

Risk Management Report

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. At Coronation, the Board is ultimately responsible for ensuring that risks are managed effectively within a defined tolerance (risk appetite). The Board has delegated responsibility for overseeing risk management to the Risk Committee and, ultimately, to management and the risk management function.

Risk management is a multifaceted discipline that requires appropriate governance, independent monitoring, frequent communication, the application of judgement and robust knowledge of specialised products, operations, legislation and markets. Coronation's risk management objectives are to:

- create risk awareness and understanding across all levels of the business;
- integrate risk consciousness into daily decision-making and implementation processes;
- facilitate risk identification and mitigation across the Group within the risk appetite and risk tolerance parameters defined by the Board;
- improve the ability to prevent, detect, correct, escalate and respond to critical risk issues by conducting risk monitoring; and
- apply appropriate risk management and corporate governance frameworks and guidelines.

Our Risk Management Strategy and Framework (the Risk Framework) more fully articulates the Risk Management Policy and guides the approach to risk management across the business. The Risk Framework describes the key elements of risk management as illustrated in the adjacent diagram. Risk management is 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 process, client and product-specific risks. Management are risk owners and take an active role in day-to-day risk management. This includes responsibility for identifying, evaluating, mitigating, monitoring and reporting risk in accordance with the Risk Framework.

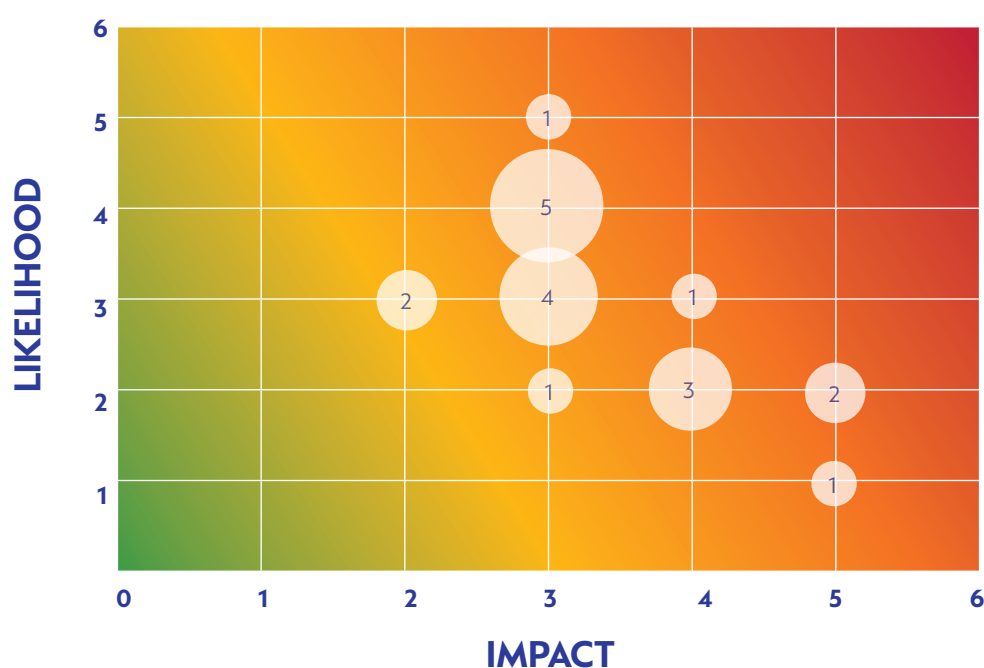


The risk management function comprises the Risk Officer, who reports to the Head of Global Risk and Compliance. The Risk Officer is responsible for overseeing and reporting on management's procedures to manage risk across the Group. More specifically, the Risk Officer is responsible for ensuring that policies and procedures are established for measuring, managing and reporting risk.

All Risk Committee meetings are attended by the Head of Global Risk and Compliance and the Risk Officer, each of whom deliver their reports separately at each meeting. The Committee reports back to the Board at quarterly meetings and escalates material matters to the Board. Additionally, ongoing interaction occurs with executive members of the Board and the senior management team.

We have developed, implemented and continuously improve the Risk Framework to ensure that the management of risk is integrated into the organisation's overall corporate governance structures, strategy, planning, reporting, policies, values and culture. We recognise that in a complex financial services environment, risk management processes and strategies should evolve, and should be subject to ongoing review and modifications, considering risk appetite, risk tolerance and risk resilience.

