Scancom PLC (MTN Ghana)

Risk, Compliance & Information Technology Governance Committee Terms of Reference

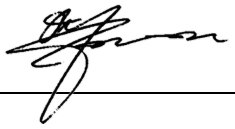
Business Area	Company Secretariat		
Reference	MTN-Ghana-RCITGC-TOR	**Version**	v01 2022
Effective Date	February 2022	**Next Review Date**	January 2023
TOR Owner	RCITGC Chair	**Signature**	
Board Chair on behalf of the Board	Ishmael Yamson	**Signature**	

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

These Terms of Reference are a governance document intended to be used as a reference for Scancom PLC's (MTN Ghana) Risk, Compliance, Information Technology Governance Committee and have been drafted in accordance with the Securities and Exchange Commission's Corporate Governance Code.

The Terms of Reference set out a standard and practical approach for measuring MTN Ghana's compliance with applicable laws, regulations and codes as well MTN Ghana's internal policies and guidelines. The Terms of Reference define the mandate of the RCITG Committee, and also serve as a guide for assisting the Board of MTN Ghana in fulfilling its oversight responsibility to MTN Ghana's risk and compliance management and for the governance of information technology and associated risks.

2. APPROVAL OF TERMS OF REFERENCE

These Terms of Reference are a governance document and shall take effect upon approval by the Board.

3. DEFINITIONS

	Term	Definition
3.1.	**Board**	means the Board of Directors of the Company, acting either through itself, through any committee of its members appointed by it and/or through a duly authorized Company official.
3.2.	**Companies Act**	means the Companies Act, 2019 (Act 992).
3.3.	**CRCO**	means the Chief Risk and Compliance Officer.
3.4.	**Executive**	means an employee of the Company in senior management role as a direct report of the Chief Executive Office (CEO).
3.5.	**INED**	means Independent Non-Executive Director.
3.6.	**IT**	means Information Technology.
3.7.	**NED**	means Non-Executive Director.
3.8.	**RCITG Committee/the Committee**	means the Risk, Compliance, Information Technology Governance Committee of Scancom PLC.

	Term	Definition
3.9.	**Scancom PLC/MTN Ghana/the Company**	means a public listed company registered under the laws of the Republic of Ghana.
3.10.	**SEC Corporate Governance Code**	means the Securities and Exchange Commission's Corporate Governance Code for Listed Companies 2020 (SEC/CD/001/10/2020).
3.11.	**Terms of Reference/ToR**	means the Terms of Reference of the Committee.

4. INTRODUCTION

The RCITG Committee is constituted as a Committee of the Board in accordance with Paragraph 20 of the SEC Corporate Governance Code.

5. PURPOSE

5.1. The purpose of the Committee is to carry out the Board's oversight responsibility for company-wide or enterprise risk management, for compliance with applicable laws and regulations, and for the governance of IT and associated risks.

5.2. The Committee shall:

5.2.1. assist the Board in discharging its duties regarding the governance and oversight of risk management;

5.2.2. assist the Board with oversight of compliance with applicable laws, codes, and regulations, together with the Company's own policies, codes and guidelines;

5.2.3. assist the Board with governance of IT and related risks; and

5.2.4. monitor the effects of risk on performance via a management information system implemented for the Board.

5.3. The Committee shall not perform any executive functions or responsibilities which remain the responsibility of the executive directors, officers and other members of senior management.

5.4. The duties and responsibilities of the Committee as set out in these ToR are in addition to the general duties and responsibilities that the members of the Committee have as members of the Board.

5.5. The deliberations of the Committee do not reduce the individual and collective responsibilities of Board members as required under the Companies Act, the SEC Corporate Governance Code and the constitution of the Company such as their fiduciary duties, and their responsibilities to exercise due care and judgment in accordance with their legal obligations.

5.6. These ToR is subject to the provisions of the Companies Act, the SEC Corporate Governance Code, the Constitution of the Company, general principles of corporate governance and any other applicable laws or regulatory provisions.

6. COMPOSITION OF THE COMMITTEE

6.1. The Committee shall be composed of at least three (3) members, all of whom shall be NEDs, and a majority of which shall be INEDs.

6.2. The Board shall appoint members of the Committee, and the chairman, who shall be an INED and shall not be the chairman of the Board.

