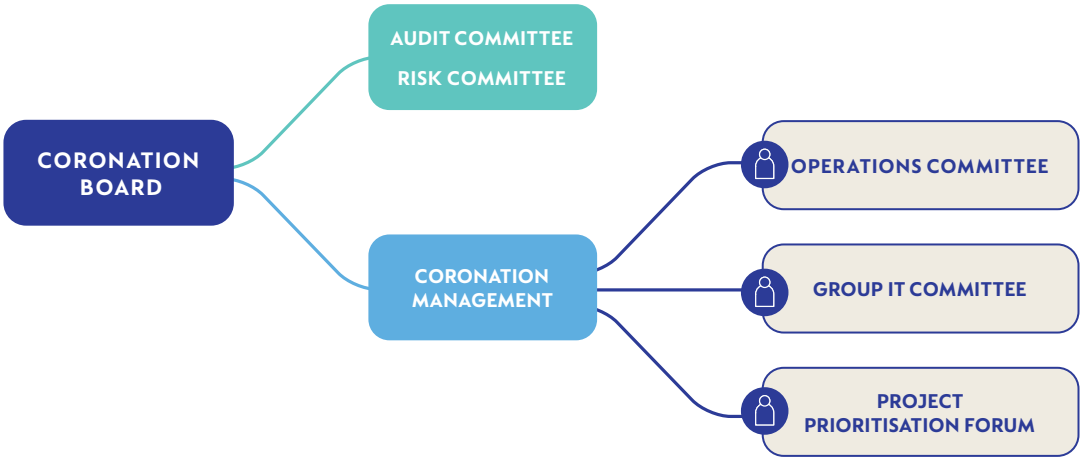
Information Technology and Systems Report

The effective management of information technology (IT) and information systems (IS) is key to achieving our strategic objectives, particularly in delivering excellent client service and supporting long-term investment outperformance. The Board aims to represent the interests of all stakeholders in delivering a successful and sustainable business. Accordingly, the Board is accountable for governing the ethical and effective application of resources towards the achievement of strategic outcomes to create value for stakeholders. At Coronation, IT and IS are viewed as key enablers of the Group's strategic objectives and, as such, require robust governance. The Board has identified the following as key technology and information governance objectives:

- Monitoring the alignment of the short-, medium- and long-term strategies of the business and technology;
- Maintaining formalised IT governance at Coronation, aligned to existing corporate governance structures and leading practices;
- Monitoring the integrity and availability of technology and information to meet business needs in a timely manner;
- Developing and maintaining appropriate organisational structures, relationships, frameworks and processes to support IT governance;
- Measuring and managing the cost and the value received from technology;
- Managing technology resources and assets, including information, in an efficient and effective manner, such that the value derived from these resources is maximised;
- Safeguarding technology resources and information;
- Monitoring adherence to legislative requirements and other guidance as it pertains to IT management relevant to the Group, including but not limited to King IV™, Control Objectives for Information and Related Technologies, the Information Technology Infrastructure Library and the International Organization for Standardization 27000 series supporting information security (ISO 27000);
- Establishing appropriate policies and frameworks that articulate and give effect to the key technology and information objectives set by the Board; and
- Establishing performance criteria aligned with operational expectations and periodic measurement of actual versus desired performance levels.

The Board has delegated to management the responsibility of implementing and executing effective technology and information management. Management approves the direction for how IT should be managed and is supported by the Operations Committee, the revamped Group Information Technology Committee and the Project Prioritisation Forum. In addition, the Board has mandated the Audit and Risk committees to oversee the adequate and effective risk management and system of internal control, including those pertaining to technology. The organisational and governance structure is illustrated below. We also set up dedicated committees to deal with specific technology projects.



Party	Role and responsibility
Coronation Board	› Sets strategic goals and objectives for the business, including IT-related goals and objectives. › Evaluates and approves significant IT-related initiatives. › Exercises ongoing oversight of IT management. › Evaluates the effectiveness of the Company's IT arrangements, including outsourced services, in achieving strategic objectives. › Monitors implementation of significant technology initiatives/projects. › Monitors the management of technology-related risks, including cyber risk, with the support of the Audit and Risk committees.
Audit and Risk committees	› Monitor the management of IT-related risks, including cyber risk. › Oversee technology, IS and information-related assurance.
Management	› Establishes the target business and operating model to achieve strategic goals established by the Board. › Responsible for implementation and execution of effective IT management within the business. › Proposes significant IT-related initiatives prior to seeking Board approval to implement. › Oversees major IT projects.
Operations Committee	› Drives implementation of IT-related projects. › Recommends technology-related projects to executives based on strategic goals and objectives. › Oversees end-user acceptance of technology. › Responsible for the operational management of IT.
Group Information Technology Committee	› The Committee is responsible for ensuring that the effectiveness and efficiency of the Group's IT systems are met from a risk and strategic alignment perspective so that IT systems support the strategic objectives of the Group. › This Committee has the broad overall responsibility to monitor the adequacy, efficiency and effectiveness of all the Group systems relevant to IT, both operational and strategic, in as much as these may impact the business strategy, financial performance, risk profile and IT Strategy of the Group.
Project Prioritisation Forum	› Prioritises and optimises efficient delivery of approved projects.

