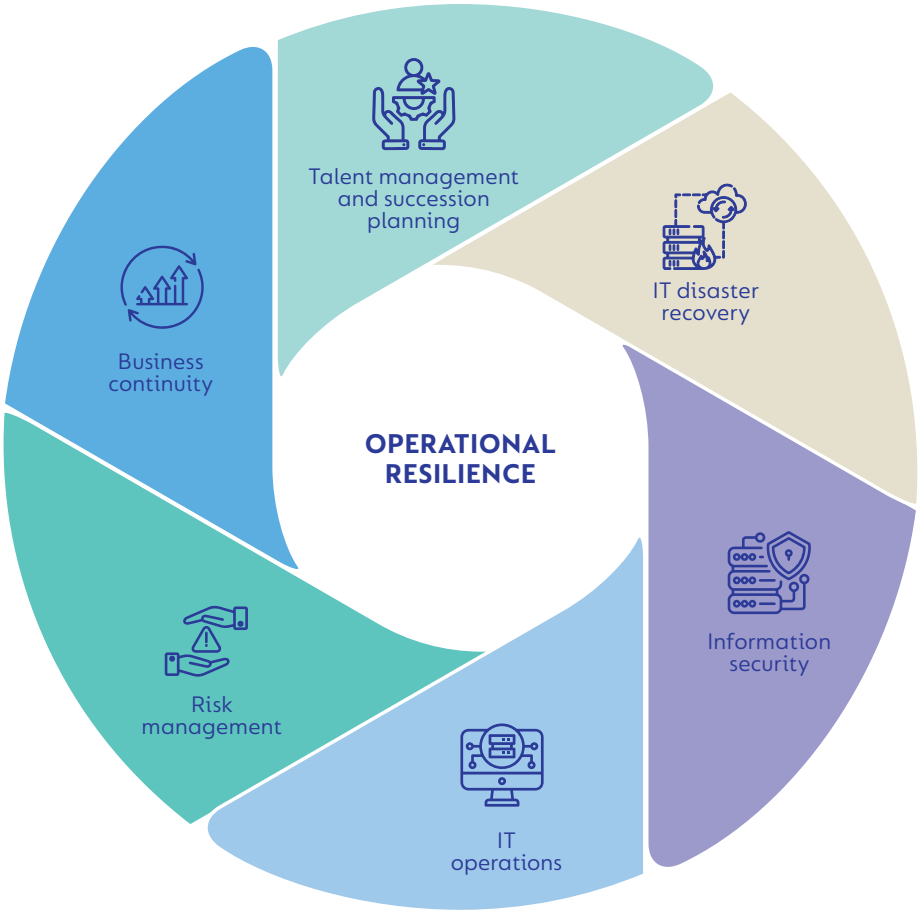
STRENGTHENING OPERATIONAL RESILIENCE

Coronation's ability to maintain business sustainably is contingent on our most valuable assets – our people and the enabling technology that supports them. We are committed to investing in both our technological capabilities and our people to benefit our clients and other stakeholders.

The key pillars of our operational resilience relate to the strengthening and efficacy of our business processes and related risk mitigation.



We actively invest in our people and the technology that enables their success, with a particular focus on maintaining a highly skilled workforce via education, training and wellness initiatives. From a technology perspective, we are focused on achieving efficiencies, greater innovation and robust risk management. The key investments are in client service systems, strengthening our local and global investment capabilities, optimising information systems, data management and cybersecurity.

Talent management and succession planning

In a highly competitive industry, the long-term retention of world-class talent is critical to the success of our business. Our investment team remains one of the most experienced and stable in the industry. Similarly, we have an enviable staff retention ratio and our employees across the business are highly skilled. Coronation is a meritocratic, team-based organisation, with a strong ownership culture.

Ownership is a key pillar to our success and aligns employees' interests with those of all other stakeholders, empowering employees and entrenching long-term thinking across all areas of the business. This is evidenced by the fact that 29% of our business is owned by our employees and our remuneration structure facilitates entrenchment of this culture.

In order to retain and motivate our employees we have maintained a number of initiatives focused on education, training, wellness, and culture. These initiatives include but are not limited to the following:

- Encouraging employees to further their education and to further develop their skills, with a key focus on supporting investment team members to become CFA Charterholders
- Continuous professional development which is facilitated by a wide range of training initiatives
- Holistic wellness initiatives including making mentorship and coaching available to employees
- The Aspiring Leader Project, our formal continued workplace career development initiative

Looking ahead

In order to ensure the sustainability of our business, employee retention and succession planning are key focus areas. Future talent such as junior employees, interns and bursary students are earmarked in our succession planning processes. Management takes an active role in on-the-job training and mentorship of this talent. Succession plans for key roles across the business were reviewed both internally and by the Remuneration and Nominations Committee and relevant plans put in place.

