SBM HOLDINGS LTD

RISK MANAGEMENT COMMITTEE – TERMS OF REFERENCE

1. RESPONSIBILITIES

The Committee shall carry out the following roles and responsibilities on behalf of the Board, within its delegated authority:

1.1 Risk Governance and Enterprise Risk Management Framework

1.1.1 Ensure the establishment, maintenance and consistent implementation of a robust and effective Enterprise Risk Management Framework ("ERMF") across the Group

1.1.2 Implement a risk-based approach to ensure that risk management efforts commensurate with the scale, nature and complexity of the risks identified across all subsidiaries and business lines

1.1.3 Advise the Board on, and review, the adequacy, effectiveness, and regulatory alignment of the ERMF, including underlying risk management frameworks, methodologies and internal controls

1.1.4 Oversee the Three Lines of Defence model, ensuring clear delineation of risk ownership, oversight, and assurance across the Group

1.1.5 Review and approve significant changes to the ERMF, risk policies, and risk governance structures

1.2 Risk Appetite and Risk Profile

1.2.1 Review and recommend the Group Risk Appetite Statement ("RAS") to the Board for approval on an annual basis, or more frequently as conditions require

1.2.2 Oversee and challenge the risk appetite framework, ensuring its ongoing relevance, effective implementation, and alignment with macroeconomic conditions and regulatory expectations

1.2.3 Monitor the Group's risk profile, Key Risk Indicators ("KRIs") and concentrations against approved appetite

1.2.4 Review breaches of risk limits, including the adequacy and timeliness of management actions and remediation

1.3 Oversight of Principal Risks

1.3.1 Review and assess the Group's exposure to financial and non-financial risks, including emerging risks, in the context of its risk appetite

1.3.2 Ensure appropriate frameworks, governance, and reporting are in place, and evaluate the Group's capacity to effectively manage and mitigate these risks

1.4 Financial Risk Oversight

1.4.1 Credit Risk: Oversee credit risk governance frameworks, including concentration risk, large exposures, provisioning methodologies (IFRS 9) and impairment assessments

1.4.2 Market Risk: Review market risk exposures (e.g. interest rate, foreign exchange, commodity), VaR limits and trading book governance

1.4.3 Liquidity and Funding Risk: Oversee liquidity risk management, the Internal Liquidity Adequacy Assessment Process ("ILAAP"), contingency funding plans and adherence to regulatory liquidity ratios (such as Liquidity Coverage Ratio and Net Stable Funding Ratio)

1.4.4 Capital Adequacy: Review the Internal Capital Adequacy Assessment Process("ICAAP"), capital adequacy ratios, capital planning and stress scenarios in line with Basel III/IV requirements

1.5 Operational Risk Oversight

1.5.1 Oversee the operational risk management framework including loss event reporting, risk and control self-assessments ("RCSAs") and KRIs

1.5.2 Review material operational risk events, near-misses and management actions

1.5.3 Ensure appropriate governance structures for the management of model risk, third-party/outsourcing risk and conduct risk

1.6 Cybersecurity and Information Security Risk

1.6.1 Oversee the Group's cybersecurity strategy, framework and governance, including alignment with international standards

1.6.2 Receive regular reports from the Chief Information Officers on the cyber threat landscape, material incidents, vulnerability assessments and remediation actions

1.6.3 Review the adequacy of information security policies, data classification, access controls and third-party cyber risk management

1.6.4 Oversee compliance with applicable data protection and privacy regulations across all jurisdictions (e.g., Mauritius Data Protection Act 2017, GDPR-equivalent requirements in operating jurisdictions)

1.6.5 Ensure annual independent cyber-risk assessments and penetration testing results are reviewed and acted upon

1.7 Business Continuity and Operational Resilience

1.7.1 Oversee the entities of the Group Business Continuity Management ("BCM') framework, including Business Continuity Plans ("BCPs"), Disaster Recovery Plans ("DRPs") and Recovery Time / Recovery Point Objectives (RTOs/RPOs)

1.7.2 Ensure BCPs and DRPs are tested at least annually and that results, gaps and remediation plans are reported to the Committee

