

Board Risk and ESG Committee Terms of Reference

Table of Contents

1.0 Objectives	3
2.0 Authority	3
3.0 Membership	3
4.0 Committee Meetings	4
4.1 Frequency of Meetings:	4
4.2 Notification of Meetings and Agenda Items	4
4.3 Attendance at Meetings and Minutes	4
5.0 Roles and Responsibilities	5
5.1 Risk Management and Internal Controls	5
5.2 Environmental, Social and Governance	6
5.3 Reporting Responsibilities	6
5.4 Other Responsibilities	6
6.0 Conflict of Interest	7
7.0 Performance of the Committee	7
8.0 Review of Terms of Reference	7

1.0 Objectives

Safaricom PLC operates in a complex and dynamic business environment characterized by various risks and challenges. The company recognizes the importance of effective risk management and the integration of environmental, social, and governance (ESG) considerations into its operations. To enhance the Board of Directors' oversight and governance in these areas, the establishment of a dedicated Board Risk and ESG Committee is crucial.

The Board Risk and ESG Committee ("the Committee") is a sub-committee of the Board of Directors. The primary objective of the Committee is to assist the Board of Directors in fulfilling its responsibility of oversight and effective governance over:

- The Company's risk management system and monitoring of business risks; and
- The Company's compliance activities
- The Company's Environmental Stewardship
- The Company's Social Responsibility
- The Company's Governance and Ethics

2.0 Authority

- The committee has the authority to oversee and review all aspects of risk management and ESG practices within Safaricom PLC, including policies, frameworks, processes, and performance.
- The committee has the power to request and receive relevant information, reports, and data from management, internal auditors, and external consultants to fulfill its responsibilities effectively.
- While the committee does not have executive management responsibilities, it has the authority to make recommendations and propose actions to the Board of Directors based on its assessment of risk and ESG matters.
- The committee may establish subcommittees or engage external experts and professional advice as necessary to support its work in specialized areas, such as cybersecurity, climate change, or stakeholder engagement.

3.0 Membership

- The Committee shall consist of at least five non-executive Directors who shall report to the Board. The members of the Risk and ESG Committee shall be appointed by the Board of Directors. As per King IV Code of Corporate Governance at least one member of this committee shall be a member of Board Audit Committee or its equivalent.
- Appointments of Independent Directors to the Committee shall be for a period of up to three years, which may be extendable for no more than two further terms of three-year periods each, so long as members continue to be independent.
- The key attributes of committee members shall include the following:
 - i. broad business knowledge relevant to the company's business
 - ii. keen awareness of the interests of the investing public and familiarity with basic risk management principles; and
 - iii. objectivity in carrying out their mandate without any conflict of interest.
- The Chairperson of the Committee shall be a non-executive Director who is not the Chairperson of the Board of Directors. The Chairperson of the board shall not be a member of the committee.

- The Board of Directors shall appoint the Committee Chairperson. In the absence of the Committee Chairperson, the remaining members present shall elect one of themselves to chair the meeting.
- The Company Secretary shall act as the secretary of the Committee.

4.0 Committee Meetings

4.1 Frequency of Meetings:

- The Committee shall meet at least four times in a year, or more frequently at appropriate intervals in the financial year and as it deems necessary to carry out its responsibilities. The meetings shall be held in person, by video conference and/or other remote meeting technologies agreeable to all members.
- Outside of the formal meeting programme, the committee Chairperson, and to a lesser extent, the other committee members, will maintain a dialogue with key individuals involved in the Company's governance, including the Board Chairperson, the Chief Executive Officer, the Chief Finance Officer and the Chief Corporate Security Officer.

4.2 Notification of Meetings and Agenda Items

The Committee Secretary shall be responsible for issuing proper notices of meetings, preparation of agenda and circulation of the relevant papers and will ensure that the committee receives information and papers in a timely manner at least 5 days in advance to enable full and proper consideration to be given to issues.

4.3 Attendance at Meetings and Minutes

- Every member has a duty to attend Committee meetings regularly and to effectively participate in the conduct of the business of the Committee.
- Every member of the Committee should attend at least 75% of the Committee meetings in any financial year. Attendance is disclosed in the Annual Report.
- At a full meeting of the Committee, the members shall review the suitability of a member who has failed to comply with the 75% attendance rule, without a compelling reason.
- The quorum necessary for meetings of the Committee shall be three members of the Committee.
- The Committee shall adopt resolutions by a simple majority of votes of all members of the Committee.
- The Company's Chief Executive Officer (CEO), Chief Finance Officer (CFO), the Chief Corporate Security Officer (CCSO), Executive Director of Foundations and Director Internal Audit shall be permanent invitees to the Committee meetings. Other non-members may be invited to attend all or part of any meeting as and when appropriate and necessary, in consultation with the Chairperson of the Committee.
- The Committee Secretary shall be responsible for keeping minutes, which provide an accurate record of the names of all persons present, deliberations and resolutions of all Committee Meetings, including recording the names of those present and in attendance.
- Draft minutes of the committee meetings shall be agreed with the committee Chairperson and then circulated promptly to all members of the committee unless it would be inappropriate to do so in the opinion of the committee Chairperson.
- The minutes of the Meetings shall be considered at the next meeting, approved, and signed by the Chairperson of the meeting.