6.3. Members of the Committee shall be members of the Board.

6.4. Members of the Committee should have relevant knowledge and experience across the subject areas of risk, compliance, and governance of IT.

6.5. The Company Secretary shall serve as secretary to the Committee and shall be responsible for the formulation and recommendation of improvements to this ToR annually or whenever necessary.

6.6. Members of the Committee shall retire after three (3) years continuous service but will be eligible for immediate re-appointment for two (2) further three (3) year periods. Their membership on the Committee will run concurrently with members' nomination as director of the Scancom PLC board.

6.7. The Board shall have powers at any time to remove any member(s) from the Committee and to fill any vacancies created by such removal.

7. AUTHORITY

7.1. The Committee in carrying out its responsibilities under this ToR:

7.1.1. Is authorized to investigate any activity within the ToR;

7.1.2. Is authorized to consider the appointment, dismissal or re-assignment of the head(s) of the Risk and Compliance (R&C) functions, and IT governance functions accountable to the Committee, and make such recommendations as are required to the Human Resources, Remuneration and Nominating Committee for their consideration and for decision making;

7.1.3. May, at the discretion of the Committee, require other employees of the Company to attend full meetings or parts of meetings;

7.1.4. May consult with and seek information it requires from any employees and all employees shall be required to cooperate with any request made by the Committee in the course of its duties; and

7.1.5. Shall permit a director who has been granted approval by the chairman of the Committee to attend a meeting provided that upon approval of such request, such director shall not be entitled to remuneration / fees for such attendance and shall not be entitled to vote at the meeting.

8. DUTIES & RESPONSIBILITIES

The Committee has an independent role with oversight of the risk, compliance and the governance of IT, and may make necessary recommendations to the Board for its consideration and final approval.

8.1. Risk Management

It is the Committee's responsibility to ensure that the Company has a clearly defined risk management framework and maintains a risk-awareness culture across the Company which are aligned on the delivery of a risk-adjusted strategy, to:

8.1.1. Set out the nature, roles, responsibility and authority of the R&C function within the Company and outline the scope of risk management;

8.1.2. Ensure the formulation of an independent and objective review of risk management within the Company, with risk assessment policies and procedures which shall be documented and communicated to employees;

8.1.3. Review and assess the integrity of the risk control systems and ensure that risk policies and management structures, including the maintenance of related records, are effectively implemented to support corporate strategies and business objectives;

8.1.4. Ensure the definition of the risk appetite of the Company, and thereby assess the extent to which risks shall be accepted, be subjected to

mitigation, or removed;

8.1.5. Review risks facing the Company, the assessment and prioritization of the risks on an aggregate basis in the context of the Company's strategy and business objectives, the corresponding risk tolerance levels and monitoring thereof;

8.1.6. Consider the effectiveness of risk mitigation measures;

8.1.7. Make recommendations to the Board on its risk management strategy, including but not limited to:

8.1.7.1. products and services provided;

8.1.7.2. financial management of the Company;

8.1.7.3. technology infrastructure;

8.1.7.4. market, significant emerging trends and competition;

8.1.7.5. data and information held by the Company;

8.1.7.6. human resources available to the Company;

8.1.7.7. physical premises;

8.1.7.8. potential for internal fraud; and

8.1.7.9. any other material risks;

8.1.8. Make recommendations to the Board to review and adopt contingency plans, which shall be tested, at least annually, for business continuity in the event of risks including:

8.1.8.1. technology failure;

8.1.8.2. major cyber security incidents;

8.1.8.3. loss of access to the Company's offices;

8.1.8.4. loss of records or access to records;

8.1.8.5. the default or failure of a counterparty; and

8.1.8.6. the loss of key personnel;

8.1.9. Review the risk management reports detailing the adequacy and overall effectiveness of the Company's programme for identifying, assessing and controlling risks that pertain to the business of the Company. This includes the review of management reports on the effectiveness of internal controls and to further ensure that recommendations thereof on appropriate action are adopted and implemented;

8.1.10. Ensure that an evaluation is conducted, either by the CRCO or independently (e.g. by the external auditor) regarding risk assessment and the effectiveness of risk management processes at least annually, which will be reviewed by the Committee for necessary action and recommendations to the Board, all of which shall be documented; and

