Committee of the Level 3 Head, and the auditors of Level 3 institutions in the Level 3 group as required. (3PS 310, paragraph 15)

17. A Level 3 Head must ensure that its Board or Board Audit Committee are provided with:

    (a) reports provided by the Appointed Auditor in accordance with this Prudential Standard, and any associated assessments and other material provided by an Appointed Auditor to the Level 3 Head on request;

    (b) commentary or responses provided by APRA to the Level 3 Head on reports provided by the Appointed Auditor, and any associated assessments and other material; and

(c) any commentary or response on the reports, associated assessments and other material provided by the Appointed Auditor that are given by the Level 3 Head to APRA (3PS 310, paragraph 17)

26. The responsibilities of the Appointed Auditor include reporting simultaneously (subject to paragraph 23) to APRA and the Board or Board Audit Committee of the Level 3 Head, within three months of the end of the financial year of the Level 3 Head[63], on:

(a) matters relating to APRA data collections; and

(b) internal controls at a Level 3 basis,

as referred to in paragraph 27. For this purpose, 'APRA data collections' means any data collected in accordance with FSCODA. (3PS 310, paragraph 26)

31. Under the responsibilities of an Appointed Auditor for a special purpose engagement, the auditor's report must be submitted within three months of the date of the notice commissioning the report, simultaneously to APRA and to the Board (or Board Audit Committee) of the Level 3 Head, unless otherwise determined by APRA and advised to the Level 3 Head (subject to paragraph 23). (3PS 310, paragraph 31)

6.2 3PS 221 Aggregate risk exposures (2017)

Board oversight

12. The Board of a Level 3 Head must:

(a) approve the aggregate risk exposures policy for the Level 3 group;

(b) ensure that adequate systems and controls are in place to identify, measure, aggregate, manage, monitor and report on material risk exposures in the Level 3 group in a timely manner and that those systems and controls are documented;

(c) engage in oversight, which may be via a board committee, of the approach to the identification, measurement, management and monitoring of aggregate risk exposures and compliance with the aggregate risk exposures policy, which includes receiving regular reviews of material aggregate risk exposures of the Level 3 group; and

(d) review the aggregate risk exposures policy at least annually to ensure that this policy remains adequate and appropriate for identifying, measuring, aggregating, managing and monitoring the Level 3 group's risk exposures. (3PS 221, paragraph 12)

[63] For a Level 3 Head that is an ADI or non-operating holding company authorised under the Banking Act that is not a disclosing entity within the meaning of the *Corporations Act 2001*, the relevant period is four months.

3PG 221

1. The Board of a Level 3 Head (the Board) is responsible for the effective management of material risks posed to the Level 3 group. The Board is best positioned to have a holistic view of the risks posed to the group, and oversee controls to ensure that the group does not assume risks beyond its risk appetite. (3PG 221, paragraph 1)

2. 3PS 221 requires a Level 3 Head to establish and maintain an aggregate risk exposures policy. The policy is a part of the group's risk management framework and supports the ability to identify, measure, aggregate, manage and report on material aggregate risk exposures. An aggregate risk exposure refers to risks external to the Level 3 group that have the potential to result in losses for the Level 3 group, and can arise from the external exposures to prudentially regulated and non-prudentially regulated institutions. Risk data aggregation capabilities and risk reporting practices support the Board in making appropriate risk-based decisions in normal times and in periods of stress. (3PG 221, paragraph 2)

3. Material aggregate risks include those that could have a material impact, both financial and operational, on the Level 3 group or on a prudentially regulated institution in the group. APRA expects that the Board would determine what it considers to be a material aggregate risk, and that this would vary according to the group's risk profile. Where an institution is considered to have business operations that are material to the Level 3 group, a material external risk to that institution would normally constitute a material aggregate risk exposure for the group. (3PG 221, paragraph 3)

4. The materiality of an aggregate risk exposure depends on the size, nature and complexity of the exposure to the group. Where a material aggregate risk exposure is identified, the Board would also need to understand the material drivers of this risk. For instance, decision-makers may need to understand whether the aggregate risk exposure is comprised of a high number of small exposures or a low number of material individual risk exposures. (3PG 221, paragraph 4)