5.0 Roles and Responsibilities

In carrying out its oversight responsibilities, the Committee will be relying, in part, on the expertise of Management. To fulfil this oversight responsibility, the Committee should receive reports from Management as appropriate. The roles and responsibilities of the Committee shall be as follows:

5.1 Risk Management and Internal Controls

- 1) Review and assess the Company's risk management programs (Enterprise Risk, Cyber Security, Privacy, Physical Security, AML, Business Assurance, Ethics and Compliance) and the adequacy of the overall control environment including regularly reviewing the nature and extent of the Company's risk appetite as well as monitoring the significant risks that the Company is willing to take in achieving its strategic directives.
- 2) Ensure that the annual report includes appropriate reporting on risk management, including an explanation of how principal risks have been managed or mitigated.
- 3) Evaluate the Company's procedures to safeguard assets, prevent fraud, detect fraud, and bribery incidents.
- 4) Review quarterly reports on the Company's Anti Money Laundering programs, systems, and controls.
- 5) Assess the adequacy of Cybersecurity and Privacy programs and controls, including investments and budget allocations, to address emerging risks, threats, and vulnerabilities appropriately.
- 6) Provide oversight, guidance, and strategic direction on Technology and IT governance to ensure that Technology/ IT risks are properly managed, and IT systems and processes support the organization's objectives while mitigating potential risks.
- 7) Review reports and updates on cyber security threats landscape, breaches, privacy incidents, and responses to ensure appropriate actions are taken to mitigate against cyber and privacy threats.
- 8) Review and monitor the effectiveness of the company's resilience and business continuity arrangements and the testing of these from time to time.
- 9) Review and approve the organization's ethics code of conduct, ensuring it sets clear ethical standards for employees and stakeholders.
- 10) Review the Company's systems, controls and processes for the prevention of bribery, promote accountability, ethical conduct and transparency throughout the organization and receive reports on any non-compliance.
- 11) Review the Company's measures in place for revenue and margins protection.
- 12) Review the Company's process for ensuring compliance with Laws and Regulations and meeting all requirements set by regulators.
- 13) Make recommendations to the Board regarding any matters listed above that the Committee deems appropriate.

5.2 Environmental, Social and Governance

- 1) Review and make recommendations to the Board for the approval of an ESG strategy including related targets that are in line with globally acceptable standards (e.g., as described by the Global Reporting Initiative (GRI)) and against which the Company's performance shall periodically be measured and reported to the Board.
- 2) Advise the Board on the effectiveness of the Company's ESG strategy, clarity of the Company's purpose, the application of its values and its management of sustainable development risks and opportunities.
- 3) Ensure that ESG related policies are in place, advise the Board on the appropriateness of the ESG related policies and programs required to implement the ESG Strategy.
- 4) Regularly receive reports and consider updates from Management on the Company's ESG performance; review current and emerging ESG trends and any relevant international standards and legislative requirements to identify how these are likely to impact the strategy, operations, and reputation of the Company.
- 5) Monitor and assess the activities relating to the United Nations Global Compact's (UNGC) 10 principles covering human rights, labour, environment, responsible supply chain and anti-corruption.
- 6) Review and monitor policies and procedures to assess compliance with applicable health, safety and environmental laws and regulatory requirements.
- 7) Oversee timely ESG Disclosures in accordance with best governance practices, legal and regulatory requirements and approve all internal and external ESG reporting including information to be included in the annual report.
- 8) Approve audits and risk assessments of the Company's ESG activities and review the Company's performance in line with compliance requirements under established ESG principles, with recommendations to Management for upscaling or course correction of strategy as appropriate.
- 9) Ensure the organization has robust process and structures implemented to enhance business prosperity, ensure corporate accountability, and ultimately achieve long-term shareholder value.
- 10) Making recommendations to the Board on ESG matters, including resourcing, ESG investments, and performance management.
- 11) Make recommendations to the Board on any of the matters listed above that the Committee considers appropriate.

5.4 Reporting Responsibilities

- 1) The Committee Chairperson shall report to the Board of Directors with respect to the proceedings of the Committee after each meeting.
- 2) The Committee Chairperson shall facilitate the annual disclosure by the Board of the activities of the Committee including the committee's composition, the number of Committee meetings held and details of attendance at the meetings.