8.1.11. Review the adequacy of insurance covers on an annual basis.

8.2. COMPLIANCE

The Company's operations fall under various regulatory bodies, statutory authorities and laws, together with industry standards and other adopted codes and practices that altogether constitute a regime of compliance requirements and responsibilities. To assist the Board in its responsibilities relating to the Company's compliance obligations, the Committee shall:

8.2.1. ensure that the Company has an effective compliance programme and regime of internal controls that will enable the operation of an ethical and compliant organization;

8.2.2. review and approve the compliance function mandate, objectives and assurance in conjunction with the internal audit function on related controls, and review the adequacy and effectiveness of the programme for ensuring compliance with the Company's legal and regulatory responsibilities;

8.2.3. direct appropriate resources of the Company to ensure the execution of the compliance programme, including the maintenance of proper records on material compliance matters and actions undertaken by the compliance function;

8.2.4. review at least annually with the Company's legal advisors:

8.2.4.1. any legal matters that could have significant impact on compliance with applicable local or international laws and regulations;

8.2.4.2. communications with regulatory authorities which raise material issues affecting the Company; and

8.2.4.3. initiatives and developments of the Company that may lead to regulatory and/or compliance risks in the future; and

8.2.5. review regulatory reports and examinations together with management's responses and follow-up on the implementation of proposed remedial actions.

8.3. GOVERNANCE OF INFORMATION TECHNOLOGY

The Company deploys IT resources in delivering business objectives.

To assist the Board in its responsibilities relating to the governance of IT, the Committee shall:

8.3.1. set out the nature and scope of IT governance and determine the structure for coordinating the executive functions responsible for the various components;

8.3.2. oversee the governance of IT to ensure that it supports the Company in setting and achieving its strategic objectives;

8.3.3. review and recommend to the Board, IT and data governance policies which will be beneficial to the Company;

8.3.4. monitor the progress of major IT projects in the context of development risks, organizational risks and market risks that may impact achievement of project goals;

8.3.5. review the assessment of risks related to IT, including but not limited to:

8.3.5.1. cyber security, which covers information and network security;

8.3.5.2. data integrity, data security and data privacy protection;

8.3.5.3. third party vendors and implementers of platforms and infrastructure; and

8.3.5.4. emerging and potentially disruptive technologies.

9. REPORTING RESPONSIBILITIES, ACCOUNTABILITY AND PROCEDURES

9.1. The chairman of the Committee shall be responsible for reporting to the Board on its activities and make recommendations to the Board regarding the adoption of any matters arising from the stated responsibilities.

9.2. **Delegation**: The Committee may in its discretion, delegate a portion of its duties and responsibilities to a subcommittee or Executives. Where the Committee delegates duties and responsibilities to a subcommittee or the Executive, it shall retain the ultimate responsibility for such duties and responsibilities and shall be liable.

9.3. **Professional advice**: The Committee in carrying out its tasks under this ToR, may obtain such external or other independent professional advice in accordance with the Company's Policy on Engaging External Professional Experts as it considers necessary to effectively assist with the execution of its duties.

9.4. **Limitations**: Whilst the Committee has the responsibilities and powers set forth in this ToR and as spelt out by relevant authorities such as the SEC Corporate Governance Code, it is management's responsibility to develop or implement the risk and compliance programme of the Company.

9.5. **Annual Report**: The Committee shall report on its activities in the Company's annual report including to describe and assess material foreseeable risk factors, with measures taken to mitigate the risk.

9.6. **Annual general meeting**: The chairman of the Committee shall attend the Annual General Meeting of the Company to answer questions falling within the ambit of the Committee.

10. COMMITTEE MEETINGS AND OPERATION

10.1. Meetings of the Committee will be held as frequently as deemed appropriate, but not less than four (4) times a year to discharge its duties as set out under this ToR. Further meetings may be called by the Board or any member of the Board, members of the Committee, the Chief Executive Officer (CEO) and the CRCO.

10.2. **Agenda**: A minimum of five (5) working days prior notice of meetings and the business to be conducted shall be given to the members of the Committee, the Chairman of the Board, the CEO, the CRCO and other Executives as applicable, in order for them to make agenda proposals as necessary.

10.3. **Receipt of notice**: All attendees shall receive notice of the meeting from the secretary of the Committee, and not less than five (5) working days prior to the

meeting, shall receive a formal agenda together with the working documentation where necessary, to ensure adequate preparation for and effective contribution at meetings. This minimum notice requirement shall not apply in the case of emergency meetings and may be varied by the Committee as appropriate.

