Approved 4 May 2026

Terms of Reference – Risk Management Committee (RMC)

1. Purpose

The Risk Management Committee (RMC) is established as part of the Second Line of Defense under FSBM's Enterprise Risk Management (ERM) Framework.

It provides oversight, governance, and strategic direction for Group-wide risk management, ensuring that risk information from the Risk Working Group (RWG) and business units is evaluated, escalated, and addressed in alignment with FSBM's risk appetite, strategic objectives, and regulatory obligations.

2. Objectives

The RMC's objectives are to:

1. Oversee the implementation, adequacy, and effectiveness of FSBM's ERM Framework across all business and functional areas.
2. Review and monitor key risks, including strategic, financial, operational, compliance, health, safety, environmental, project, and reputational risks.
3. Evaluate consolidated risk reports, risk registers, and Key Risk Indicators (KRIs) submitted by the RWG.
4. Endorse Group-level risk treatment plans and ensure that appropriate mitigation and control measures are in place.
5. Recommend risk appetite levels, risk policies, and significant mitigation strategies to the Board Risk Committee (BRC).
6. Promote a consistent and proactive risk-aware culture throughout FSBM.

3. Roles & Responsibilities

Governance and Oversight

- Ensure risk management practices are integrated into strategic and operational planning.
- Review the adequacy of risk treatment plans, mitigation actions, and internal controls.
- Endorse updates or amendments to the ERM Policy and Framework for Board approval.
- Oversee emerging risks, regulatory developments, and changes in FSBM's external environment that may impact risk exposure.

Monitoring and Reporting

- Review quarterly Corporate Risk Reports and significant departmental risk registers consolidated by the RWG.

- Evaluate the effectiveness of Key Risk Indicators (KRIs) and ensure early warning signals are acted upon.
- Monitor implementation of corrective and preventive actions for high or significant risks.
- Ensure that all high-rated or strategic risks are escalated promptly to the Board Risk Committee.

Advisory

- Provide guidance to the RWG and Business Units on risk prioritization and resource allocation.
- Recommend training, awareness, and capacity-building initiatives to strengthen the risk culture.
- Support Management in aligning business strategies with the Group's risk appetite and tolerance.

4. Membership & Meetings

The RMC shall comprise of selected representatives from the Board to ensure adequate cross-functional oversight.

The RMC shall convene at least quarterly, and additionally when material risks or emerging issues require attention. The Secretariat shall circulate the agenda and relevant documents at least five (5) working days prior to each meeting.

5. Reporting

The RMC shall:

- Receive monthly risk reports and quarterly consolidated risk updates from the RWG.
- Submit quarterly Corporate Risk Reports to the Board Risk Committee and Audit Committee.
- Ensure significant and high-rated risks, control failures, or emerging risk trends are escalated promptly to the Board.
- Provide feedback and recommendations to the RWG to improve operational risk management practices.

6. Authority

The RMC is authorised to:

- Access any necessary information, documentation, or personnel relevant to risk management.
- Direct the RWG and business units to implement corrective measures or enhanced controls.
- Commission risk assessments, scenario analyses, or independent reviews as required.
- Recommend policy changes, resource allocations, and strategic responses to emerging risks.

7. Relationship to Other Committees

Committee	Interaction
Board of Directors (BOD)	Receives quarterly reports and recommendations from the RMC. Provides strategic oversight and final approval of Group risk policies.
Risk Working Group (RWG)	Reports to the RMC on operational and departmental risk status and escalations.
Business Units / Departments	Serve as the First Line of Defense, responsible for identifying, assessing, and controlling risks within their scope.

8. Review of Terms of Reference

This Terms of Reference shall be reviewed annually by the Risk Lead in consultation with the RMC and RWG, to ensure continued relevance, alignment with FSBM's ERM Policy and Framework, and compliance with ISO 31000 and Bursa Malaysia Corporate Governance guidelines.