Risk & Compliance Committee Charter

Introduction

1. The Charter outlines the roles, responsibilities and composition of the Risk & Compliance Committee (**Committee**) of the Board of the Commonwealth Bank of Australia (**CBA** or **Bank**) and the manner in which it discharges its responsibilities for CBA and its subsidiaries (**Group**).

Purpose

2. The primary purpose of the Committee is to provide objective review and oversight across the Group for all categories of risk, setting risk appetite and ensuring an appropriate risk framework.

Role of the Committee

3. The Committee has been established to assist the Board in discharging its responsibilities on a range of matters relating to the oversight and review of:
   - The oversight and governance of risks impacting the Group;
   - The design, implementation and operation of the Group's Risk Management Framework (**RMF**) and Group's Risk Management Approach (**RMA**);
   - Monitoring the risk appetite and assessing the overall risk profile of the Group and within the material risk types;
   - Monitoring the effectiveness of the compliance management framework impacting the material risk types; and
   - Risk culture and behaviours.
4. The Committee is responsible for overseeing risk and risk-related activities of the Group, other than those that are the responsibility of the Board or delegated to other Board Committees.
5. The Board has delegated authority to the Committee to fulfil its responsibilities as set out in the section entitled *Responsibilities of the Committee* of this Charter and may make other delegations to the Committee from time to time.

Composition

6. The Board appoints the members and Committee Chair.
7. The Committee will consist of at least four directors, all of whom must be independent non-executive directors.
8. At least one member of the Committee is to have experience in identifying, assessing and managing risk exposures of large complex groups, and between them, the membership is to have the necessary technical knowledge and sufficient understanding of banking and financial services to be able to discharge its responsibilities.

9. The Group Company Secretary of the Bank, or such other person as the Board may nominate, will act as the Committee Secretary.

10. The Audit Committee Chair will be a member of the Committee, and the Committee Chair will be a member of the Audit Committee, this is to assist with the flow of relevant information between the two Committees.

11. At least one member of the Committee will be a member of the People & Remuneration Committee.

Role of the Chair

12. The Committee Chair must not be the Chair of the Board.

13. The Committee Chair is responsible to lead the Committee and oversee the processes for the Committee's performance of its role in accordance with this Charter.

14. The Committee Chair has specific responsibilities to:
    - Foster an open, inclusive and, where appropriate robust discussion and debate by the Committee;
    - Set the agenda with the Group Company Secretary, ensuring that appropriate time and attention is devoted to matters within the responsibilities of the Committee; and
    - Liaise with the Group Chief Risk Officer (**CRO**) to ensure the Committee has the information necessary to enable effective decision-making.

Meetings

15. The Committee will meet six times per year, or more frequently if necessary.

16. The presence of one-half of members of the Committee (rounded upwards if not a whole number) will constitute a quorum.

17. All CBA directors will have access to Committee papers and may attend Committee meetings.

18. The CRO, Chief Executive Officer (**CEO**), Chief Financial Officer and the Group Auditor will be invited to attend all Committee meetings.

19. The Committee will meet periodically with the CRO and biannually with the Chief Compliance Officer without management present.

20. The Committee will meet concurrently with the Nominations Committee, People & Remuneration Committee and Audit Committee, at least biannually, to:
    - consider material, financial, non-financial risk and people-related matters relevant to executive performance (including the performance of the Group Auditor) and the determination of the remuneration outcomes for the CEO, direct reports to the CEO and the Group Auditor;
    - share information about key matters where appropriate to ensure ongoing oversight of these matters; and

- consider and provide input into any other matters within the responsibility of the Committee.

21. The Committee will refer an issue to the Board or another Board Committee where the issue falls within the Board or that Board Committee's responsibility, or if it would benefit from having the Board or that Board Committee's consideration.

Access, reliance and advice

22. The Committee will have free and unfettered access to other Board Committees, the CEO and the CEO's direct reports, any other relevant internal and external party and information, and may make any necessary enquiries to fulfil its responsibilities.

23. The CRO and the Chief Compliance Officer will be provided with unfettered access to the Committee.

24. The CRO is responsible for the preparation, presentation, quality and integrity of information provided to the Committee.

25. The Committee may, with the prior approval of the Board Chair, where practicable, obtain independent advice at the Bank's expense. This includes by engaging and receiving advice and recommendations from appropriate independent experts. The engagement and any advice received will be independent of management.

26. Committee members are entitled to rely on information, advice and assurances provided by management on matters within their responsibility, and on the expertise of independent experts, as long as they are not aware of any grounds that would make such reliance inappropriate.

Responsibilities of the Committee

The Committee is responsible for:

Risk Management Framework

27. Overseeing the design, implementation and operation of the RMF (including key controls), and reviewing reports on the RMF to ensure that it continues to operate effectively within the risk appetite set by the Board.

28. Reviewing and recommending to the Board for approval of, and changes to, the Group Risk Appetite Statement (**RAS**).

29. Monitoring, and reporting to the Board on, the Group's current and future risk profile as assessed against the RAS and the implications of such assessment for either varying risk limits or recommended management actions.

30. Monitoring, and reporting to the Board on new and emerging sources of risk and the controls and mitigation measures put in place to deal with those risks.

31. Overseeing the design of the RMA and reviewing and recommending to the Board for approval the RMA.

32. Reviewing and approving, or endorsing to the Board for approval, the key risk frameworks and policies (including material changes to those

frameworks or policies) relating to the Group's material risk types, other than those that require, or are reserved for, Board approval or which have been delegated to management.