10.4. **Quorum**: The quorum required for Committee meetings shall be a simple majority of members present, of whom at least one (1) must be an INED, present throughout the meeting.

10.5. A decision or resolution of the Committee given in writing such as by electronic means, but not in a meeting of the Committee, shall require the signatures of all members of the Committee to be as effective as a decision passed at a meeting of the Committee.

10.6. **Attendance**: The CEO, CRCO, and any other members of the Executive deemed necessary by the Committee for its business, including but not limited to:

10.6.1. the General Manager, Internal Audit & Forensics ("GM IAF"),

10.6.2. the Chief Corporate Services Officer ("CCSO"),

10.6.3. the Chief Information Officer ("CIO"),
10.6.4. the Chief Capital Projects Officer ("CCPO"),

10.6.5. the Chief Technical Officer ("CTO"),

shall be in attendance at meetings (other than in-camera sessions with the CRCO) and shall have unrestricted access to the chairman or any other member of the Committee as may be required in relation to any matter falling within the ambit of the Committee.

10.7. **Voting rights**: Where circumstances necessitate the conduct of a vote, apart from members of the Committee, no attendee shall be entitled to vote at meetings of the Committee.

10.8. **Minutes**: Minutes of meetings shall be taken by the Committee secretary and shall be reviewed and approved by members of the Committee and a summarized report thereof shall be tabled for noting at the first available Board meeting thereafter.

10.9. **Recusal**: The chairman of the Committee shall have the right to recuse an Executive director, or a Committee member from the meeting or exclude an agenda item, if in the chairman's opinion, maintaining the Executive director, Committee member or agenda item for the meeting may result in a conflict of interest.

10.10. The Committee and the chairman may hold periodic meetings with the CRCO and other members of senior management where necessary, at least once a year.

10.11. Unless varied by this ToR, meetings and proceedings of the Committee shall be governed, by the relevant provisions of the Company's Constitution.

10.12. Each regularly scheduled meeting shall conclude with an internal session of the Committee, without the involvement of management.

11. TRAINING, EVALUATION AND REVIEW

11.1. **Training**: Committee members are required to undertake continuous development training on related matters in order to keep their skills and knowledge abreast with industry, legislative and regulatory changes and to make meaningful contribution in directing the affairs of the Company.

11.2. **Annual performance evaluation**: The Committee shall perform a review and evaluation at least annually, of the performance of the Committee and its members, including an evaluation of the compliance of the Committee with this ToR, and shall submit the outcome of the evaluation to the Board.

11.3. In addition, the Committee shall review and re-assess, at least annually, the adequacy of these ToR and recommend any improvements that the Committee considers necessary to the Board.

12. REMUNERATION

The remuneration/ fees of the chairman and Committee members will be recommended by the Human Resources Remuneration and Nominating Committee to the Board for approval by the shareholders.

13. DISPUTES

Any material issue on which consensus cannot be reached by the Committee shall be determined by a simple majority of members present and voting and recommended to the Board for approval, setting out dissenting views for the consideration of the Board.

14. DISSOLUTION

The Committee shall be dissolved on the passing of an ordinary resolution by the Board.

APPENDICES

APPENDIX I: Standing items for Committee meetings

Action	Q1	Q2	Q3	Q4
Risk Management				
Review the adequacy and overall effectiveness of the Company's programme and related management structures for identifying, assessing, and controlling risks, as well as the promulgation of an organization-wide risk-aware culture	✓		✓	
Review and consider the stated risk appetite and related tolerance levels in the context of the strategic business objectives, for recommendation and approval by the Board	✓		✓	
Review the risk profile of the Company in context of the risk appetite and risk capacity, and consider: • Assessment & prioritization of risks • Risk tolerance • Indicators & triggers • Adequacy of risk responses	✓	✓	✓	✓
Review the effectiveness of activities undertaken in risk mitigation under the Company's risk escalation policy	✓	✓	✓	✓
Review emerging risks and trends that may lead to new risks and opportunities not yet identified	✓	✓	✓	✓
Review, approve and/or ratify risks recommended for acceptance by management in accordance with the Company's risk acceptance policy	✓	✓	✓	✓
Review the adequacy of insurance policies for insurable risks and the adequacy of corresponding insurance cover		✓		
Compliance				
Assess the adequacy and effectiveness of the compliance programme, related management structures and corresponding regime of internal controls	✓			
Assess compliance with regulatory bodies, statutory authorities, local and	✓	✓	✓	✓