7. The Board is responsible for determining the appropriate level of aggregate risk exposures. The policy would be expected to outline the governance arrangements for procedures, systems and controls that are in place for the appropriate management of exposures. The Board is required to approve this policy but can delegate implementation of policy and oversight of exposures to a board committee, such as the Board Risk Committee. (3PG 221, paragraph 7)

10. 3PS 221 requires the aggregate risk exposures policy to include exposure limits that are commensurate with the Level 3 group's capital strength, risk appetite, risk profile, and the size, business mix and complexity of the group. A Board may consider how exposures of the Level 3 group interact to change the aggregate risk of the group. For instance, an exposure to an overseas counterparty would be considered as part of a limit to that counterparty and to the relevant geographical location. APRA expects that the Level 3 Head would have processes to confirm that the classifications of risks facilitate an appropriate assessment of the risk profile and to ensure the group does not assume more risk than its risk appetite. (3PG 221, paragraph 10)

11. 3PS 221 requires the aggregate risk exposures policy to outline the roles and responsibilities of the Board, its board committees, and senior management of the Level 3 group. APRA expects a Level 3 Head would also consider the role of the group's risk management function in supporting the management of material aggregate risk exposures. (3PG 221, paragraph 11)

12. APRA expects the Board and senior management of the Level 3 group to understand the limitations and assumptions relating to material aggregated risk exposures. A Level 3 Head is expected to use stress testing and scenario analysis to assess the adequacy of its aggregation capabilities and risk reporting. The results of these assessments would feed into the Board's awareness of aggregate risk exposures and would prompt consideration as to the Board's appetite for these exposures and the appropriateness of limits. In addition, these assessments would highlight any limitations with aggregation capabilities and risk reporting in periods of stress. (3PG 221, paragraph 12)

18. APRA expects a Level 3 group to have practices and procedures to identify data deficiencies and, where necessary, implement an improvement program so that data management does not impede effective risk management. Where there is a deficiency in data quality, APRA expects the Board to allocate sufficient oversight and resources for rectification. APRA expects that a Level 3 group would already have the data necessary for appropriate risk aggregation and that this data would not be encumbered by unnecessary barriers to retrieval, or rely on onerous manual adjustments for collation. (3PG 221, paragraph 18)

Board approval

19. A Level 3 Head must submit to APRA a copy of its aggregate risk exposures policy as soon as practicable, and no more than 10 business days, after Board approval. (3PS 221, paragraph 19)

Information for the Board

13. The aggregate risk exposures policy for a Level 3 group must:

    (d) include a description of the procedures for identifying, aggregating, reviewing, controlling and reporting material risk exposures within the Level 3 group. This must include:

        (i) a clear statement of the respective responsibilities and compliance obligations of the Board of the Level 3 Head, its board committees and senior management of the Level 3 group in relation to the monitoring and management of aggregate risk exposures;

        (iv) thresholds and procedures for reporting material changes to the Board of the Level 3 Head, in both formal reporting cycles and outside formal reporting cycles;

        (vi) a timetable for a regular review of the reports by the Board of the Level 3 Head. (3PS 221, paragraph 13 (d))

3PG 221

5. A Level 3 Head's governance arrangements, risk data aggregation capabilities and reporting would reflect how the Board makes decisions and oversees aggregate risk exposures. APRA expects that risk aggregation capabilities and risk reporting are relevant, appropriate for the intended purpose and meet business specifications (i.e. fit-for-purpose) for the needs of the Board and other decision-makers in the Level 3 group. (3PG 221 paragraph 5)

19. Good practice is that risk reporting is accurate, comprehensive, clear and useful, and can be provided to decision-makers on a timely basis. Risk reporting would be based on adequate aggregate risk data capabilities and be presented in a manner that is clear, concise and useful to the intended recipient. A Level 3 Head would determine respective risk reporting requirements that best suit the needs of its Board and the group's senior management given the size, business mix and complexity of the group. (3PG 221, paragraph 19)

20. APRA expects a Level 3 Head to have access to and commission both regular and flexible ad hoc reporting. The frequency of risk reporting depends on the needs of decision-makers. APRA expects reporting on material aggregate risk exposures to be presented to the Board at least quarterly. In periods of stress, given the speed of decision-making likely to be needed and that the nature of aggregate risks can change quickly, the frequency of reporting would be expected to increase. (3PG 221, paragraph 20)