Included below is the residual risk rating description utilised across the Group and the related risk heat map. The risk heat map is a diagrammatic representation of the risk profile. The risk profile aligns to Coronation's risk tolerance and appetite. Any risk exceeding the risk appetite is monitored on an ongoing basis and plans are put in place to reduce the risk rating.








Note: Numbers plotted indicate number of risks per applicable likelihood and impact



The Group risk profile remains in line with the prior period, as there were no changes to the risk ratings. Refer to the key risk types on the following page.





Residual risk rating	Description of residual risk
From 0 – 8	Minor risks: risks are within the tolerable level and no further actions are required
From 9 – 10	Cautionary risks: should be monitored on a regular basis
From 12 – 15	Major risks: risk appetite has been exceeded. The risks must be managed, monitored on an ongoing basis and escalated
From 16 – 25	Critical risks: current control strategy should be reassessed immediately and escalated

The table below outlines the key risk types facing the business, along with the relevant mitigating controls. Refer to the residual risk rating table on the previous page.

Risk	Definition	Management and mitigation
STRATEGIC RISKS		
Reputational risk 	An action, event or transaction that may cause a loss of confidence in Coronation's integrity or otherwise damage the Coronation brand.	<ul style="list-style-type: none"> ➤ Our ownership culture, long-term strategic thinking and client-centric philosophy drive our behaviour, protect stakeholder interests and mitigate reputational risk. ➤ All forms of media are regularly monitored to enable a proactive approach to reputational risk management. ➤ Material events that may impact the Group are directly escalated to the CEO and Chairperson of the Board for consideration.
Market change risk 	The failure to respond to fundamental changes in the fund management industry, such as disruptive technologies, evolving distribution patterns or products to meet the changing profile and needs of clients.	<ul style="list-style-type: none"> ➤ Continuous investment in the Coronation brand and our direct investor infrastructure. ➤ Affirm our commitment to our long-term investment philosophy through ongoing client engagement and demonstration of thought leadership. ➤ Frequent review of fee structures to remain competitive and stay abreast of competitor consolidation and aggregation strategies. Active participation in industry bodies to influence legislative outcomes where possible. ➤ Develop new products in response to changing client needs, subsequent to in-depth research and viability assessments.
External environment risk 	The pandemic limits the achievement of strategic objectives and/or has negative impacts on the business.	<ul style="list-style-type: none"> ➤ Business Continuity Plan reviewed and updated. ➤ Continue to work closely with our third-party service providers to ensure minimal disruption to operations.
Transformation risk 	Not responding in a considered manner to achieving true transformation and potential non-achievement of Financial Sector Code targets.	<ul style="list-style-type: none"> ➤ The Employment Equity (EE) Committee reports to the SET Committee and: <ul style="list-style-type: none"> › oversees achievement of transformational targets in accordance with our EE Plan; and › ensures that policies and practices encourage sourcing and retaining of talented black individuals. ➤ Significant investment in educating previously disadvantaged youth is made through our bursary, internship and graduate recruitment programmes to support the recruitment pipeline (→ <i>refer to page 77</i>).
Environmental risk 	Our investment and corporate activities having an unintended environmental (including climate change), social and economic impact.	<ul style="list-style-type: none"> ➤ The Board has mandated management to conduct a carbon footprint assessment of the Company and to report on the measurements. ➤ The Board has further resolved that the Company should prioritise and invest in projects that would offset its carbon footprint by no later than the end of 2021, with the aim of achieving a carbon neutral footprint. ➤ There is a three-pronged approach to ESG: Integration, Engagement and Collaboration as detailed in our Stewardship Report, which is available on our website. ➤ Carbon intensity benchmarks for our portfolios are below the industry benchmarks.

