

Risk and Information Technology Committee Mandate

1. Introduction

- 1.1. The Risk and Information Technology Committee (Committee) is constituted as a committee of the board of directors (Board) in respect of the duties assigned to it by the Board.
- 1.2. The Committee thus derives its authority from the Board.
- 1.3. The duties and responsibilities of the members of the Committee as set out in this mandate are in addition to those duties and responsibilities that they have as members of the Board. The deliberations of the Committee do not reduce the individual and collective responsibilities of the directors regarding their fiduciary duties and responsibilities, and they must continue to exercise due care and judgment in accordance with their legal obligations.
- 1.4. This mandate is subject to the provisions of the Companies Act, the Company's Memorandum of Incorporation and any other applicable law or regulatory provision.
- 1.5. In carrying out its responsibilities in the achievement of its objectives, the Committee must do so in a manner that upholds and promotes the Group's values of Passion, Value and Partnership, which are its guiding principles.

2. Composition and tenure

- 2.1. The Committee shall have a minimum of three members, which should comprise of executive and non-executive directors, at least one of which is also an Audit and Compliance committee member, and the majority of which must be non-executive directors.
- 2.2. The Committee members shall be appointed by the Board.
- 2.3. The Committee must as a whole have the necessary knowledge, skills, experience and capacity to fulfil its duties. In order to discharge their responsibilities, committee members are required to keep up-to-date with economic, legislative, risk, IT and other developments which impact the Committee's areas of oversight.
- 2.4. To the extent that a Committee member has the requisite IT skills and experience, the Board, with the recommendation of the Committee, shall be entitled to designate such member as an "IT Specialist" for purposes of the Committee and to delegate additional IT governance oversight responsibilities to such Committee member, if necessary and relevant.
- 2.5. The Board shall annually appoint a non-executive director to chair the Committee.
- 2.6. The Committee has an indefinite tenure, unless otherwise determined by the Board or applicable law or regulatory provision and subject to the evaluation of the Committee.

3. Authority

- 3.1. The Committee acts in terms of the delegated authority of the Board as recorded in this mandate and is accountable for its performance in this regard and has the power to investigate any activity within the scope of its mandate. The Board remains ultimately accountable for responsibilities delegated to the Committee and retains the power to make decisions in this regard.
- 3.2. The Committee may consult with specialists or consultants, at the Company's cost, to assist it with the performance of functions, but must consult with either the Board chair or lead independent director prior to doing so. Such specialists or consultants may be invited to present at Committee meetings on matters in respect of which they have been consulted. The Committee, in the fulfilment of its duties, may call upon the chairs of the Board and Board committees, any of the executive directors, the company secretary or other executives of the Company to provide it with information.
- 3.3. The Committee has reasonable access via the CEO to the Group's records, facilities and any other resources necessary to discharge its duties and responsibilities.
- 3.4. The Committee may form sub-committees and delegate authority to one or more designated members of the Committee or to one or more executives of the Company.

4. Role and responsibilities

- 4.1. The Committee has an independent role with accountability to the Board and shareholders. The Committee is not an executive committee and as such it shall not perform any management functions or assume the functions of management.
- 4.2. The Committee shall consider from time to time the need to obtain independent assurance on the effectiveness of the Group's management of risk and IT and shall review and consider such assurance evaluations.

5. Risk

- 5.1. The Committee has the delegated responsibility to govern risk in a way that enables the Group to sustain and optimise its strategy and objectives. Policies, frameworks and standards to give effect to this should be considered and approved by the Committee.
- 5.2. The Committee is also responsible for overseeing that the implementation and execution of risk control, which is delegated to management, is effective and results in the required appropriate outcomes.
- 5.3. In overseeing the management of risk, the Committee shall review and consider the Group's -
 - 5.3.1. enterprise risk management policy and framework;
 - 5.3.2. risk appetite and tolerance levels;
 - 5.3.3. risk rating matrices;
 - 5.3.4. assessment of risks;
 - 5.3.5. risk register and key risks;
 - 5.3.6. appropriateness of the risk mitigation controls;
 - 5.3.7. business resilience and crises response management framework and key assumptions that allow for Group's resilience, including ability to operate under conditions of volatility and to withstand and recover from acute shocks;
 - 5.3.8. combined assurance plan; and
 - 5.3.9. risk deep dives (as and when requested by the committee / main board).
- 5.4. In addition, the Committee is responsible for -
 - 5.4.1. monitoring that risks and opportunities arising from the economic, social and environmental context are managed within the approved levels of tolerance and appetite;
 - 5.4.2. identifying key risk indicators and monitoring progress thereto;
 - 5.4.3. considering the deliberations of management and governance committees to ensure appropriate consideration of key risk exposures;
 - 5.4.4. reviewing major project risks and ensuring that adequate response plans are in place and effective;
 - 5.4.5. monitoring significant risk events, performance surprises and incidents to understand root causes and required actions;
 - 5.4.6. evaluating and determining the nature and extent of changing conditions and emerging risks that could have in pursuit of its strategic objectives;
 - 5.4.7. ensuring the adequacy and appropriateness of the Group's insurance cover;
 - 5.4.8. considering high impact/low likelihood risks (black swan events);
 - 5.4.9. integration and embedding of risk management into day-to-day operations and decision-making processes as part of the organisational culture;
 - 5.4.10. reviewing the effectiveness of the overall enterprise risk management process by reviewing the summary reports prepared by the risk management function, the status and progress of corrective actions and the adherence to the enterprise risk management framework.