international applicable laws including, but not limited to: • Companies law • Securities law/codes • Telecommunications industry laws • Environmental, safety and health law • Employment and labour law • Tax laws • Financial and credit laws • Data Protection laws • Other applicable laws, codes, regulations				
Receive reports on alleged or potential breaches of compliance and any disciplinary action taken	✓	✓	✓	✓
Assess significant legal matters: • pending in the courts or in arbitration that could have impact on compliance with applicable laws and regulations	✓	✓	✓	✓
Action	**Q1**	**Q2**	**Q3**	**Q4**
IT Governance				
Assess alignment of IT with overall strategy and business objectives	✓			
Review major IT projects/investments to assess progress in line with set targets and metrics	✓	✓	✓	✓
Assess effectiveness of control and mitigation strategies in lieu of cyber risk; review reports of major cyber security incidents and emerging related risks	✓	✓	✓	✓
Assess data governance for effectiveness in preserving data integrity, privacy and security	✓		✓	
General				
Review the Committee's ToR				✓
Conduct a formal assessment of the efficiency and effectiveness of the Committee and take action to remedy any significant deficiencies				✓
Prepare a statement for inclusion in the annual report to describe and assess material foreseeable risk factors, with measures taken to mitigate the risk	✓			

APPENDIX II:

List of Regulators

- National Communications Authority
- National Information Technology Agency
- Securities and Exchange Commission
- Ghana Stock Exchange
- Data Protection Commission
- Environmental Protection Agency

List of some relevant laws, statutes, codes and regulations

- Companies Act, 2019 (Act 992)
- SEC Corporate Governance Code for Listed Companies 2020 'SEC/CD/001/10/2020'
- Electronic Communications Act, 2008 (Act 775); ECA Amendment Act, 2009 (Act 786)
- Electronic Transactions Act, 2008 (Act 772)
- Communications Service Tax Act, 2008 (Act 754); CST Amendment Act 2019 (Act 998)
- Data Protection Act, 2012 (Act 843)
- Payment Systems and Services Act, 2019 (Act 987)
- Cybersecurity Act, 2020 (Act 1038)
- Anti-Money Laundering Act, 2020 (Act 1044)
- Guidelines for the Deployment of Communications Towers
- Listing Rules of the Ghana Stock Exchange

Specific areas of coordination with other committees and functions

- **Whistle-blowing**: the Committee, in collaboration with the AC , will receive specific notice of any events reported under the Company's whistle-blowing policy and determine any subsequent course of action under its ToR;

- **Internal fraud**: the Committee, in collaboration with the AC , shall receive notice of any reported incidences of internal fraud or risks thereof and will determine subsequent course of action under its ToR;

- **Financial risk**: the Committee, in collaboration with the AC , shall receive notice of any assessment of financial risk and carry out any due course of action under its ToR;

- **Personnel or talent risk**: the Committee, in collaboration with the Human Resources, Remuneration and Nominations Committee, shall receive notice of any assessment of significant risk with regards to talent and determine the necessary course of action where applicable.

APPENDIX III: Reference Documents

Document Name / Description	Publication Date	Published By
Job description, responsibilities of CRCO		
Code of Ethics	January 2014	Corporate Services
Conduct Passport	May 2019	Risk and Compliance
Enterprise Risk Management Policy	September 2021	
Compliance Policy	February 2021	
Business Continuity and Resilience Policy	February 2021	
Conflict of Interest Policy	June 2020	
Data Privacy and Protection Policy	February 2021	
Whistle Blowing Policy	October 2021	Internal Audit and Forensic Services
Acceptable Usage Policy	September 2021	Information Technology
Information Security Policy	October 2021	
Information Technology Service Mgt Policy	September 2021	
Cloud Usage Policy	August 2021	
Backup and restoration Policy	August 2021	
Use Your Own Device Policy	August 2021	

APPENDIX IV: Annual Evaluation of Risk, Compliance and IT Governance Functions

The Committee evaluates the performance of the CRCO (and by extension the R&C function), as well as Executive(s) designated with responsibility for IT governance, based on its expectations, in parallel with the assessments of management and external auditors.