1.7.3 Review the Group's operational resilience strategy, including identification of critical business services and impact tolerances as required by applicable regulators

1.7.4 Receive reports on significant business disruptions and assess the adequacy of recovery actions

1.8 Major Incident and Crisis Management

1.8.1 Oversee the Group's Crisis Management Framework ("CMF"), ensure it is tested regularly and have clear escalation procedures, defined roles and responsibilities and appropriate crisis response capabilities

1.8.2 Receive timely reports on all major incidents (operational, cyber, reputational, financial, environmental or other) affecting the Group or its subsidiaries and assess management's response

1.8.3 Ensure appropriate post-incident reviews are conducted and that lessons learned are embedded into risk frameworks and controls

1.8.4 Oversee the Group's Crisis Communication Plan, ensuring pre-approved communication protocols are in place for engagement with regulators, shareholders, customers, media, and other key stakeholders during a crisis

1.8.5 Ensure the Crisis Communication Plan is aligned with the Group's reputational risk policy and regulatory notification obligations across all operating jurisdictions

1.9 Occupational Health and Safety ("OHS") Risk

1.9.1 Oversee the Group's OHS risk management and ensure compliance with applicable OHS legislation in all jurisdictions it operates

1.9.2 Receive periodic reports on OHS incidents, near-misses, workplace injury rates and regulatory inspections

1.9.3 Ensure that OHS risks are adequately reflected in the operational risk framework and that management action plans address identified deficiencies

1.10 Compliance Risk Oversight

1.10.1 Oversee the effectiveness, independence and adequacy of resourcing of the Compliance function across the Group

1.10.2 Monitor the Group's exposure to compliance risk, including:

- Anti-Money Laundering and Combating the Financing of Terrorism ("AML/CFT")
- Completion and reporting of Enterprise-Wide Risk Assessment ("EWRA"), both at a consolidated Group level and at respective entity level
- International sanctions (OFAC, UN, EU, and domestic)
- Financial crime and fraud prevention
- Market conduct and fair customer treatment
- Consumer protection and complaints management
- Regulatory reporting obligations
- Data protection and privacy compliance

1.10.3 Review significant regulatory breaches, enforcement actions, remediation plans, and supervisory engagement outcomes

1.10.4 Promote a strong compliance culture and zero-tolerance approach to non-compliance across the Group

1.10.5 Review the annual Compliance Risk Assessment and Compliance Monitoring Plan

1.11 Legal Risk Oversight

1.11.1 Oversee the Group's exposure to legal risk, including material litigation, regulatory actions, contractual disputes, and changes in applicable laws across operating jurisdictions

1.11.2 Review significant legal matters, including their potential financial, operational and reputational impact

1.11.3 Ensure robust frameworks for legal risk identification, escalation and management are in place

1.11.4 Monitor the adequacy of provisions for legal matters and the appropriateness of related disclosures in financial statements and regulatory returns

1.11.5 Receive reports on legislative and regulatory developments in all jurisdictions that may materially affect the Group's risk profile or compliance obligations

1.12 Strategic and Transactional Risk Oversight

1.12.1 Evaluate risks arising from material strategic initiatives, including mergers, acquisitions, divestitures, joint ventures, new market entry, new product launches and significant investments

1.12.2 Ensure alignment with the Group's risk appetite and long-term strategic objectives

1.12.3 Review due diligence findings and seek independent advice where appropriate

1.13 Environmental, Social, and Governance ("ESG") and Climate Risk

1.13.1 Oversee the integration of climate risk and ESG-related risks (physical risk, transition risk) into the ERMF, in alignment with regulatory expectations and international frameworks (e.g. Task Force on Climate Related Financial Disclosures "TCFD")

1.13.2 Review the Group's ESG risk exposures and the adequacy of scenario analysis for climate-related financial risks

1.14 Whistleblowing and Ethical Conduct

1.14.1 Oversee the independence and confidentiality of the Group Whistleblowing Framework

1.14.2 Ensure robust protections against retaliation and integrity and impartiality of investigation processes

1.14.3 Review whistleblowing reports, including trends and outcomes, and assess the effectiveness of the whistleblowing framework and processes through analysis of reported data and resolution timelines