6. Information and Technology

- 6.1. The Committee has delegated responsibility for the strategic direction and accountability for the effective compliant and ethical management and control (including acquisition, creation, use, dissemination and disposal) of data and information ('data' and 'information'), and the acquisition, development, use and distribution of technology ('technology') within the group Policies, standards and frameworks to give effect to this should be considered and approved by the Committee.
- 6.2. The Committee is responsible for overseeing that the implementation and execution of IT control, which is delegated to management, is effective and results in the required appropriate outcomes.
- 6.3. In overseeing the management of data, information and technology (IT), the Committee shall consider, *inter alia*, the following –
 - 6.3.1. the role and impact of data, information and technology on the achievement of the Group's strategic and operational objectives;
 - 6.3.2. the approval of significant IT investments in technology assets, resources, products and services in accordance with the Group delegated limits of authority and whether the investments are delivering the required returns and create sustainable value for the group within its economic, social and environmental context;
 - 6.3.3. the appropriateness of the internal IT governance structures and decision making bodies;
 - 6.3.4. management's assessment of benefits realisation of material IT projects integration and mitigation of risk associated with the management and control of data and information and

- acquisition and utilisation when using outsourced services, suppliers and third parties, including across jurisdictions;
- 6.3.5. assessing, evaluating and responding to the risks and opportunities associated with emerging, innovative and disruptive technologies; arrangements for business resilience and disaster recovery planning and testing;
 - 6.3.6. compliance with laws and regulations;;
 - 6.3.7. ethical and responsible management and control of data resources and information assets and disposal of obsolete technology having regard to the environmental impact as well as data and information security;
 - 6.3.8. data and information security including identification and classification of the group's resources and information assets;
 - 6.3.9. protection of privacy of personal data and information;
 - 6.3.10. adherence to quality requirements for data and information;
 - 6.3.11. the monitoring and management of IT incidents, including cyber-attacks;
 - 6.3.12. the Group's cyber security and cloud strategies and practices;
 - 6.3.13. the appointment and management of external service providers, technology developments and IT global best practice;
 - 6.3.14. IT internal audit report in relation to IT audits;
 - 6.3.15. external audit findings relating to IT, including periodic assurance on the effectiveness, compliance and ethics of the group's management and control (including acquisition, creation, use, dissemination and disposal) of data and information; and regarding artificial intelligence, adherence to the values of ethics, human centricity, accountability, transparency, explainability, security, privacy, fairness and trustworthiness and clear accountability for decisions, actions, outputs and outcomes which includes subjecting all artificial intelligence to human oversight and mechanisms that commensurate with the level of risk to the group.

7. Meetings and procedures

7.1. Agenda and Minutes

- 7.1.1. The Committee must establish an annual diary to ensure that all relevant matters are covered by the agendas of the meetings planned for the year.
- 7.1.2. The company secretary shall be responsible for, together with the chair of the Committee, determining the agenda and circulating the meeting agenda, minutes, and supporting material to all Committee members and invitees at least one week prior to each scheduled meeting.
- 7.1.3. Committee members must be fully prepared for Committee meetings to provide appropriate and constructive input on matters discussed.
- 7.1.4. The minutes of the Committee should be completed by the company secretary as soon as reasonably possible after the meeting and circulated firstly to the Committee chair for input and thereafter to members of the Committee for review.
- 7.1.5. The minutes must be formally approved by the Committee at its next scheduled meeting and signed by the chair of the Committee. These should be distributed to all Board members for information purposes.

7.2. Frequency

- 7.2.1. The Committee must hold sufficient scheduled meetings to discharge all its duties as set out herein but subject to a minimum of two meetings per year.
- 7.2.2. Meetings in addition to those scheduled may, with approval of the Committee chair, be held at the request of executive management or at the instance of the Board.