The CRCO and the Executive (s) responsible for IT Governance functions will be advised on the outcome of their respective evaluations with the opportunity to discuss the findings, including trends developed from prior periods.

The rating scale to be applied for the evaluation ranges from 1 to 5 as follows:
1 – inadequate
5 – best practice,
or where appropriate, marked as "n/a" connoting "not applicable".

A. Evaluation of Risk & Compliance Function

For completion by Committee members:

	Rating
Understanding	
How well does the CRCO demonstrate that he/she recognises their direct reporting responsibility to the Board and its risk committee?	
How strongly does the CRCO demonstrate an understanding of the Terms of Reference, and by extension, the responsibilities and operation of the Committee?	
How well does the CRCO demonstrate that he/she understands the expectations of the Committee and the chairman?	
How well does the CRCO demonstrate that he/she understands the Company's business and risk environment?	
Does the CRCO consistently demonstrate a realistic commercial view of the business?	
Comments:	
Charter and structure	
Do the Terms of Reference for the risk and compliance function (and thereby of the CRCO) define:	
Roles and responsibilities, including those in relation to other internal functions?	
Expectations of management?	
Scope of risk and compliance (R&C) work?	
Access to information?	

Has the Terms of Reference for the R&C function been reviewed in the past two years?	
Are R&C Terms of Reference visible to everyone in the Company?	
Does the structure of R&C facilitate consistency in the quality of service to the Company?	
Does the structure of R&C facilitate an understanding of the Company's business issues?	
Does the structure of R&C facilitate the delivery of value to the Company?	
Comments:	
Skills and experience	
How well does R&C's staff reflect its role and responsibilities?	
On the basis of the work performed by R&C over the past 12 months, does the team have the right mix of competencies?	
How would you assess the Committee's confidence in the CRCO and the R&C team?	
Comments:	
Communication	
Has the CRCO (or properly designated representative(s) of the R&C team) attended all the Committee meetings it was scheduled to attend?	
Has the CRCO made himself/herself available for consultation outside of Committee meetings?	
How responsive has the CRCO been to requests from the Committee?	
What is the level of the CRCO's frankness and candour with the Committee?	
How well has the CRCO handled difficult or contentious issues?	
Does the CRCO ensure that the chairman of the Committee is fully briefed on significant findings or developments prior to Committee meetings?	
Is the CRCO adequately prepared for Committee meetings?	
Does the CRCO prepare relevant and clear reports and papers tabled with the Committee?	
Have reports been received from the CRCO on a sufficiently timely basis?	
Does the CRCO promptly advise the Committee about significant issues and significant developments?	
Comments:	

Performance	
Are the risk management framework and the compliance programme comprehensive, understandable, and timely?	
Does the risk management plan cover all priority and high-risk areas?	
Did the original risk management plan or compliance programme leave unanswered any significant issues of concern to the Committee?	
In what way have the R&C functions delivered value to the organization?	
How would you assess the CRCO and the R&C team's overall performance?	
Comments:	

For completion by indicative heads of major business units and by the CFO:

	Rating
Planning	
Is the risk and compliance (R&C's) Terms of Reference sufficiently visible to everyone in your business?	
Did R&C discuss its approach and major areas of risk management focus with you?	
Did you raise any major areas of concern that were not reviewed by the R&C team?	
Comments:	
Skills and experience	
From the dealings with members of R&C team, do you consider that they have sufficient professional experience, project management, interpersonal skills and seniority to effectively carry out the work required?	
From the dealings with members of the R&C team, do you consider that they have sufficient expertise in the functional specialisation areas (e.g. risk assessment, IT, etc.) to effectively carry out the work required?	

From your dealings with senior members of R&C, what is your assessment of the strength of understanding of the organisation and its risk environment?	
From your dealings with senior members of R&C, how strongly did they demonstrate an appreciation of the issues key to your role and responsibilities?	
Did members of the R&C team consistently demonstrate independence in all of their obligations?	
In you view, does the way in which R&C is funded impair its independence?	
Were members of the R&C team adequately supervised?	
Comments:	
Work programme	
Was effective co-operation achieved between the R&C team and your business/department, including the avoidance of undue disruption of normal activities?	
How responsive was R&C to the business's needs of the Company?	
Were R&C reports relevant, clear and constructive?	
Were R&C functions reports and assessments discussed with you prior to being tabled with the committee?	
Did you have any major unresolved disagreements with R&C?	
Comments:	

