

4011 Board Risk & Compliance Committee Charter – V11.0

Authorisations		Review	
Approval Authority:	Board	Date Approved:	26 May 2025
Recommended by:	Risk & Compliance Committee	Next Review:	July 2027
Maintenance Responsibility:	Company Secretary	Review Period:	2 Years

CONTENTS

1. Introduction	2
2. Standing Rules	2
3. Purpose	2
4. Responsibilities	2
5. Membership	9
6. Meetings	9
7. Committee Secretary	9
8. Board directions	9
9. Responsible Person	9
10. Access and administration	9

1. Introduction

- 1.1 The Risk & Compliance Committee (**Committee**) is a committee of the Board of Directors (**Board**) of Teachers Mutual Bank Limited (**Company**).
- 1.2 The Committee has been established and appointed by the Board in accordance with the Company's Constitution (**Constitution**). The Committee is a key part of the Company's Corporate Governance Framework and Risk Management Framework.
- 1.3 This Charter, including the Standing Rules referred to in para. 2, outlines the purpose, responsibilities, composition, authority and operating rules of the Committee, and the manner in which the Committee discharges its responsibilities.
- 1.4 The Committee's responsibilities apply in relation to the Company and its wholly-owned subsidiaries (**Corporate Group**).

2. Standing Rules

- 2.1 The Company's Board Committee Standing Rules (**Standing Rules**) apply to the Committee, except where expressly excluded in this Charter or by a resolution of the Board.
- 2.2 If there is any inconsistency between the terms in this document and the Standing Rules, the terms in this document prevail to the extent of the inconsistency.

3. Purpose

- 3.1 The Board approves the Corporate Group's Risk Management Strategy (**RMS**), sets the risk appetite for the Corporate Group within which it expects management to operate, including by approving the Corporate Group's Risk Appetite Statement (**RAS**), and is ultimately responsible for the Corporate Group's overall risk management framework for all material risk classes across the Corporate Group (together the "**Risk Management Framework**"), including oversight of its operation by management.
- 3.2 The primary purpose of the Committee is to assist the Board in the effective discharge of its responsibilities in relation to oversight of the Risk Management Framework, including by providing objective oversight of the Corporate Group's risk profile, risk appetite, the implementation and operation of the Risk Management Framework and management of material risks, and the Company's risk culture.
- 3.3 In discharging its responsibilities, the Committee will seek to ensure that the strategies, frameworks, policies and practices it oversees comply with legal and regulatory requirements, align with the Company's purpose and values, and are consistent with the Company's strategic objectives and risk appetite.

4. Responsibilities

The responsibilities of the Committee include:

Risk Management Framework

- 4.1 Reviewing, and making recommendations to the Board in relation to, the RMS, including, where required, recommending changes to the Board for approval.
- 4.2 Reviewing, and making recommendations to the Board in relation to, the Corporate Group's current and future risk appetite (including key risk appetite metrics, limits and tolerances), including, where required, recommending changes to the Board for approval.
- 4.3 Monitoring the effectiveness of governance structures and arrangements for the oversight of the Risk Management Framework and the management of material risks.

- 4.4 Overseeing the design, implementation and operation, including the adequacy and effectiveness, of the Risk Management Framework (including key controls), in line with the RMS and the Board-approved risk appetite, including by:
- (a) monitoring, including by receiving reports from management on, an enterprise-wide view of the Corporate Group's current and future risk profile relative to the Board-approved risk appetite and the Corporate Group's capital strength and financial and operational resilience, and the implications of such assessment for either varying key risk appetite metrics, limits and/or tolerances or recommended management actions;
 - (b) monitoring, including by receiving reports from management on:
 - (i) the Company's key material risks by material risk class; and
 - (ii) the implementation and operation of key frameworks, systems, policies, processes and controls supporting the RMS, including those required to facilitate the identification and effective and consistent assessment and management of the Company's material risks (including the effectiveness of key controls) across the Corporate Group;
 - (c) reviewing, and making recommendations to the Board in relation to, key risk management and compliance frameworks and policies (including material changes) for the management of material risk classes that are subject to review by the Committee, as set out in the Company's Policy Register or directed by the Board;
 - (d) receiving reports from management on the identification, development, implementation, monitoring and testing of key risk controls and the outcomes of regular control effectiveness assessments and recommended management actions;
 - (e) considering and recognising uncertainties, limitations and assumptions in relation to the measurement of material risks;
 - (f) receiving reports from management or other Board committees on:
 - (i) compliance with key risk management policies, limits and tolerances;
 - (ii) any significant breaches of, or material deviations from, the Risk Management Framework, including significant incidents involving a breakdown of risk controls or where management becomes aware that the Risk Management Framework does not adequately address a material risk, and recommended management actions;
 - (iii) the resolution of significant risk exposures, events, incidents or other matters, and the completion and closure of significant remediation plans or other actions;
 - (iv) the risk profile and performance of credit portfolios, including portfolio composition, risk concentrations, portfolio analytics, arrears performance, provisioning, non-performing loans and loss performance; and
 - (v) new or emerging risks that may materially impact the Company's risk profile, relevant market, economic and regulatory developments, and management's plans to manage these risks and developments; and
 - (g) constructively challenging management's proposals and decisions on all aspects of risk management and compliance matters arising from the Corporate Group's activities that may have a material impact on the Corporate Group,
- and reporting and making recommendations to the Board as required.
- 4.5 Reviewing risk-related matters escalated or referred to the Committee by management, another Board committee, Internal Audit, the External Auditor, a regulator or other external party for consideration by the Committee, including requests from management for risk acceptance, and reporting and making recommendations to the Board as required.