Improving direct client service experience and security

We have embarked on a rewrite of our Client Online Services (COS), our online transactional platform for our direct clients. The vision for the project is to provide an intuitive portal that reflects our long-term investment philosophy, where investors can easily find the information they need and transact in a simple and secure environment. The new site will be mobile friendly and will introduce new features that are currently not available on our existing platform. The first major release was in November 2021 and existing COS users were automatically migrated onto the new platform.

Data Disruption Project

This project is focused on the delivery of high quality, timeous data via a scalable cloud platform. Data is becoming an increasingly important asset by global standards and our management of data has evolved by thinking about our data differently, the formalising of data definitions and introducing improved governance to every aspect of data management.

We expect the project to deliver significantly better data more efficiently, and that we will have greater insight into each data point from definition through to where it is either presented or used. This will result in both a golden source of data and a much better understanding of the impact of our data across our business, and its use and value to each individual business area.

The business risk of incorrect reporting and/or incorrect calculations will be reduced, and data management significantly improved, as we manage what we measure and formalise data ownership. We are taking an iterative approach to the delivery of this project, with the first iteration currently running in parallel with production. The overall benefits will be the improved speed and accuracy of data outputs. The data sets and related reporting outputs associated with the first phase of the project are planned to be taken live in the first half of 2022.

The management of technology risks

Coronation's key technology risks are detailed below. During the past year, there was no material breach of our IT and IS security processes. We measure the value added by our IT Strategy and investments against the following benchmarks:

- Vulnerability of the platform to cyber attacks;
- Improvements in client service and meeting the evolving needs of clients;
- Derisking of the business;
- The scalability and flexibility of systems;
- Operational efficiencies and cost savings; and
- Platform stability.

Outcomes are measured through active monitoring and feedback from clients and intermediaries. Our evaluation of our performance against these benchmarks is favourable. We remain committed to ensuring that they are met through our efficient delivery of sustainable, scalable technology solutions.

IT and IS risk management

We consider technology risks as part of our overall risk assessment. These risks are incorporated in an annual operational risk assessment and material IT/IS risks are escalated to the key risk register, which is submitted to the Risk Committee. The Committee also reviews regular reports on IT and IS risk. Key technology risks are detailed on the following page.

Risk	Mitigation strategies
Cyber security risk	• Cyber risk is holistically managed across people, processes and technology. This includes: › enforcing appropriate policies; › conducting ongoing employee awareness; and › employing technology to prevent and/or detect potential or actual threats to the security of our environment. • Vulnerability management occurs regularly whereby the server and desktop environments are scanned for threats and patches deployed as needed. • Independent subject matter experts perform penetration testing on a regular basis, and the implementation of recommendations is closely monitored. • Live monitoring of cyber threats and system logs occurs via our dedicated Security Operations Centre.
The inability to maintain accurate, complete, consistent and reliable data	• A significant amount of data has been migrated to a data warehouse. • A Master Data Management process has been implemented for static and analytics data. • An accelerated and extensive Data Disruption Project was initiated in 2020.
Policies and processes do not adequately ensure protection of client data, including sufficient oversight of data at our service providers	• Improving information management and security is a never-ending journey. A cross-functional team in the form of an Information Management Steering Committee actively identifies and manages information-related risks and improves information management processes. Focus areas of the programme over the period included: › improving the maturity of information management processes and systems; › reviewing and enhancing systems that proactively protect against common data breach vulnerabilities; and › managing third-party access to data stores and emphasis on employee awareness and training. • Subject matter experts were engaged to assist with our improvement programme and to test the effectiveness of IT security at various intervals throughout the year.
Disaster recovery and business continuity	• Comprehensive business continuity and disaster recovery plans are tested at least twice a year to ensure complete restoration of core business functions in the event of a disaster, within a defined recovery objective. This includes user acceptance testing to verify recovered systems are fully operational. • The continuity and recovery plans include offsite retention of data backups and access to a recovery warm site.
Failure to resolve data validation and integration errors between internal and external systems accurately and in a timely manner	• We have a number of procedures in place for the early detection and resolution of variances, including automated and manual reconciliations that are performed to detect variances, as well as an alert system on automated errors.

Risk	Mitigation strategies
Unavailability of cloud-based solutions	› Highly available connectivity is provisioned for all cloud-based services. › Strong relationships are maintained with vendors and connectivity is continually monitored and evaluated. In addition, clear escalation paths are defined, and cloud due diligence assessments are performed.
Inability to recruit IS employees with the relevant skills and experience	› Coronation has talent management initiatives (→ *refer to page 70*) to attract highly skilled employees. In the event that it is not possible to recruit IS employees of suitable skills and experience, an insourcing arrangement will be entered into.
Failure to upgrade or replace key systems and infrastructure to meet changing business needs/business priorities	› An IS strategy is in place, which governs the replacement strategy of key systems and the achievement of business requirements. › Furthermore, IT and IS report to the COO, facilitating integration of alignment between business and technology.
Failure to secure client and other confidential data on mobile devices	› Encryption and Bring Your Own Device policies are in place. Mobile devices are secured before allowing Company data consumption. › Our systems also have the ability to remotely wipe and secure mobile phones.

The IT general control environment is annually assured in accordance with ISAE 3402. The results of these reviews are reported to the Audit and Risk committees.

Future focus

- We continue to focus on the security of our environment.
- Governance, management and security of data remain a priority.
- Enhancing and extracting additional efficiencies from our outsourced services.
- The wider rollout of customer relationship management systems, improved automation and workflow.
- Effective management of vendors.
- Technology to complement ongoing flexible working scenarios.