For completion by the external auditor:

	Rating
Terms of Reference	
How would you evaluate Risk and Compliance's (R&C) overall performance given your understanding of the Company's business needs, complexity and risk environment?	
How would you evaluate R&C's current Terms of Reference given your understanding of developments in R&C?	
From your understanding of R&C and industry best practice, do you consider R&C's current Terms of Reference to reflect a "high water mark"?	
Comments:	

Skills and experience	
From your dealings with R&C, do you consider that they have the professional experience, technical skills, interpersonal skills and seniority to carry out the R&C work effectively?	
From your dealings with senior members of R&C, how would you evaluate their understanding of the organisation, its business and its risk environment?	
From your dealings with R&C, assess their experience in the following key functional specialisations in the context of what is required for the proper discharge of their responsibilities:	
IT	
Risk management	
Regulatory environment	
Other	
From your dealings with R&C and your knowledge of R&C and the industry, do you consider R&C has sufficient resources to satisfy their Terms of Reference?	
From your dealings with R&C and your knowledge of R&C and industry best practice, how would you evaluate the sufficiency of R&C's resources to render the services outlined in its risk management plan adequately in the time frames identified?	
Does the structure of R&C appear to facilitate understanding of the Company's business issues?	
Does R&C's staffing appear to adequately reflect its roles and responsibilities?	
In your assessment, is the R&C methodology robust and does it reflect the latest thinking in enterprise risk management and in effective compliance programmes?	
Comments:	
Work programme	
To the best of your knowledge, are there any major areas of risk or concern that R&C did not appear to cover?	
Did you receive copies of all reports and analysis issued by R&C?	
Were copies of R&C reports and analysis received in a timely manner?	
Are R&C reports and analytical outputs of a standard comparable to best practice in comparable organisations?	

Comments:	

B. Evaluation of IT Governance Executive Function(s)

In the absence of a sole Executive designated responsible for the management components that fall within the scope of IT governance, this evaluation shall refer generally to the IT Governance Executives ("ITGEs"), which covers the various Executives with related functional responsibility including the CIO, CCPO, CTO and other senior management members where applicable.

For completion by Committee members:

	Rating
Understanding	
How well do the ITGEs demonstrate that they recognize the scope of their reporting responsibility to the Board and this Committee?	
How strongly do the ITGEs demonstrate an understanding of the nature and scope responsibility, and by extension, the responsibilities and operation of the Committee?	
How well do the ITGEs demonstrate that they understand the expectations of the Committee and the chairman?	
How well do the ITGEs demonstrate that they understand the Company's IT governance scope, including but not limited to the governance of cybersecurity risk, data privacy and data integrity, major IT projects?	
Do the ITGEs consistently demonstrate a realistic commercial view of the business?	
Comments:	
Structure	
Does scope of responsibility across IT governance functions define:	
Roles and responsibilities?	
Expectations of management?	
Scope of IT governance work across various components including cybersecurity, data privacy and integrity, major IT projects?	
Access to information?	
Have the relevant scope of responsibility references been reviewed in the past two years?	
Are the relevant scope of responsibility references visible to everyone in the Company?	

Does the structure of the IT governance functions facilitate consistency in the quality of service to the Company?	
Does the structure of IT governance functions facilitate an understanding of the Company's business context?	
Does the structure of IT governance functions facilitate the delivery of value to the Company?	
Comments:	
Skills and experience	
How well do ITGEs and staff reflect their roles and responsibilities?	
On the basis of the work performed by ITGEs over the past 12 months with particular reference to significant projects and significant risks identified, does the team have the right mix of competencies?	
How would you assess the Committee's confidence in the ITGEs and corresponding teams?	
Comments:	
Communication	
Have the ITGEs (or properly designated representatives) attended all the Committee meetings they were scheduled to attend?	
Have the ITGEs made themselves available for consultation outside of Committee meetings?	
How responsive have the ITGEs been to requests from the Committee?	
What is the level of ITGEs' frankness and candour with the Committee?	
How well have ITGEs handled difficult or contentious issues?	
Do ITGEs ensure that the chairman of the Committee is fully briefed on significant findings or developments prior to Committee meetings?	
Are ITGEs adequately prepared for Committee meetings?	
Do ITGEs prepare relevant and clear reports and papers tabled with the Committee?	
Have reports been received from ITGEs on a sufficiently timely basis?	
Do the ITGEs promptly advise the Committee about significant issues and significant developments?	
Comments:	