- 4.6 Reviewing the outcomes of scenario and sensitivity analysis and stress testing of the Corporate Group's material risks (including resilience to operational risks) and reporting and making recommendations to the Board as required.
- 4.7 Monitoring the completion, and approving the closure, of significant risk-related issues or actions.

Risk culture

- 4.8 Monitoring, and assisting the Board in guiding, the Company's risk culture, including:
 - (a) advising and making recommendations to the Board to support the Board in satisfying its obligations in relation to risk culture under prudential requirements, including forming a view of the Company's risk culture and, where required, identifying required changes and monitoring the implementation of those changes;
 - (b) monitoring the adequacy and effectiveness of the approach outlined in the RMS for ensuring staff and others within the Company have awareness of the Risk Management Framework as it relates to their role and for instilling an appropriate risk culture across the Corporate Group;
 - (c) reporting to the Board on risk culture-related matters, including those that affect the Company's ability to operate consistently within the Board-approved risk appetite; and
 - (d) monitoring the extent to which risk culture contributes to other targeted risk management outcomes.

Triennial comprehensive review of Risk Management Framework

- 4.9 Receiving and considering the report on the triennial comprehensive risk management review by an independent expert of the appropriateness, effectiveness and adequacy of the Risk Management Framework (including the Company's management of operational risks) required under Prudential Standard CPS 220 Risk Management (**CPS 220**) and Prudential Standard CPS 230 Operational Risk (**CPS 230**), including whether the:
 - (a) Risk Management Framework is implemented and effective; remains appropriate, taking into account the Company's current business plan; remains consistent with the Board-approved risk appetite; and is supported by adequate resources; and
 - (b) RMS accurately documents the key elements of the Risk Management Framework that give effect to the Company's strategy for managing risk.

CPS 220 annual risk management declaration

- 4.10 Reviewing, and making recommendations to the Board in relation to, the annual Risk Management Declaration required under CPS 220 (**Risk Management Declaration**) and supporting assurances and other reports and declarations before the risk management declaration is presented to the Board for review and approval, including:
 - (a) reviewing the External Auditor's annual APS 310 Audit & Related Matters Report;
 - (b) reviewing the report on the most recent triennial comprehensive risk management review;
 - (c) reviewing a report from management, for subsequent consideration by the Board, to ascertain if the Committee and Board have fulfilled their prudential and other relevant compliance responsibilities, and addressing any actions (if any) arising from the report;
 - (d) reviewing a report from Internal Audit and/or the External Auditor and any recommendations of the Audit Committee, for subsequent consideration by the Board, in relation to the Company's compliance with, and the effectiveness of, the Risk

Management Framework, including having regard to the declarations in the Risk Management Declaration; and

- (e) receiving and considering recommendations from the CEO; the CRO; the Internal Auditor and/or the External Auditor; and the Audit Committee, in relation to the Risk Management Declaration,

and reporting and making recommendations to the Board as required.

- 4.11 Monitoring the completion, and approving the closure, of any action items arising from the annual and comprehensive reviews of the Risk Management Framework under CPS 220.

Compliance Framework

- 4.12 Reviewing, and making recommendations to the Board in relation to, the Corporate Group's compliance management framework (**Compliance Framework**), including, where required, recommending changes to the Compliance Framework to the Board for approval.

Note: The Compliance Framework is part of the Risk Management Framework.

- 4.13 Overseeing the implementation and operation of the Compliance Framework, including reviewing reports from management and/or, as required, other Board committees and/or external parties, in relation to the adequacy and effectiveness of the Compliance Framework for:
 - (a) identifying, assessing and managing material compliance risks;
 - (b) monitoring compliance with Board-approved frameworks and policies;
 - (c) monitoring compliance with legal and regulatory requirements (including prudential requirements), industry and other codes to which the Company subscribes, and other external obligations;
 - (d) anticipating and effectively managing the impact of regulatory change on the Corporate Group's operations; and
 - (e) monitoring the design and implementation of remediation plans.
- 4.14 Reviewing reports from management on significant findings and recommendations in relation to the Compliance Framework, including the Company's compliance with its obligations, and monitoring management's responses to any such findings and recommendations.
- 4.15 Overseeing the adequacy of resourcing of the Company's compliance function.