5.5 Other Responsibilities

- 1) Perform other activities related to this Terms of Reference as requested by the Board.

- 2) Review and recommend for Board approval of key policies including those mandated by various regulatory bodies such as CMA and CBK.
- 3) Attend various board trainings to enhance understanding of risk management, environmental, social, and governance (ESG) issues, and relevant regulations, in order to effectively advise the board on these matters.
- 4) Regularly assess the committee's own performance, ensuring that it is fulfilling its oversight responsibilities effectively and making necessary enhancements.

6.0 Conflict of Interest

- 1) The Committee shall agree on a code of conduct to ensure that there is no conflict of interest in the performance of its duties.
- 2) Members of the Committee will not participate in discussions and will not vote on any issue in respect of which there is an actual or perceived conflict of interest.
- 3) Members will be required to declare any interest that could constitute a real, potential, or perceived conflict of interest with respect to their role in the affairs of the Committee.
- 4) The declaration must be made on appointment to the Committee and in relation to specific agenda items at the onset of each Committee meeting and will be updated as necessary.

7.0 Performance of the Committee

- 1) The Committee shall perform a self-assessment at least once a year and agree on actions to improve the effectiveness of the Committee.
- 2) If deemed necessary external training should be arranged for existing and any new members introduced to the Committee. This will be arranged through the Chairperson of the Committee.

8.0 Review of Terms of Reference

- 1) These Terms of Reference sets out a framework of corporate governance structures and principles for the Committee and shall be reviewed by the Board every two years, or at such other time as may be deemed necessary to ensure it remains relevant, objective and practical.
- 2) Any proposed changes to these Terms of Reference shall be submitted to the Board of Directors for approval.
- 3) The Board of Directors may conduct its own external review of the efficacy of the Committee and its Terms of Reference on an annual basis.

Work plan matrix attached as an appendix.

APPENDIX A

STANDING AGENDA FOR THE SAFARICOM BOARD RISK & ESG COMMITTEE

	MEETINGS			
	Feb/ Mar	Apr/ May	Aug/ Sept	Oct/ Nov
Approval of minutes of previous meetings	X	X	X	X
Matters arising from minutes	X	X	X	X
OVERALL BUSINESS ASSURANCE PLAN				
Review of annual combined assurance plan across ERM, AML, Cyber Security, Privacy, Ethics & Compliance, Physical Security and Business Assurance		X		
RISK MANAGEMENT UPDATES				
Review reports from the Chief Corporate Security Officer on issues that potentially impact upon or are related to the responsibilities of the Committee	X	X	X	X
Review the key Principal and Strategic Risks for the business and opportunities		X		X
Review the key Principal and Strategic Risks for Safaricom PLC subsidiaries	X		X	
Review the risk tolerance and appetite for recommendation to the Board		X		
Review any material litigation that could present a material risk to the business	X	X	X	X
Business Continuity Planning Update	X	X	X	X
Risk Transfer (Insurance) Update	X			
ISO Standards and Certifications	X	X		
Security Management Update	X	X	X	X
ETHICS & COMPLIANCE				
Fraud Risk Update	X	X	X	X
Key Investigations Update	X	X	X	X
Internal Fraud Statistics	X	X	X	X
Compliance and Controls Update	X	X		
Ethics Hotline and Fraud Helpdesk Statistics	X	X	X	X
Unclaimed Financial Assets Update	X			

PRIVACY AND DATA GOVERNANCE				
Customer Privacy Program Update	X	X	X	X
AML/ CFT PROGRAM				
AML/CFT Program Update	X	X	X	X
AML CFT Program Update of Key Subsidiaries		X		X
Independent Review of the AML Program		X		
BUSINESS ASSUARANCE				
Business Assurance Update		X		X
Key Business Projects Update	As Required			
CYBER SECURITY AND TECHNOLOGY GOVERNANCE				
Cyber Security Program & Risk Update Including Cyber Incidents	X	X	X	X
Cyber Security Baseline Program	X	X	X	X
Patch and Vulnerability Program Update		X		X
Managed Security Services Program	X		X	
Independent Review of Cyber Security Program		X		
ESG PROGRAM				
ESG Program Update	X	X	X	X
ESG Strategy, Plan and Targets Approval		X		
ESG Initiatives Deep Dive	As Required			
GENERAL				
Board Trainings - AML, Cyber Security, Privacy • Others (Governance etc) – As required	Once annually			
Policies Reviews	As required			
Review the Committee's Charter annually		X		
Evaluate the performance of the Committee and its members annually	As required			
General: Private discussions with management	As required			