IT disaster recovery

To ensure the continuation of our core functions in the event of a disaster scenario, a combination of Business Continuity and Disaster Recovery Plans have been established (refer below for business continuity). The ultimate goal is the recovery of the critical functions required to enable our business to continue with minimal disruption, until such time as the full operational environment has been restored.

Three key phases of disaster recovery:

- Notification/Activation Phase: to detect and assess damage and to activate the BCP
- Recovery Phase: to restore temporary operations and assess damage to the system
- Reconstitution Phase: to restore system processing capabilities to normal operations

There is regular business continuity testing to ensure we are adequately prepared for any business disruptions.

Information security

As custodians of client and third-party data as well as our proprietary information, Coronation has an ethical and legal obligation to apply accepted industry standards in how we safeguard that information. This includes safeguards from risk of loss, theft, unavailability, and unauthorised access, and to treat the information we gather and create as a corporate asset.

It is Coronation's intent to ensure that information will be protected from a loss of:

Confidentiality: information is accessible only to authorised individuals.

Integrity: safeguarding the accuracy and completeness of information.

Availability: that authorised users have access to relevant information when required.

We adopt a risk-based approach to information security and apply leading practice standards in designing and implementing controls where relevant to our business.

IT operations

IT and IS infrastructure, systems and business support functions are maintained by experienced in-house teams, each respectively reporting to the Head of Information Technology and Head of Information Systems. We apply a holistic approach to managing IT and IS risks across the business, focusing on both the technology and systems and the people who run them, as well as the people and processes they support.

Technology

- We maintain infrastructure on site as well as virtual hosting and storage platforms
- We have active monitoring systems measuring the health of our infrastructure and systems, and monitoring our cloud and/or hosted application programming interface (API) endpoints
- Technology includes advanced access control systems, environmental monitoring and detection systems, and power management. Backup and redundancy systems are employed as appropriate
- Data security is managed via advanced threat intelligence, monitoring systems and a 24/7 active Security Operations Centre (SOC)
- The Head of Information Technology and the Head of Information Systems work closely with the Risk and Compliance team to maintain technology-specific risk registers, and report regularly to the Audit and Risk Committees on IT- and IS-related risks

People

- Users are regularly made aware of their individual responsibility regarding information security, as encompassed in our various policies
- We are part of a South African financial services industry cybersecurity forum and global cyber intelligence community through the Financial Services Information Sharing and Analysis Centre (FS-ISAC). This facilitates sharing information regarding industry-specific risk and employs a qualified information security team whose collective certifications include:
  - Certified Information Security Manager (CISM)
  - Certified Information Systems Security Professional (CISSP)
  - Certified Ethical Hacker (CEH)
- Our Senior Management team frequently attends technology and cyber panels and events to ensure we remain ahead of the curve

Process

- Key IT processes are documented and periodically revised to remain current
- Independent assurance is regularly obtained

Risk management

Risk is an inherent and unavoidable part of any business. Appropriate risk management is crucial to protect stakeholder interests, ensure adherence to regulatory requirements and maintain the long-term sustainability of the business while entrenching corporate governance principles.

Risk management is a multi-faceted discipline that requires appropriate governance, independent monitoring, frequent communication, the application of judgement and robust knowledge of specialised products, operations, legislation, technologies, and markets.

Risk management is thus a continuous process that should effectively deploy resources to minimise the probability of negative events while maximising the realisation of opportunities. We adopt a dual top-down and bottom-up approach to identifying risks, which considers the external environment and strategic planning to identify key strategic risks, as well as identifying risks at the operational level, which includes technology, process, client, and product-specific risks.

Business continuity

A significant focus of our Business Continuity Plan relates to key personnel dependency and succession planning. Coronation mitigates this risk as follows:

- Key senior managers: we endeavour to have at least two senior managers covering similar oversight responsibilities
- Key functions: investment team follows a co-portfolio manager model
- Succession plan for all key managers addressed annually and reviewed both internally and by the Remuneration and Nominations Committee

Incident management

When faced with incidents that could disrupt the delivery of critical operations, the Exco is responsible for decision-making, supported by internal and external resources. This includes the following:

- Maintaining an inventory of incident response and recovery resources, including learnings from the experience of others
- Co-ordinated incident response procedures, including regular formal meetings on the matter in order to make timely decisions and the appointment of key persons
- Managing communication to stakeholders with an emphasis on mitigating risk and reputational impact
- Conducting detailed post mortems and incident reports to ensure appropriate measures are implemented to prevent recurrence