Insurance program

- 4.16 Overseeing the Corporate Group's insurance strategy and the adequacy of the Corporate Group's insurance program, including by reviewing reports from management and/or external parties on the insurance strategy and insurance program (including coverage, limits and other material terms, premiums and market trends), and making recommendations to the Board, having regard to the Corporate Group's business needs and insurable risks.

Other responsibilities

The responsibilities of the Committee also include:

Note: The following additional responsibilities do not limit the more general responsibilities of the Committee described above and are included to assist with the demarcation of responsibilities and co-ordination between the Board's committees.

ICAAP

4.17 Participating in the Internal Capital Adequacy Assessment Process (**ICAAP**) to support compliance with Prudential Standard APS 110 Capital Adequacy (**APS 110**), by, at least annually:

- (a) reviewing reports and recommendations from management, and making recommendations to the Board in relation to, the development of key assumptions and methodologies to be used in the ICAAP, including for scenario and sensitivity analysis and stress testing;
- (b) reviewing reports from management, and making recommendations to the Board in relation to, the outcomes of ICAAP scenario and sensitivity analysis and stress testing and their application in setting the Corporate Group's capital targets and tolerances;
- (c) reviewing, and making recommendations to the Board in relation to, the Company's:
 - (i) ICAAP summary statement (**ICAAP Statement**);
 - (ii) annual report on the implementation of its ICAAP (**ICAAP Report**); and
 - (iii) policy for reviewing its ICAAP, including key roles and responsibilities (**ICAAP Policy**); and
 - (iv) reviewing, and making recommendations to the Board in relation to, the annual capital management declaration by the CEO required under APS 110 (**Capital Management Declaration**) and supporting assurance and other reports and declarations before the ICAAP Report and Capital Management Declaration are presented to the Board for review and approval, including:
 - (A) reviewing the processes undertaken throughout the year to support the ICAAP Report and the CEO's ability to conduct due enquiry and make the required Capital Management Declaration;
 - (B) receiving and considering recommendations from the CEO; the CRO; Internal Audit and/or the External Auditor; and the Audit Committee, in relation to the Capital Management Declaration;
 - (C) receiving and considering a report from Internal Audit on its annual review of the ICAAP and Capital Management Declaration and any recommendations from the Audit Committee on ICAAP-related matters, including, where appropriate, recommending the ICAAP Summary Statement, ICAAP Report, ICAAP Policy and Capital Management Declaration to the Board for approval before submission to APRA, where required.

4.18 Monitoring the completion, and approving the closure, of any action items arising from the Committee or Board's annual review of the ICAAP.

Operational resilience - Critical operations and tolerances levels and material service providers

4.19 Reviewing reports from management on the identification, assessment and management of material operational risks, including the Company's resilience to operational risks and disruptions.

- 4.20 Reviewing, and making recommendations to the Board in relation to, the Company's critical operations and tolerance levels under CPS 230, including, where required, recommending changes to the Board for approval.
- 4.21 Reviewing reports from management on the identification, assessment and management of material operational and other risks arising from the Company's use of material third party service providers.
- 4.22 Reviewing, and making recommendations to the Board in relation to, the Company's Service Provider Management Policy, including, where required, recommending changes to the Board for approval.

Business Continuity Plan

- 4.23 Reviewing, and making recommendations to the Board in relation to, the Company's business continuity plan(s) (**BCP**) required under Prudential Standard CPS 230 at least annually, including, where required, recommending changes to the Board for approval.
- 4.24 Monitoring, and considering the outcomes of, reviews and testing of the BCP as required under CPS 230, including periodic audit and other assurance reviews of the BCP.
- 4.25 Reviewing reports from management on the adequacy of Company's resources and capabilities to execute the BCP.
- 4.26 Monitoring the completion, and approving the closure, of any action items arising from the review of the BCP.

Recovery and Exit Plan

- 4.27 Reviewing, and making recommendations to the Board in relation to, the Company's recovery and exit plan(s) (**Recovery and Exit Plan**) required under Prudential Standard CPS 190 Recovery and Exit Planning at least every three years, including, where required, recommending changes to the Board for approval.
- 4.28 Monitoring the completion, and approving the closure, of any action items arising from the review of the Recovery and Exit Plan.

Risk incidents and regulatory breaches

- 4.29 Reviewing reports from management on material themes and trends in risk incidents and regulatory breaches, including management's responses.

Technology, information and cyber security and data risks

- 4.30 Reviewing reports from management on the identification, assessment and management of material technology (including digital technology and artificial intelligence), information and cyber security, and data-related risks.