Performance	
Is the management focus led by ITGEs comprehensive, understandable and relevant?	
Do the IT governance functions cover all priority and high-risk areas and contribute to the business risk management framework a constant assessment of and adequate response with regards to emerging risks?	
In what ways have the IT governance functions delivered value to the Company?	
How would you assess the ITGEs and corresponding teams overall performance?	
Comments:	

APPENDIX V: Annual Performance Evaluation Matrix (Committee)

This evaluation form is to be completed annually with ratings against each statement in the sections below, on a scale of 0 to 5 as follows:

0 – insufficient knowledge or not applicable
1 – strongly disagree
2 – disagree
3 – neutral / neither agree nor disagree
4 – agree
5 – strongly agree

Evaluators may provide additional relevant information in the "Comments" section where applicable.

		Rating	Comments
Composition and Quality			
Members of the Committee meet the requirements of independence.			
Committee members have the necessary experience and qualifications to carry out and deliver on the Terms of Reference.			
The Committee demonstrates a high level of integrity, credibility, engagement & participation, ability to handle conflict constructively, and adequate and timeous addressing of matters before it.			
The Committee undertakes continuous education and relevant training to enhance its knowledge and understanding of risk, compliance and IT governance, and in the context of the market and industry.			
Understanding of the business context in relation to risk, compliance & IT governance			
The Committee emphasizes and supports the adoption of an organization-wide risk-aware culture			
The Committee demonstrates its understanding and applies its oversight responsibility accordingly on the various categories of risk that may impact business, including but not limited to: • Financial • Regulatory • Fraud • Reputation • Business continuity • Emerging market and competitive trends			

The Committee in its review and assessment of risk management of the Company, engages management on the determination of the Company's risk appetite, risk capacity, profile and tolerance levels pertaining to specific risks, as well as challenges potential bias, altogether in the context of the strategic objectives of the business.			
The Committee engages management on the process by which risks are identified, assessed and prioritized, and on the adequacy of risk responses as well as the effectiveness of mitigation actions upon escalated risks.			
The Committee demonstrates its knowledge of the compliance obligations of the Company and applies its oversight responsibility accordingly with regards to: • Governance • Legal • Industry/telecommunications • Data protection & privacy • Environment, health & safety • Employment and labour • Stock Exchange (GSE listing rules) • Other applicable areas of law and regulation			
The Committee demonstrates its knowledge of IT governance and applies its oversight responsibility in lieu of: • Progress and value assessments of major IT projects and investments, in line with the strategic objectives of the Company • Data governance including the maintenance of integrity, privacy and security of corporate data assets • Security of information, systems, programme, devices, networks, etc. (cyber security)			
Committee Operations			
The Committee maintains adequate minutes of its meetings and submits its report of proceedings, including findings and recommendations to the Board, in the agreed timeframe, following each meeting.			
The Committee convenes meetings and engagements with sufficient frequency, i.e. beyond the minimum quarterly schedule where			

necessary in order to address emerging and significant issues requiring attention.			
Committee meetings are conducted with efficiency and commensurate time and attention are allocated to address significant issues			
The notice for Committee meetings together with minutes of prior meetings, related reports, etc., are circulated well in advance to provide adequate time to enable members and participants study the information and contribute agenda proposals as necessary			
The chairman and members of the Committee maintain appropriate engagement and communication with the CRCO, the CEO and other members of senior management who participate in Committee proceedings			
The Committee sets clear expectations on the responsibility, scope and mandate of the CRCO, and provides feedback and recommendations to the HR Committee and to the Board with regards to performance			
The Committee holds regular private or in-camera sessions with the CRCO, head of internal audit and other senior management participants as necessary			
The Committee maintains the limits of oversight in lieu of management of risks within the Company			
Committee members attend meetings adequately prepared			
Monitoring & Resourcing			
The Committee conducts a performance evaluation annually with the corresponding output and any related findings and recommendations both addressed / un-addressed, submitted to the Board.			
The Company adequately resources the Committee to enable it to fulfill its mandate under the Terms of Reference, including where required, the funding of access to external professional expertise.			