21. The reporting of aggregate risk exposures to the Board would have sufficient breadth to provide the Board with a holistic view of the aggregate risk exposure profile of the Level 3 group. APRA expects that the Board would request reports for more detail on individual exposures or particular risk categories, accompanied by meetings with relevant senior management. Reporting would support the Board in understanding, and the senior management of the Level 3 group in understanding and tracking, aggregate risk exposures against the group's risk appetite and capital strength. (3PG 221, paragraph 21)

6.3 3PS 222 Intra-group Transactions and Exposures (2017)

Board oversight

10. The Board of a Level 3 Head must:

    (a) approve the Intra-group Transactions and Exposure (ITE) policy for the Level 3 group;

    (b) ensure that adequate systems and controls are in place to identify, measure, manage, monitor and report on material ITEs in the Level 3 group in a timely manner and that those systems and controls are documented;

    (c) engage in oversight, which may be via a board committee, of the approach to the identification, measurement, management and monitoring of ITEs and compliance

with the ITE policy, which includes receiving regular reviews of which ITEs are deemed to be material to the operations of the Level 3 group; and

(d) review the ITE policy at least annually, to ensure that this policy remains adequate and appropriate for identifying, measuring, managing and monitoring material risks in relation to ITEs. (3PS 222, paragraph 10)

3PG 222

1. ITEs expose Level 3 institutions in a Level 3 group to contagion risks. Where an institution is facing financial or operational stress, this may affect other institutions within the group with material ITEs to that institution. Therefore, the Board of a Level 3 Head (the Board) needs to understand the material ITEs within the group and manage the associated risks prudently. ITEs that can pose a risk of contagion would include, for example:

   (a) equity investments;

   (b) loan or funding arrangements;

   (c) reinsurance arrangements;

   (d) guarantees or indemnities; and

   (e) operational risks from intra-group service provision. (3PG 222, paragraph 1)

4. Material ITEs include those that would have a potential to have a material impact, both financial and operational, on the Level 3 group or a prudentially regulated institution in the group. APRA expects that the Board would determine what it considers to be a material ITE, and that this would vary according to the group's risk profile. Where an institution is considered to have business operations that are material to the Level 3 group, a material ITE to that institution would constitute a material ITE for the group. (3PG 222, paragraph 4)

5. The materiality of an ITE depends on the size, nature and complexity of the exposure to the group. Where a material ITE is identified, the Board would also need to understand the material drivers of this risk. For instance, decision makers may need to understand whether the ITE is comprised of a high number of low risk intra-group arrangements or a low number of material individual risk exposures. (3PG 222, paragraph 5)

8. APRA expects the Board to have a holistic view of material ITEs within the group and establish a framework to monitor and control the associated risks. The Board would consider the group's critical business operations and assess the potential impact of a stress on these operations to the group. (3PG 222, paragraph 8)

18. APRA expects a Level 3 group to have practices and procedures to identify data deficiencies and, where necessary, implement an improvement program so that data management does not impede effective risk management.[64] Where there is a deficiency

[64] Refer to CPG 235.

in data quality, APRA expects the Board to allocate sufficient oversight and resources for rectification. APRA expects that a Level 3 group would already have data on material ITEs and expects that this data would not be encumbered by unnecessary barriers to retrieval, or rely on onerous manual adjustments for collation. (3PG 222, paragraph 18)

Board approval

11. If a prudentially regulated institution in the Level 3 group proposes to accept terms and conditions, in dealing with Level 3 institutions in the group, that are not consistent with terms and conditions that would be negotiated on an arms-length basis in such a dealing, those terms and conditions must first be approved by the Board of the Level 3 Head with justification fully and clearly documented. (3PS 222, paragraph 11)

19. A Level 3 Head must submit to APRA a copy of its ITE policy as soon as practicable, and no more than 10 business days, after Board approval. (3PS 222, paragraph 19)

3PG 222

10. The risks associated with ITEs could be magnified where the transactions with related parties have not been conducted on an arms-length basis or on equivalent terms and conditions given to third parties. APRA expects a Level 3 Head to have processes and controls to mitigate such risks. In accordance with 3PS 222, the Board is required to approve these non-arm's length transactions. (3PG 222, paragraph 10)

Information for the Board

12. The ITE policy for a Level 3 group must:

    (c) include limits on acceptable levels of ITEs for a Level 3 institution in the Level 3 group having regard to:

        (i) the Level 3 institution's Board-approved limits on exposures to unrelated institutions of broadly equivalent credit status; and