Fraud and financial crime

- 4.31 Reviewing reports from management on financial crime-related matters, including compliance with AML/CTF obligations and the Company's Anti-Bribery and Corruption Policy.
- 4.32 Reviewing reports from management on:
 - (a) the identification, assessment and management of material fraud and financial crime (including AML/CTF) related risks;
 - (b) material incidents involving proven or suspected internal fraud; and
 - (c) significant incidents involving proven or suspected external fraud.
- 4.33 Reviewing, and making recommendations to the Board in relation to, the Company's AML/CTF Program Part A and Anti-Bribery and Corruption Policy, including, where required, recommending changes to the Board for approval.

Modern slavery risks

- 4.34 Reviewing, and making recommendations to the Board in relation to, the Company's annual Modern Slavery Statement required under the *Modern Slavery Act 2018* (Cth), including, where required, recommending changes to the Board for approval.

Departmental risk reviews

- 4.35 Reviewing reports from individual Executives (excluding the CEO) on material risk-related matters within the area(s) of the business they are accountable for (**Department**), including how they manage and oversee risk management and compliance and monitor material risks within their Department.

Risk management function**Effectiveness and independence, resources and roles and responsibilities**

- 4.36 Monitoring the ongoing effectiveness and independence of the Company's CRO and risk management function, and the adequacy of resourcing of the risk management function, including by considering whether the risk management function is appropriate for the size, business mix and complexity of the Corporate Group.
- 4.37 Ensuring the Company has clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks.

Chief Risk Officer (CRO)

- 4.38 In consultation with the CEO, overseeing, and making recommendations to the Board in relation to:
- (a) the appointment of the CRO; and, if required, the removal of the CRO; and
 - (b) the setting of objectives for, and the review of the performance of, the CRO.

Note: The remuneration outcomes of the CRO are a matter for the People & Remuneration Committee and the Board to consider, with input from the Committee.

Note: If the CRO is removed from their role, the reasons for the removal must be discussed with APRA as soon as practicable (and, in any event, within 10 business days of the removal decision).

Auditors and other Board committees**Auditors**

- 4.39 Receiving and considering reporting from Internal Audit and/or the External Auditor on audit issues and insights relating to risks, controls and/or risk culture.
- 4.40 Reviewing any issues raised by Internal Audit or the External Auditor that concern the Risk Management Framework or the Corporate Group's management of risk.

Other Board committees

- 4.41 Considering any information arising at a meeting of, and/or any issues referred by, another Board committee that concerns or affects the adequacy or effectiveness of the Risk Management Framework or the Corporate Group's management of risk.
- 4.42 Providing information to the Audit Committee in relation to any significant internal control weakness, deficiency, gap or other matter, including where the control is inadequate or is not operating effectively or as intended, that comes to the attention of the Committee and which could have a significant impact on the Corporate Group's financial statements.
- 4.43 The Committee may refer any matter relating to financial, accounting or taxation-related risks to the Audit Committee.
- 4.44 The Committee may refer any matter relating to people and conduct-related risks to the People & Remuneration Committee.

- 4.45 Consulting with the People & Remuneration Committee and the Board to enable risk-related matters and outcomes to be appropriately reflected in performance and remuneration (including variable remuneration) assessments and outcomes for management accountable persons under the Financial Accountability Regime, other persons in specified roles (as defined in the Prudential Standard CPS 511 Remuneration) and other persons within the remit of the People & Remuneration Committee.

5. Membership

- 5.1 The Committee must consist of at least four members, including the Committee Chair.
- 5.2 As per para. 5.3 of the Standing Rules, a majority of the members of the Committee must be independent, Non-Executive Directors of the Company (as defined in Prudential Standard CPS 510 Governance).

6. Meetings

- 6.1 The Committee will meet at least four times each calendar year.

7. Committee Secretary

- 7.1 The Responsible Person (or their delegate), or such other person as the Board may appoint, will be the secretary of the Committee (**Committee Secretary**).

8. Board directions

- 8.1 The Board may, at any time, and in its absolute discretion, give directions to the Committee as to the procedures it is to follow.

9. Responsible Person

- 9.1 The Executive responsible for the Committee is the Chief Risk Officer (referred to in the Standing Rules and this document as the **"Responsible Person"**).

10. Access and administration

- 10.1 The CRO will have a direct reporting line to the CEO and regular unfettered access to the Committee and the Board.
- 10.2 Without limiting para. 12 of the Standing Rules, the Committee may meet with the CRO, the Internal Auditor and/or the External Auditor without management present at any time, including when requested by the CRO, the Internal Auditor and/or the External Auditor.
- 10.3 Without limiting para. 7.2 of the Standing Rules, the Committee Chair will call a meeting of the Committee if requested to do so by any Committee Member, the CEO, the CRO, the Internal Auditor and/or the External Auditor.

End.