Committee Terms of Reference

Risk & Compliance

For People. For Better.

Regulated by the Central Bank of Kenya

RISK & COMPLIANCE COMMITTEE TERMS OF REFERENCE

ESTABLISHMENT OF COMMITTEE

The Board of Directors of KCB Group Plc (the "Board") has established a Committee of the Board known as the Risk & Compliance Committee (the "Committee").

PURPOSE

The purpose of the Committee is to assist the Group Board in meeting its oversight of the following activities in line with the Groups consolidated oversight obligations:

- Group strategy, capital allocation alignment and financial budgets.
- Digital and cyber and innovation strategy.
- Material investments/M&A, and
- performance and governance oversight of strategic matters of the banking and non-banking subsidiaries, including material intra-group and related-party transactions.
- ESG strategy and integration.

MEMBERSHIP

- The Committee shall consist of a minimum of three (3) directors of the Board, a majority of whom must be independent non-executive directors.
- One member who is a Non-Executive Director shall serve as the Committee Chairman (the "Chair"). The Members of the Committee and the Chair shall be appointed and removed by the Chairman of the Board.
- In the absence of the Chair, one of the other members of the Committee present shall be chosen by the Committee to preside as Chair at that meeting.
- Each member shall serve as a member of the Committee until a successor is appointed, unless the member resigns, is removed or ceases to be a director.
- If a member is unable to act for any reason, the Chair of the Board may co-opt another independent Non-Executive Director as an additional member if deemed necessary.
- The Chair of the Board will, on an annual basis, review the performance of the Committee.

MEETINGS & PROCEDURE

a) Frequency of Meetings

The Committee shall meet at least four (4) times in a year with other meetings held as required.

b) Quorum

The quorum shall be two (2) members both of whom must be independent Non-Executive Directors. No member is permitted to appoint a proxy.

Attendance of meetings may include physical appearance, telephone or video conferencing provided that all participants in the meeting can be heard simultaneously.

c) Decisions

The Committee's decisions shall, to the extent possible, be by consensus. Where no consensus is reached, the Committees decisions shall be taken by a majority of votes of those present. In case of a tie, the Chair shall have a casting vote.

The Chair shall at his sole discretion and as he deems appropriate use the casting vote or refer the matter to the full board for decision.

A Committee member is required to abstain from deliberations and voting in respect of any matter which may give rise to any actual or perceived conflict of interest situation.

d) Circular Resolution
The Committee may from time to time and if deemed appropriate, consider and approve and/or recommend relevant matters via a circular resolution in writing including through the Company's electronic board platform, in lieu of formally convening a meeting.

The circular resolution shall be as valid and effectual as if it has been passed by a meeting of the Committee duly convened. Approval of the Committee obtained through a circular resolution must be signed by or approved by all Committee members subject to paragraph (c) above

e) Attendance at Meetings
The Group Chief Risk Officer or his delegate and, where relevant, appropriate internal attendees and external advisers, may attend meetings of the Committee by invitation.

f) Committee Secretary
The Company Secretary shall be the Secretary to the Committee and shall be responsible for providing guidance on all governance issues and for taking minutes of the proceedings of all meetings of the Committee.

g) Reporting to the Board
The Chair or his designate shall report to the Board on matters arising at Committee meetings and, where applicable, present the Committee's recommendations to the Board for its approval.

AUTHORITY OF THE COMMITTEE

The Committee is authorised by the Board:

- To investigate any activity within its Terms of Reference.
- To seek any information, it requires from any employee, chairperson of other Board committee, executive director, and officer or Company Secretary within its Terms of Reference and/or subject to following a Board approved process.
- To access the Company's records, facilities and any other resources necessary to discharge its duties and responsibilities subject to the Board approved process.
- To obtain external legal or other independent professional advice, including an external remuneration consultant that it determines necessary to permit it to carry out its duties at the Company's expense, subject to the Board approved process being followed. To instruct external professional advisers to attend any meeting if it considers this necessary or appropriate.

DUTIES AND RESPONSIBILITIES

The Committee shall have the following responsibilities as well as any other matters that may be delegated to the Committee by the Board from time to time.

a) Establish standards of business conduct and ethical behaviours for directors, managers and other personnel, including policies on private transactions, self-dealing, and other transactions or practices of an arm's length nature.

b) Risk Management

1. **Risk Governance & Appetite**

- Approve and/or recommend for Board approval the Risk Governance Framework and Risk Appetite Statement, including quantitative and qualitative measures; receive regular risk dashboards and escalate breaches.
- Oversee material risk types: credit, market, liquidity, operational (incl. cyber/technology), model, strategic, reputational and conduct risk.