    (d) include a description of the procedures for identifying, reviewing, controlling and reporting material ITEs within the Level 3 group. This must include:

        (i) a clear statement of the respective responsibilities and compliance obligations on the Board of the Level 3 Head, its board committees and senior management of the Level 3 group in relation to the monitoring and management of material ITEs;

        (vii) thresholds and procedures for reporting material changes to the Board of the Level 3 Head, in both formal reporting cycles and outside formal reporting cycles; and

        (viii) a timetable for a regular review of the reports by the Board of the Level 3 Head. (3PS 222, paragraph 12 (c) and (d))

3PG 222

6. A Level 3 Head's governance arrangements, data capabilities, and reporting in relation to ITEs would reflect how the Board makes decisions and oversees material ITEs. APRA expects data capabilities and ITE risk reporting to be relevant and appropriate for the intended purpose and to meet business specifications (i.e. fit-for-purpose) for the needs of the Board and other decision makers in the Level 3 group. (3PG 222, paragraph 6)

9. APRA expects a Level 3 Head to use stress testing and scenario analysis to assess the adequacy of its data capabilities and risk reporting on ITEs. The results of these assessments would feed into the Board's awareness of material ITEs and would prompt consideration as to the Board's appetite for these exposures and the appropriateness of limits. (3PG 222, paragraph 9)

19. Good practice is that risk reporting is accurate, comprehensive, clear and useful, and can be provided to decision makers on a timely basis. Risk reporting would be based on risk data and be presented in a manner that is clear, concise, and useful to the intended recipient. A Level 3 Head would determine respective risk reporting requirements that best suit the needs of its Board and senior management of the Level 3 group given the size, business mix and complexity of the group. (3PG 222, paragraph 19)

20. APRA expects a Level 3 Head to have access to commission both regular and flexible ad hoc reporting. The frequency of risk reporting depends on the needs of decision makers. APRA expects reporting on the group's material ITEs to the Board at least quarterly. In periods of stress, given the speed of decision-making likely to be needed and that the nature of risk can change quickly, the frequency of reporting would be expected to increase in such circumstances. (3PG 222, paragraph 20)

21. The reporting of material ITEs to the Board would have sufficient breadth to provide the Board with a coordinated view of the roles and relationships between subsidiaries to one another and to the Level 3 Head. This coordinated view would assist the Board in understanding, and senior management of the Level 3 group in understanding and tracking, how ITEs affect the risk profile of prudentially regulated institutions within the group. (3PG 222, paragraph 21)

22. APRA expects that the Board would request reports on material individual ITEs or the ITEs to particular institutions, accompanied by meetings with relevant senior management. Reporting would support the Board in understanding, and the Level 3 group's senior management in understanding and tracking, of ITEs against the group's risk appetite and capital strength. (3PG 222, paragraph 22)

6.4 APS 610 Prudential requirements for providers of purchased payment facilities (2015)

8. The Board of a PPF provider must ensure that the PPF provider maintains an appropriate level of capital commensurate with the level and extent of risks to which the PPF provider is exposed from its activities. To this end, the PPF provider must:

(a) have adequate systems and procedures in place to identify, monitor and manage the risks arising from its activities to ensure that capital is held at a level consistent with the PPF provider's risk profile; and

(b) maintain and implement a capital management plan, consistent with the overall business plan, for managing its capital levels on an ongoing basis. The plan must set out:

(i) the PPF provider's strategy for maintaining capital resources over time, for example, by outlining its capital needs for supporting the degree of risks involved in the PPF provider's business, how the required level of capital is to be met, as well as the means available for sourcing additional capital where required; and

(ii) actions and procedures for monitoring the PPF provider's compliance with minimum capital adequacy requirements, including the setting of trigger ratios to alert management of, and avert, potential breaches to the minimum capital required by APRA. (APS 610, paragraph 8)

13. The Board and senior management of a PPF provider must develop, implement and maintain a risk management framework to address operational risk that is appropriate to the size, complexity and business mix of the PPF provider. (APS 610, paragraph 13)