1.14.4 Promote an ethical culture and tone from the top across the Group

1.15 Risk Culture and Conduct

1.15.1 Oversee the Group's conduct risk framework, including fair treatment of customers, market integrity and staff behaviour

1.15.2 Oversee risk culture across the Group, including accountability structures, behavioural indicators and incentive alignment with prudent risk-taking

1.15.3 Review the outcome of conduct risk assessments and monitor management actions to address identified conduct issues

1.16 Risk Data, Technology and Reporting

1.16.1 Oversee the integrity, accuracy, completeness and timeliness of risk data and reporting, aligned to regulatory principles

1.16.2 Ensure adequate systems, data infrastructure and data governance frameworks support risk reporting requirements across all Group entities

1.17 Stress Testing and Resilience

1.17.1 Review and challenge the design, assumptions and outcomes of the entities of the Group's stress testing and scenario analysis programmes, including regulatory stress tests and internal stress tests

1.17.2 Oversee the alignment of stress-testing frameworks with Basel III/IV requirements and applicable central bank guidelines

1.17.3 Ensure stress-testing results are integrated into capital planning, risk appetite setting and strategic decision-making

1.18 Controls, Internal Audit Liaison and Remediation

1.18.1 Review the effectiveness of the internal control environment and risk mitigation measures across the Group

1.18.2 Oversee the timely closure of internal and external audit findings, independent review, regulatory inspection findings and remediation plans

1.18.3 Ensure prompt escalation to the Board of any material control failures or unacceptable residual risks

1.18.4 Receive reports from Internal Audit on the scope and results of risk-focused audits

1.19 Oversight of Risk and Compliance Functions

1.19.1 Oversee the performance, independence, effectiveness, and adequacy of resourcing of the Risk and Compliance functions at Group and subsidiary level

1.19.2 Ensure both functions are empowered with clear mandates, appropriate structures and direct access to the Committee and the Board

1.19.3 Review and approve the annual risk and compliance work plans and budgets

1.20 Subsidiary and Cross-Border Risk Oversight

1.20.1 Review and challenge risk exposures, risk appetite alignment and risk management practices across all subsidiaries of the Group

1.20.2 Ensure material risks identified at subsidiary level are escalated promptly to the Committee and, where appropriate, to the Board

1.20.3 Oversee cross-border risk, including regulatory, geopolitical, currency and country risk exposures

1.20.4 Ensure risk governance standards are consistently applied across subsidiaries, with appropriate localisation for regulatory requirements

1.21 Reporting and External Disclosures

1.21.1 Review and recommend the Risk Management Report of the Integrated Annual Report to the Board for approval

1.21.2 Ensure that risk disclosures are accurate, comprehensive and aligned with regulatory expectations and applicable accounting standards

1.22 Training and Risk Awareness

1.22.1 Oversee risk training and awareness programmes across the Group, ensuring they are relevant, current and effectively delivered

1.22.2 Receive periodic reports on risk training completion rates and the effectiveness of awareness initiatives

1.23 Succession Planning

1.23.1 The Committee shall, in coordination with the Corporate Governance and Conduct Review Committee and the Nomination & Remuneration Committee, oversee the succession planning process for the Executive Management (Risk, Compliance and Legal)

1.23.2 Ensure that succession plans for key Second Line of Defence roles are robust, reviewed at least annually and maintain the technical competence, independence and authority of the Risk, Compliance and Legal functions

1.23.3 Review the adequacy of emergency succession protocols and interim arrangements for unplanned vacancies in critical risk compliance and legal roles at both Group and subsidiary levels

1.24 Engagement with Management

1.24.1 Meet periodically with the Group Chief Risk Officer ("GCRO"), Group Head of Compliance ("GHoC") and Group Head of Legal ("GHoL"), including meetings without Management present

1.24.2 Ensure that the GCRO, GHoC and GHoL have direct and unfettered access to the Board and Committee

1.25 Other Responsibilities

1.25.1 Consider reports from the Group Risk Management Forum and the Group Compliance Forum, review risk-related strategic initiatives and enhancements, and perform any other duties delegated by the Board