Risk and IT Committee Report

The main impact of this committee's deliberations on the group's value creation elements is reflected below:

Capitals

F M I H ○ ○

Stakeholders

Business Activities

King IV™ Governance Outcomes

- Good performance
- Effective control

Strategic Pillars

Sustainable Development Goals

9 11 12

Role

The committee is constituted as a committee of the board and has been delegated responsibility for governing and overseeing the risk and information technology (IT) activities of the group. The committee mandate is published on the group's website www.mrpricegroup.com. The committee members, their qualifications and experience, the number of meetings held and attendance at meetings is detailed in the board report on pages 70, 71 and 79.

The committee is responsible for assisting the board in its oversight of risk, reviewing the group's risk appetite and risk profile in relation to strategy, reviewing the effectiveness of the group's risk management framework and the methodology used in determining the group's risk profile and respective responses. The committee's responsibility is to ensure that risks and opportunities are considered and managed in a manner that influences and fulfils the setting and achievement of the group's strategy (detailed in the strategy, material matters and key risks section on pages 38 - 51).

To fulfil its role, the committee oversees management's implementation and execution of effective risk management which includes mitigation responses to key risks, reducing risks to within risk tolerance, insurance cover, business resilience, IT risk management and related assurance mechanisms. In addition, the committee plays an oversight and advisory role over the group's IT strategy.

Key areas of focus for the reporting period were:

- Guiding and monitoring management's response to the COVID-19 pandemic
- Promoting and monitoring a paradigm shift to a more integrated, proactive and continuous enterprise risk management (ERM) approach
- Improved integration of risk into the revised group strategy
- Oversee progress towards the successful delivery of the group's IT transformational projects
- Monitor and review ongoing improvements to the IT security posture in accordance with the targeted end state

Committee Statement

The committee is satisfied that it has fulfilled its responsibilities in accordance with its mandate for the 2021 financial year.

Enterprise Risk Management

Risk management is intertwined into the annual strategy build process across all trading divisions and centres of excellence. The philosophy of the group is to promote risk-taking in a responsible and informed manner. Thus, the synchronisation between strategy and risk and its effect on overall performance is critical to ensure value creation. Post the outsourcing of the internal audit function, the group retained its chief audit executive and pivoted the role into director of integrated assurance reporting to the CFO. The continuity of skills and prior business knowledge has added tremendous credibility to this role, elevating its importance and ensuring traction.

Risks are carefully considered in achieving a given strategy and business objective. Executive management routinely challenge divisional management on their capabilities to achieve their strategy and business objectives and, in doing so, receive formal quarterly updates on progress. The analysis of divisional risk registers ensures completeness, progress and alignment to group strategic risks. This focus on risks, embedded in strategy and business objectives, remains critically important. In addition, the group and risk management functions perform risk assessment pulse checks to identify internal and external events that may impact the group in achieving its objectives. Driving focus on upside risk exploitation (opportunity), rather than just downside risk mitigation, is of equal importance. Opportunistic thinking is an essential consideration of the group-wide and divisional strategy-setting processes.

Two significant initiatives over the year have accelerated the group's journey of continuous improvement in ERM maturity.

1: Risk Maturity Assessment

At the request of executive management to continuously improve and enhance the group's ERM strategic approach, KPMG completed an independent maturity assessment of risk processes across the group. A maturity continuum has been developed by considering recognised and leading practice, various governance and risk codes, and reference to the KPMG Global ERM Methodology. It is aimed at guiding organisations in achieving their desired risk maturity status. Accordingly, the results of the review were plotted against the KPMG risk maturity framework that considers seven key ERM life cycle elements with sub-elements as illustrated below:

Risk strategy and appetite	Linkage to corporate strategy	Risk strategy	Risk appetite and tolerance				
Risk governance	Board and oversight committee	Company risk operating structure	Risk guidance	Roles and responsibilities	Decisions		
Risk culture	Knowledge and understanding	Belief and commitment	Competencies and context	Action and determination			
Risk assessment and measurement	Risk definition and taxonomy	Risk identification	Assessment and prioritisation	Quantitative methods and modelling	Risk aggregation, correlation and concentration	Scenario analysis and stress testing	Capital and performance management
Risk management and monitoring	Risk mitigation, response and action plans	Testing, validation and management's assurance	Monitoring	Risk in projects/ initiatives			
Risk reporting and insight	Risk reporting	Business/ operational requirements	Board and senior management requirements	External requirements			
Data and technology	Data quality and governance	Risk analytics	Technology enablement				

2: Strategic Risk Assessment
Risk identification is driven through a hybrid approach of a top-down and aggregated bottom-up process. An interactive dynamic risk assessment workshop, facilitated by KPMG global risk thought leaders, helped identify the group's top-down strategic risks. Twenty-five senior associates representing all group functions participated in this session. The workshop extended far beyond traditional risk assessment methods (impact and likelihood) to capture the following features:

Velocity	Measures the speed at which risk expects to materially impact the organisation upon onset
Strongest risk clusters	Groups of risks that have been identified by the survey participants as more strongly connected and therefore should be considered in combination for risk management purposes
Most pervasive risk emitters	These risks have a greater potential to trigger or amplify other risks within the network due to their centrality by cause
Weakly-linked risks with expected severe outcomes	Combinations of risks that display weak links to each other but pose disastrous aggregate severities
Most convergent risk receivers	These risks are significant in that they are triggered or made worse by other risks due to their centrality by effect

The results of this workshop served three key purposes:

- Enabled careful and informed consideration of threats and opportunities in the finalisation of the group strategy
- Identification and confirmation of the key strategic risks facing the group to allow for risk focus throughout
- Development of a three-year strategic internal audit and assurance plan

The prevailing pandemic and related risks tested each divisional business model and reinforced the necessity for an enhanced risk discipline within strategic and tactical activities. While management could not predict every eventuality, circumstances and outcomes have confirmed the resilience of the group in arguably the most challenging operating environment in the history of the organisation.

Further detail on key strategic risks, the link to material matters and the group's response can be found in the strategy, material matters and key risks section on pages 38 - 51.

Top Ten Risks

The strategic risk assessment identified the following key strategic risks facing the group:

Risk Category		Risk Statement
1.	**Clear strategy and vision**	The risk that the lack of an articulated growth strategy will result in an inability to achieve desired growth
2.	**Competitive landscape**	The risk that actions of competitors or new entrants to the market threaten the organisation's competitive advantage or even ability to survive
3.	**Leadership and organisational agility**	The risk that leadership behaviour and its impact on organisational health impacts the ability to achieve goals
4.	**Brand reputation (incl. supplier ethical risks)**	The risk that associates, or parties with whom the company transacts, conduct themselves in a manner that damages the reputation of the company's image
5.	**Culture and behaviours**	The risk that culture and behaviours do not engender the correct values, behaviours to engender organisational health
6.	**Talent attraction and retention**	The risk that an inability to attract and retain key skills impacts the ability to execute strategy
7.	**Macro, socio-political, socio-economic and regulatory environment**	The risk that adverse political actions, social unrest, declining economic conditions and onerous legislative requirements impact growth imperatives
8.	**Systems and technology**	The risk that IT systems lack capability and capacity to support operations and future growth
9.	**Supply chain**	The risk that an inefficient, ineffective and unreliable supply chain will result in poor inventory management that will impact competitive advantage
10.	**Transformation**	The risk that a slow pace of transformation will result in adverse reputational and commercial damage

Risk Operating Model

The risk operating model allows for the aggregation and dissemination of the group's risks, enabling the group to understand the relationships between risks across multiple divisions and captures material risk exposures generated from varying perspectives. The model remains unchanged from the previous year.

Risk Oversight

Risk and IT committee

- Governance and oversight of risk activities (refer to committee mandate on www.mrpricegroup.com)
- Approve the risk appetite for the group
- Approve risk management components
- Discuss group-wide risks and opportunities facing the business (as detailed in the strategy, material matters and key risks section section on pages 38 - 51).