Glossary

Reference	Prudential standard full name
CPS 510	*Prudential Standard CPS 510 Governance*
CPS 511	*Prudential Standard CPS 511 Remuneration*
CPG 511	*Prudential Practice Guide CPS 511 Remuneration*
CPS 520	*Prudential Standard CPS 520 Fit and Proper*
APG 520	*Prudential Practice Guide APG 520 Fit and Proper*
APS 330	*Prudential Standard APS 330 Public Disclosure*
APS 310	*Prudential Standard APS 310 Audit and Related Matters*
3PS 310	*Prudential Standard 3PS 310 Audit and Related Matters*
CPS 220	*Prudential Standard CPS 220 Risk Management*
CPG 220	*Prudential Practice Guide CPG 220 Risk Management*
APS 220	*Prudential Standard APS 220 Credit Risk Management*
APG 220	*Prudential Practice Guide APG 220 Credit Risk Management*
APS 221	*Prudential Standard APS 221 Large Exposures*
3PS 221	*Prudential Standard 3PS 221 Aggregate Risk Exposures*
3PG 221	*Prudential Practice Guide 3PG 221 Aggregate Risk Exposures*
APS 222	*Prudential Standard APS 222 Associations with Related Entities*
3PS 222	*Prudential Standard 3PS 222 Intra-group Transactions and Exposures*
3PG 222	*Prudential Practice Guide 3PG 222 Intra-group Transactions and Exposures*
APG 223	*Prudential Practice Guide APG 223 Residential Mortgage Lending*
CPS 226	*Prudential Standard CPS 226 Margining and risk mitigation for non-centrally cleared derivatives*
CPG 229	*Prudential Practice Guide CPG 229 Climate Change Financial Risks*
APS 610	*Prudential Standard APS 610 Prudential Requirements for Providers of Purchased Payment Facilities*
CPS 231	*Prudential Standard CPS 231 Outsourcing*
CPG 231	*Prudential Practice Guide CPG 231 Outsourcing*

Reference	Prudential standard full name
CPS 232	*Prudential Standard CPS 232 Business Continuity Management*
CPS 234	*Prudential Standard CPS 234 Information Security*
CPG 234	*Prudential Practice Guide CPG 234 Information Security*
CPG 235	*Prudential Practice Guide CPG 235 Managing Data Risk*
APS 110	*Prudential Standard APS 110 Capital Adequacy*
APG 110	*Prudential Practice Guide APG 110 — Capital Buffers*
CPG 110	*Prudential Practice Guide CPG 110 – Internal Capital Adequacy Assessment Process and Supervisory Review*
APS 111	*Prudential Standard APS 111 Capital Adequacy: Measurement of Capital*
APS 112	*Prudential Standard APS 112 Capital Adequacy: Standardised Approach to Credit Risk*
APG 112	*Prudential Practice Guide APG 112 – Standardised Approach to Credit Risk*
APS 113	*Prudential Standard APS 113 Capital Adequacy: Internal Ratings-based Approach to Credit Risk*
APG 113	*Prudential Practice Guide APG 113 Internal Ratings-based Approach to Credit Risk*
APS 114	*Prudential Standard APS 114 Capital Adequacy: Standardised Approach to Operational Risk*
APG 114	*Prudential Practice Guide APG 114 Standardised Approach to Operational Risk*
APS 115	*Prudential Standard APS 115 Capital Adequacy: Standardised Measurement Approach to Operational Risk*
APG 115	*Prudential Practice Guide APG 115 Advanced Measurement Approaches to Operational Risk*
APS 116	*Prudential Standard APS 116 Capital Adequacy: Market Risk*
APG 116	*Prudential Practice Guide APG 116 Market Risk*
APS 117	*Prudential Standard APS 117 Capital Adequacy: Interest Rate Risk in the Banking Book (Advanced ADIs)*
APG 117	*Prudential Practice Guide APG 117 Interest Rate Risk in the Banking Book*
APS 180	*Prudential Standard APS 180 Capital Adequacy: Counterparty Credit Risk*
APS 210	*Prudential Standard APS 210 Liquidity*

Reference	Prudential standard full name
APG 210	*Prudential Practice Guide APG 210 Liquidity*
APS 120	*Prudential Standard APS 120 Securitisation*
APG 120	*Prudential Practice Guide APG 120 Securitisation*
APS 121	*Prudential Standard APS 121 Covered Bonds*
CPS 190	*Prudential Standard CPS 190 Recovery and Exit Planning*
CPS 900	*Prudential Standard CPS 900 Resolution Planning*
APS 910	*Prudential Standard APS 910 Financial Claims Scheme*

APRA