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 of the Risk Management Framework (**RMF**) for all categories of risk across the Group.

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 governance of risks impacting the Group;
   - The design, implementation and operation of the 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 this Charter and may make other delegations to the Committee from time to time.

Composition

6. The Board appoints the members and Chair of the Committee.
7. The Committee will consist of at least four directors, all of whom must be independent non-executive directors of the Bank.
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 Chair of the Audit Committee will be a member of the Committee, and the Chair of the Committee 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 Chair of the Committee must not be the Chair of the Board.

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

14. The Chair of the Committee has specific responsibilities to:
    - Foster open, inclusive and, where appropriate, robust discussion and debate by the Committee;
    - Set the agenda with the Group Company Secretary, with appropriate time and attention allocated to matters within the responsibilities of the Committee; and
    - Liaise with the Group Chief Risk Officer (**Group CRO**) to provide the Committee with 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 the 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 Group CRO, Chief Executive Officer (**CEO**), Group Chief Financial Officer and the Group Auditor[1] will be invited to attend all Committee meetings.

19. The Committee will meet periodically with the Group 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 to:
    - at least annually, consider material financial, non-financial and people-related matters relevant to executive performance and the determination of the remuneration outcomes for the CEO, and the CEO's direct reports[2];

[1] The Group Auditor leads CBA's internal audit function.

[2] **CEO's direct reports** refers to all Group Executives (GEs) and excludes those direct reports of the CEO that are not GEs. The Board of ASB Bank Limited retains direct responsibility for any decision relating to the appointment, and performance and remuneration, of its Chief Executive Officer.

- at least annually, consider material financial, non-financial and people-related matters relevant to the performance and the determination of remuneration outcomes for the Group Auditor;
- share information about key matters where appropriate to facilitate 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's or that Board Committee's responsibility, or if it would benefit from having the Board's or that Board Committee's consideration.

Access, Reliance and Advice

22. The Committee will have free and unfettered access to other Board Committees, senior management, other employees (including risk and financial control personnel) and external advisors and information, and may make any necessary enquiries to fulfil its responsibilities.

23. The Group CRO and the Chief Compliance Officer have unfettered access to the Committee.

24. 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.

25. 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

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

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

28. 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.

29. 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.

30. Overseeing the design of the RMA, and reviewing and recommending to the Board for approval of, and changes to, the RMA.

31. Reviewing and approving key risk frameworks and policies for the Group's material risk types, including material changes to those frameworks and policies, except where approval is reserved for the Board or delegated to management.

32. 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 in order that they continue to facilitate effective risk management, and making recommendations to the Board where required.

33. Overseeing 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.

34. Reviewing and recommending to the Board for approval the Group Stress Testing Policy.

35. Reviewing reports from management or any Board Committee:
    - On any significant breaches of, or material deviation from, the RMF;
    - On any material incident involving fraud or a breakdown 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 considering any thematic issues that require attention.

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

38. Every three years, or more frequently if required, reviewing a report on the appropriateness, effectiveness and adequacy of the RMF so that the Committee can 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.

43. Overseeing management's implementation and the operation of the frameworks, policies, processes, and controls supporting the management of cyber security risk across the Group.

Compliance

44. Reviewing and approving the Group Operational Risk Management Framework and the Compliance Management Framework.

45. Overseeing the framework implemented by management to effectively manage the Group's compliance risks which is part of the RMF.

46. Reviewing and recommending to the Board:
    - for approval, the business continuity plans and tolerance levels for disruptions to critical operations;
    - for reviewing, the results of testing of those plans; and
    - for oversight, the status of management's progress to address any findings.

47. Reviewing and recommending to the Board for approval, the Group Service Provider Policy, and reviewing risk and performance reporting on material service providers.

48. 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.

49. 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.

50. Reviewing reports from management on financial crime matters (including any material breaches of the Group Anti-Bribery and Corruption Policy and other financial crime compliance obligations).

Insurance matters

51. Overseeing 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

52. Overseeing the development and maintenance of 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.

53. Overseeing the process of supporting the Board in satisfying its obligations in respect of risk culture under prudential requirements.

Remuneration

54. 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's direct reports and other personnel within the remit of the People & Remuneration Committee.

Risk Management Function

55. Approving, on the recommendation of the CEO, the appointment or removal of the Group CRO.

56. Setting the objectives for, and reviewing the performance of, the Group CRO. The remuneration and remuneration outcomes are a matter for the People & Remuneration Committee and the Board to consider.

57. Approving, on the recommendation of management, the appointment or removal of the Chief Compliance Officer.

58. Monitoring the ongoing effectiveness and independence of the Group CRO, and also monitoring the ongoing effectiveness of the Group risk function including by considering whether it is appropriate for the size, business mix and complexity of the Group, including adequate resourcing.

US Requirements

59. 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

60. The Chair of the Committee 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.

61. The Chair of the Committee will report any exercise of their standing delegation at the Committee's next meeting.

Reporting

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

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

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

Committee Performance and Charter Review

65. The Committee will assess its performance and the fulfilment of its responsibilities under the Charter annually. An external Board and Committee performance review is also undertaken at least every three years.

66. The Committee will review the adequacy of this Charter every two years and recommend amendments to the Board for approval.

Other

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

68. 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 2026 (effective 13 August 2026)
Next review	June 2028