Risk Management

Executive management

- Define risk appetite
- Evaluate risk mitigation plans
- Provide risk-related information
- Focus on strategic group risks

Risk function

- Create a common risk framework
- Provide guidance on the application of the framework
- Identify and assess risks
- Aggregate, coordinate and report risk information and processes
- Ensure adequate mitigation by management relative to impact and proximity
- Track risk responses
- Provide training and guidance

Internal audit

- Provide assurance on the effectiveness of the risk management process
- Provide assurance on risk mitigation steps

Risk Ownership

Trading divisions and centres of excellence

- Operate within the risk appetite and governance structures
- Respond to risks in a timely and effective manner
- Focus on tactical risks while aligning to strategic group risks

Tactical and Operational Risk

In addition to the focus on strategic risks, the group appreciates the need to manage daily operational and tactical risks to preserve the value-driven model. Whilst these risks are managed through divisional management and as part of daily operations, there is oversight by executive management and key assurance providers on key metrics and KPIs.

Risk Incidents and Emerging Risks

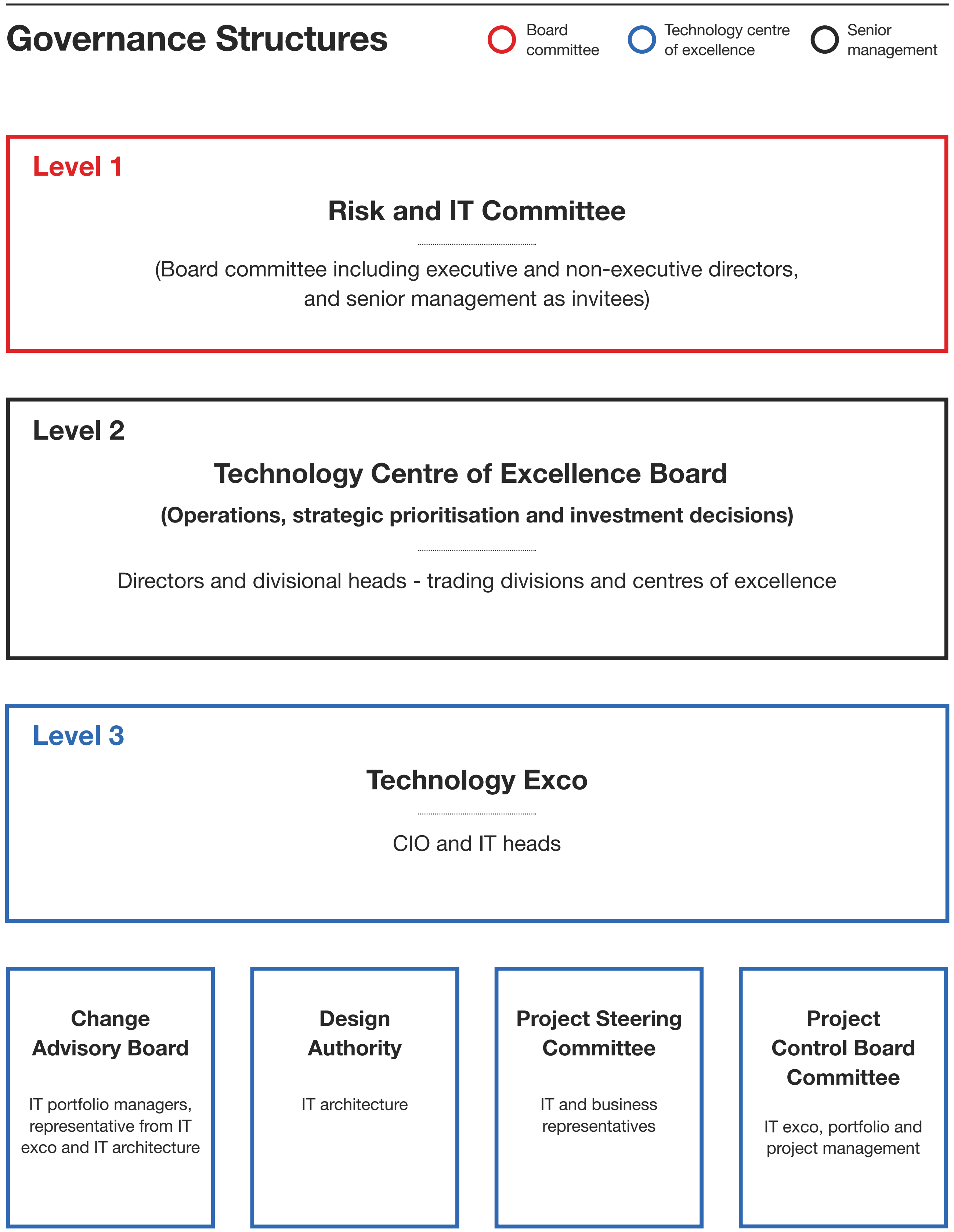
Any major risk incident is immediately reported to executive management and the board, through the committee. These include qualitative and quantitative matters such as:

- Risk of reputational damage
- Serious injury or death of a customer or associate
- Material ethics or compliance breach
- Extended IT system failure
- Significant business interruption event

Quarterly risk committee reports provide a deep level of visibility of risk events, responses, lessons learned and business changes. A structured risk screening process is in place and provides insights on emerging risks internally and externally, including potential 'black swan' events.

Information and Technology Governance

The committee is accountable for overseeing that IT is governed through the King IV™ principles. The committee has delegated the responsibilities to the CIO to manage through various IT management committees.



Governance Structures

○ Board committee ○ Technology centre of excellence ○ Senior management

Level 1

Risk and IT Committee

(Board committee including executive and non-executive directors, and senior management as invitees)

Level 2

Technology Centre of Excellence Board

(Operations, strategic prioritisation and investment decisions)

Directors and divisional heads - trading divisions and centres of excellence

Level 3

Technology Exco

CIO and IT heads

Change Advisory Board

IT portfolio managers, representative from IT exco and IT architecture

Design Authority

IT architecture

Project Steering Committee

IT and business representatives

Project Control Board Committee

IT exco, portfolio and project management

In FY2021, the technology centre of excellence set out to provide robust, agile and innovative solutions that enable the group to be a top-performing value retailer. The past year has been challenging yet rewarding.