- Evaluate and report to the board the Group's overall current and future risk strategy, tolerance and risk appetite in relation to both financial and nonfinancial risks.
- Review on behalf of the Board the aggregated risk profile for the Group and performance against risk appetite
- Ensure that the Group's overall risk profile and risk appetite remain appropriate given the evolving external environment, any key issues and themes impacting the Group and the internal control environment.
- Periodically review and approve the methodology used to establish the Group's risk appetite, stress testing and scenario analysis.
- Ensure the incorporation of risk intelligence into the strategy of the Group.
- Monitor risk profile on a consolidated basis, including intra-group exposures and concentration risks, consistent with NOHC consolidated supervision.

2. **Risk Frameworks and Governance**

- Oversee the development and implementation of enterprise risk management policies, procedures and plans to ensure a systematic and disciplined approach to risk management, internal control, compliance and governance processes within the Group.
- Ensure that appropriate policies are maintained to govern all areas of the entire KCB Group's activities, such that all activities are conducted in accordance with prudent practices as approved by the Board.
- Review reports on any material breaches of risk limits and the adequacy of proposed remediation actions.
- Review and asses the integrity of the risk management systems and monitor the effectiveness of the formal and informal communication of risk strategies, frameworks, policies, procedures, and limits throughout the Company.
- Assess and monitor the independence, adequacy and effectiveness of the Group Risk function.
- Assist the board in setting the company's risk culture towards achievement of a risk minimization and reward balance for risks accepted. Embed a culture where people at every level manage risk as an intrinsic part of their jobs.
- Review and endorse statements in relation to financial and non-financial risk made in the risk management section of the integrated report prepared annually.
- Review the Company's procedures for the prevention of bribery.
- Review and monitor management's responsiveness to the findings and recommendations of the Group Chief Risk Officer.

3. Risk Assessment and Reporting

- Review the Company's overall risk assessment processes that inform the Board's decision making, ensuring both qualitative and quantitative metrics are used.
- Regularly review and approve the parameters used in risk measurement and the methodology adopted.
- Oversee management's responsibilities to assess and manage the Group's risk profile in relation to Credit, Market, ICT, Operational, Compliance/regulatory, reputational, Strategic and Country risks.
- Oversee the accurate, timely monitoring and reporting of critical risks and exposures that may affect the Risk Profile of the Group and strategies for addressing them considering the full range of risks and potential interactions among risks and provide guidance as to the appropriate action to be taken where necessary.
- Review and evaluate the Group ICAAP report which aims to assess all important risks undertaken by the Group and determine capital requirements of the Group.

- Continually obtain reasonable assurance from management that all known and emerging risks for all risk areas have been identified and mitigated or managed through appropriate processes and systems.
- Review crisis management plans.

4. **Climate-Related Financial Risks**

- Oversee integration of climate risks (physical and transition) into risk identification, appetite, metrics, scenario analysis, and reporting; ensure governance and disclosure approaches align with CBK Climate Risk Guidance.

5. **Regulatory Compliance and Supervisory Matters**

- Oversee compliance frameworks; review significant regulatory developments, examinations/inspections, and remediation plans across the Group.

6. **Whistleblowing, AML/CFT/CPF and Financial Crime**

- Ensure that Whistleblowing policies and procedures allow proportionate and independent investigation of matters and appropriate follow up action.
- To review reports on detection and prevention of financial crime, including anti-bribery and corruption, anti-money laundering and sanctions.
- Oversee the AML/CFT/CPF framework, including risk assessment, KYC/CDD, sanctions, monitoring, FRC reporting, and effectiveness reviews, consistent with POCAMLA and CBK's supervisory mandate.

c) Assess performance of the Group Chief Risk Officer.

d)Evaluate and review the Committees performance and its compliance to its terms of reference and report to the Board.

e)Assess the appropriateness of its Terms of Reference, taking into account any applicable legislative and regulatory requirements, as well as best practices and report to the Board .

DELEGATION OF DUTIES AND RESPONSIBILITIES

The Committee may delegate any of its duties or responsibilities, as it deems appropriate, to any of its members or sub-committee of its members, to such other persons, subject to the Committee's direction and supervision, and with the express condition that the Committee retains full and exclusive authority over and responsibility for any activities of such other person or persons. Nothing contained in this paragraph shall be construed to confer upon any such person or persons any discretion, authority or control respecting any matter, unless expressly authorised in writing.

REVIEW AND APPROVAL

These Terms of Reference shall be reviewed every three years and where necessary appropriate changes and updates made.

Original Issue Date	Mar 2026
Approver:	KCB Group Plc Board
Date Approved:	Mar 2026
Owner:	KCB Group Risk & Compliance Committee Chair
Last Revision Date:	N/A
Next Review Date:	Mar 2029
Version	V1

SCHEDULE OF REVISION

Date of Approval/Revision	Content	Reason
2026	New Terms of reference	New TORs approved for implementation.


KCB
www.kcbgroup.com
For People. For Better.
Regulated by the Central Bank of Kenya