7.3. Attendance

- 7.3.1. Committee members shall attend all scheduled meetings of the Committee, including meetings called on an ad hoc-basis for special matters.
- 7.3.2. Executive management (to the extent that they are not committee members), senior management, other assurance providers or professional advisors of the Company may attend Committee meetings by invitation, at the reasonable discretion of the Committee chair, but may not vote. The permanent invitees may change from time to time as determined by the Committee.

- 7.3.3. Any director of the Company is entitled to attend Committee meetings as an observer. However such directors are not entitled to participate without the consent of the chair, and do not have a vote.
- 7.3.4. The company secretary is the Committee secretary.
- 7.3.5. If the nominated chair of the Committee is absent from a meeting, the members present must elect one of the members present to act as chair for the duration of that meeting.
- 7.4. Quorum**
- 7.4.1. A quorum for meetings is a majority of members present (either in person or by electronic means), provided that if the Committee consists of an even number of members a quorum shall be constituted if fifty percent of such members are present.
- 7.4.2. Persons in attendance at Committee meetings by invitation do not form part of the quorum for Committee meetings.
- 7.4.3. A duly convened meeting of the Committee at which a quorum is present shall be competent to exercise all or any of the authorities, powers and discretions vested in or exercisable by the Committee.
- 7.4.4. Each member shall have one vote at any meeting of the Committee and all decisions taken by simple majority.
- 8. Reporting and disclosure**
- 8.1. After each meeting the chair shall report to the Board on its proceedings, activities, issues and related recommendations and all significant matters within its duties and responsibilities as set out in this mandate.
- 8.2. The Committee shall make whatever recommendations to the Board it deems appropriate on any area within its remit, where action or improvement is needed.
- 8.3. The Committee shall consider annually for the reporting period whether it is satisfied that it has fulfilled its responsibilities in accordance with this mandate and shall disclose whether it is so satisfied.
- 8.4. The Committee shall compile a report to stakeholders on its activities to be included in the Company's annual integrated report, which report shall include the necessary disclosure items, including all material risks specific to the Group, the retail industry and/or its securities, the extent of the risks and opportunities the Group is willing to take, without compromising sensitive information;
- 8.5. The Committee shall disclose, at least annually, -
- 8.5.1. whether the committee is satisfied that the risk function, the Group's risk management system and overall internal control framework are effective and that significant weaknesses in internal controls have been effectively addressed;
- 8.5.2. whether the committee is satisfied that the management and control of data and information and the acquisition, development, use and distribution of technology are effective, compliant and ethical;
- 8.5.3. whether the committee is satisfied that the arrangements for and the prevention and detection of information privacy breaches and cyber-attacks are effective, and that significant incidents have been appropriately responded to, to manage consequences and prevent future occurrences;
- 8.5.4. whether the committee is satisfied that the ethical, legal and operational risks associated with the use of emerging, innovative and disruptive technologies are effectively managed and addressed;
- 8.5.5. with regards to AI, whether the committee is satisfied that the accountability for decisions, actions, outputs and outcomes is clearly established;
- 8.5.6. the committee's overall role and associated responsibilities and functions;
- 8.5.7. committee's composition, including qualifications and experience of committee members;
- 8.5.8. any external advisors or invitees who regularly attend the committee meetings
- 8.5.9. number of committee meetings held during the reporting period and attendance at those meetings; and
- 8.5.10. key areas of focus during the reporting period and planned areas for future focus.
- 8.6. The above disclosure must be properly considered and generic disclosure must be avoided. This disclosure must ensure that material risks are coherently grouped together, and material risks with the most immediate significance are prominent at the beginning of such disclosure.

9. Evaluation and review

- 9.1. At least annually the Committee will consider, reflect and discuss its performance and that of its chair and its members as a whole. This will be done having regard to the progress against the Steps documents referred to below.
- 9.2. Every two years (or as deemed necessary by Board, together with the Remuneration and Nominations committee (Remnomco)) a formal evaluation process will be conducted. This process will be led by the company secretary or an independent service provider on behalf of Remnomco which methodology will be determined and whether the evaluation will be externally facilitated or not and may take the form of a questionnaire, interviews, feedback from relevant stakeholders or any other form as may be determined by the Board in conjunction with Remnomco.
- 9.3. The results of the evaluation process will be formulated by the company secretary into a Steps document which sets out the feedback received, the proposed areas requiring improvement, and the steps required to effect the improvements. The Steps document will be discussed with the chair who will provide feedback and input, and will then be considered and discussed by the Committee and the Board.
- 9.4. If so decided by the Board and Remnomco, an evaluation process which is either externally facilitated or different to the normal methodology may be followed.
- 9.5. This mandate and the Committee diary will be reviewed annually by the Committee and the Board.

Approved 30 March 2026



.....
NG Payne
Risk and Information Technology Committee Chairman
Mr Price Group