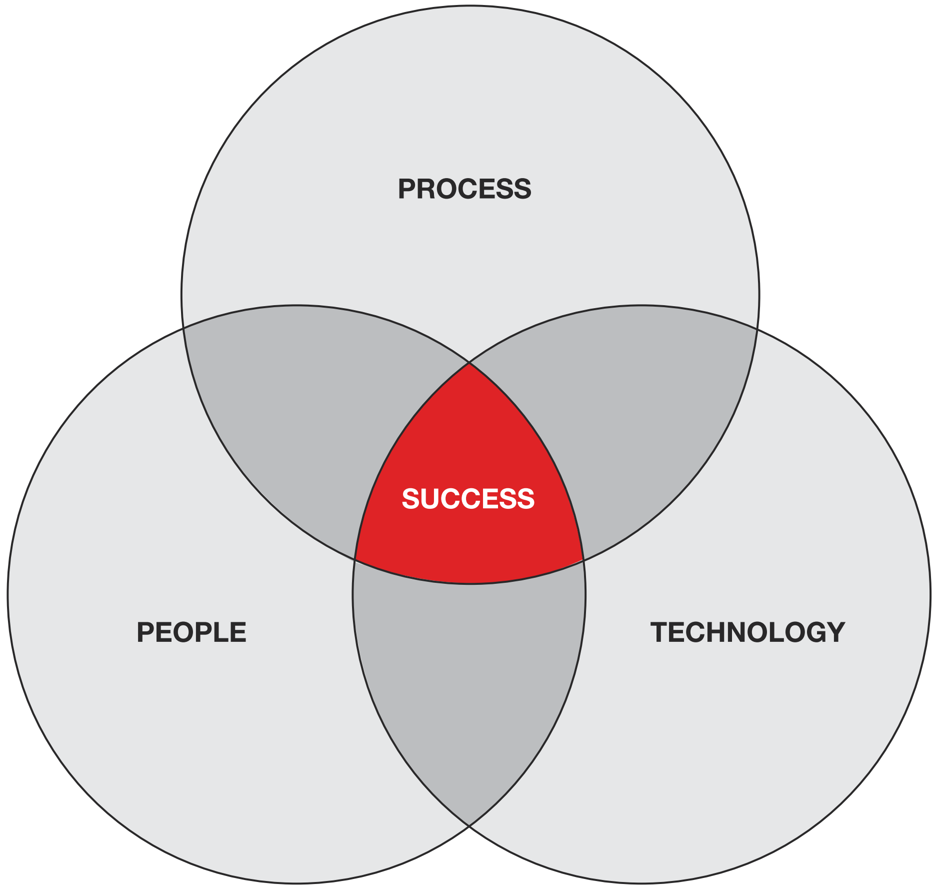
COVID-19 disrupted many plans. During the hard lockdown period, the priority was to ensure that as many associates as possible could remain productive and work from home. Support included the upgrade of any congestion points such as the network lines into head office, an accelerated acquisition of mobile devices such as laptops and data cards, and the support required to set up and manage all users to facilitate secure remote working. On the re-opening of limited retail activities, configuration changes were made to the point of sale and e-commerce systems to allow for the trade of essential items only, shifting items for sale through different lockdown levels. To support the head office environment and remote working, the committee facilitated the broader roll-out and adoption of technology. This included the expanded use of MS Teams. It is pleasing that a significant amount of both small and large innovations were delivered during this very disruptive time:

- Scan to pay solution
- Foot counter and ranging apps
- E-commerce solution for Miladys
- New payments offering — RCS payment in-store and Zapper for account payments

Whilst the country was in lockdown, the group's technology function continued to focus on the delivery of key strategic projects such as the total network migration, a disaster recovery cloud solution, the implementation of a new finance enterprise resource planning (ERP) system and the demand and fulfilment solution roll-out. These projects are key enablers for the upcoming years and to support the group's growth agenda.

During FY2021, there were no major IT incidents or security breaches. Cyber security will remain a key risk for the group due to its continuously evolving nature. The internal audit function plays a key role in monitoring the effectiveness of IT management and controls, which transitioned to KPMG during the year. The technology function remains committed to maintaining a reliable control environment, with ongoing opportunities to improve cyber security risks, project management and the operating environment.

The role of the technology centre of excellence within the group has shifted from that of a service division to a strategic enabler of business growth and innovation, helping the group compete and innovate.



The vision for the future is to provide agile and innovative solutions to enable the group to be the most valuable retailer in Africa.

Future areas of focus are:

- To develop a complete end state retail architecture to steer investment choices and enable growth and sustainability
- Transition from the legacy ERP to the Oracle ERP, which remains the number one priority, as this reduces the key reliance on an aged hardware and software landscape
- Customer centricity to service both internal (investment in new human capital management capabilities) and external customers, including investments in the omni-channel experience, which incorporates the implementation of a group CRM solution, an upgrade of e-commerce sites and a focus on improved logistics
- Investment into the foundational technology refresh to future proof and stabilise core infrastructure, including servers, storage, networks and the appropriate monitoring tools
- Newly defined cyber security roadmap will be implemented, as well as further investments in cloud disaster recovery capabilities to improve the cyber security posture of the group, while remaining vigilant of this key group risk
- Planning for the integration of the new acquisitions to ensure strategic alignment and extract synergistic opportunities

As the group progresses through the transformational ERP journey this year, opportunities in omni-channel, digital transformation, further automation and innovation will also be explored. Details of the impact of IT projects on the delivery of the group's strategy are included in the strategy, material matters and key risks section on pages 43 and 51.