33. Overseeing management's implementation and the operation of the systems, policies and processes supporting the RMA, including by:
    - Overseeing the material changes to policies relating to the Group's material risk types which have been delegated to management;
    - Reviewing and recognising uncertainties, limitations and assumptions attached to the measurement of material risk types; and
    - Reviewing changes to operational and governance structures to ensure they continue to facilitate effective risk management, and making recommendations to the Board where required.

34. Participating in the capital adequacy assessment process, by reviewing and analysing the outcomes of Group-wide stress tests and their application in setting the Group's risk appetite and capital targets, following the Board's input into the development of stress testing scenarios.

35. Receiving and reviewing reports from Group management or any Board Committee:
    - On any significant breaches of, or material deviation from, the RMF;
    - On any material incident involving fraud or a break-down of risk controls; and
    - Relating to the resolution of significant risk matters and incidents, and monitoring management's remediation plans.

36. Reviewing information on risk-related issues reported under paragraph 35 above and identifying any thematic issues that require attention.

37. Reviewing the annual Risk Management Declaration (**RMD**) ahead of the RMD being considered by the Board.

38. Receiving and reviewing a triennial report (or more frequently if required) on the appropriateness, effectiveness and adequacy of the RMF to satisfy itself that the RMF continues to be sound and that the Group is operating with due regard to the risk appetite set by the Board.

39. Constructively challenging management's proposals and decisions on aspects of risk management and compliance matters arising from the Group's activities.

40. Considering any information arising at, and referred by, the Audit Committee that affects the appropriateness or effectiveness of the RMF or management of risk, and receiving periodic reports on credit portfolio assurance findings.

41. Providing information to the Audit Committee in relation to any significant internal control matter where the control is inadequate or has not operated, or is not operating as intended, and could have a significant impact on the Group's risk profile, including the RMF and risk appetite.

42. Reviewing a report from management during the RMD process, for subsequent consideration by the Board, to ascertain if the Committee and Board have fulfilled their prudential and other relevant compliance

responsibilities (including under the relevant Charters), and addressing any actions (if any) arising from the report.

Compliance

43. Review and approve the Group Operational Risk Management Framework and Group Compliance Management Framework.
44. Overseeing the framework implemented by management to effectively manage the Group's compliance risks which is part of the RMF.
45. Reviewing reports from management on the effectiveness of the Compliance Management Framework for identifying, monitoring and managing compliance with relevant obligations that may impact the material risk types.
46. Reviewing reports from management on the compliance processes that are in place to anticipate and effectively manage the impact of regulatory change on the Group's operations.
47. Reviewing reports from management on financial crime matters (including any material breaches of the Group Anti-Bribery and Corruption Policy, compliance with AUSTRAC obligations and modification instrument[1]).

Insurance matters

48. Oversee the adequacy of the Group's insurance program and making recommendations to the Board, having regard to the Group's business needs and the insurable risks.

Risk Culture

49. Guiding management to establish and maintain a sound risk culture, and reporting to the Board on risk culture-related matters that affect the Group's ability to operate consistently within its risk appetite, including any desirable changes to the risk culture.
50. Managing the process to ensure the Board is able to satisfy its obligations in respect of risk culture under prudential requirements.

Remuneration

51. Assessing, and reporting to the People & Remuneration Committee, any risk matter that warrants the People & Remuneration Committee's or the Board's consideration in recommending variable remuneration award or other outcomes for the CEO and the CEO Direct Reports and other personnel within the remit of the People & Remuneration Committee.

Risk Management Function

52. Approving, on the recommendation of the CEO, the appointment or removal of the CRO.
53. Setting the objectives for, and reviewing the performance of, the CRO. The remuneration outcomes are a matter for the People & Remuneration Committee and the Board to consider.
54. Approving, on the recommendation of management, the appointment or removal of the Chief Compliance Officer.
55. Monitoring the ongoing effectiveness and independence of the CRO, and also monitor the ongoing effectiveness of the Group risk function to ensure that it is appropriate for the size, business mix and complexity of the Group, including adequate resourcing.

[1] Anti-Money Laundering and Counter-Terrorism Financing (Modification-Commonwealth Bank of Australia Designated Business Group) Declaration 2021 (No.4).

US Requirements

56. Overseeing, in the capacity as Risk & Compliance Committee for the Group's US combined operations, the RMF and key policies relevant to the Group's US combined operations and compliance with the framework and policies.

Standing delegation

CBA Group

57. The Committee Chair is delegated authority to review and approve matters, where temporary changes are required to the risk appetite and risk indicator values set out in the Group RAS in exceptional circumstances, where it is necessary to expedite an approval prior to the next Committee or Board meeting.

58. The Committee Chair must report the details of any exercise of the authority delegated in the next Committee Report to the Board.

Reporting

59. Minutes of Committee meetings will be made available to all Board directors.

60. The Committee Chair will report on the business of Committee meetings to the Board and convey Committee recommendations.

61. The Committee will refer any matter relating to financial, tax and accounting risks to the Audit Committee.

Committee performance and Charter review

62. The Committee will assess its performance and the fulfilment of its responsibilities under the Charter annually (including having an external review every three years).

63. The Committee will review the adequacy of this Charter annually and recommend amendments to the Board for approval.

Other

64. Committee members will meet with relevant regulatory bodies upon request.

65. The Committee will perform any other responsibilities as may be delegated to it by the Board from time to time.

Approval date

Charter approved June 2023 (effective 10 August 2023)

Next review June 2024