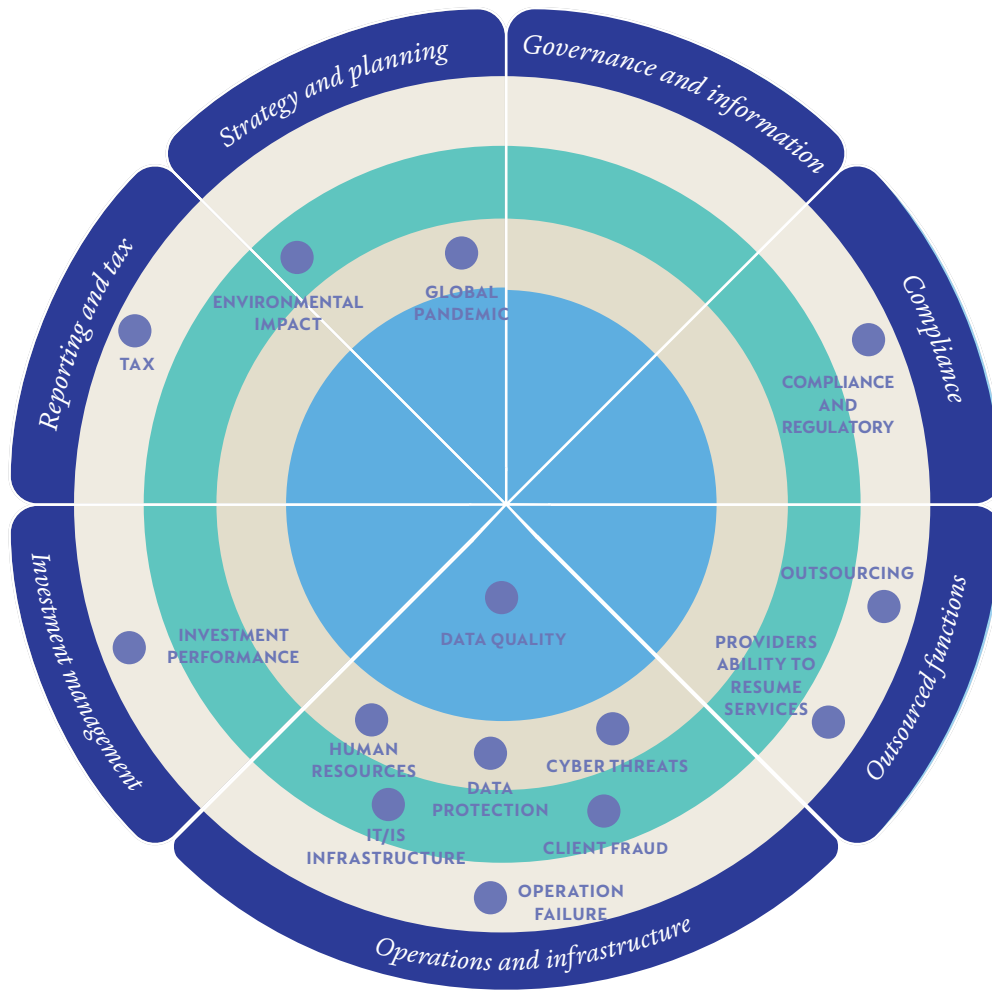
Risk	Definition	Management and mitigation
COMPLIANCE		
Compliance and regulatory risk 	Non-adherence to regulations.	<ul style="list-style-type: none"> ➤ Robust compliance programme maintained to ensure compliance with all relevant regulations. ➤ Compliance department, aided by specialised external compliance consultants as needed, implements and tests adherence to current regulation on an ongoing basis. ➤ Ongoing employee training and awareness on compliance-related matters and new regulatory requirements. ➤ Continuous monitoring of the regulatory pipeline for new or amended legislation potentially impacting the business. Periodic independent assurance on the adequacy and efficacy of our compliance arrangements.
GOVERNANCE AND ETHICS		
Conduct risk 	The failure of employees to comply with Coronation policies, resulting in behaviour that is detrimental to clients, illegal, unethical or otherwise damaging to Coronation's reputation.	<ul style="list-style-type: none"> ➤ An ethical and client-centric culture is driven from the top throughout the organisation. Acting in the best interests of clients is central to all that we do, and there is a common understanding that if we lose the trust of our clients, we will not have a business. ➤ Employees undergo robust screening and vetting prior to being appointed. ➤ Preventative and detective controls include the following: <ul style="list-style-type: none"> › Independent review and segregation of duties are embedded in the control environment; › Ongoing employee training and awareness creation of Coronation policies. The compliance department conducts regular monitoring of adherence to key policies; › Key personnel are subjected to periodic criminal and credit checks; › Externally managed whistle-blowing hotline where employees can anonymously report any unethical behaviour 24/7; and › Robust Operational Risk Assurance Plan that independently tests adherence to key processes and controls.
INVESTMENT MANAGEMENT RISK		
Investment performance risk 	Sustained poor investment returns relative to peer funds and benchmarks.	<ul style="list-style-type: none"> ➤ All client assets are managed by a single and stable investment team of highly skilled individuals who are unwavering in the application of our tried and tested investment philosophy, underpinned by our commitment to the long term. ➤ The investment team is subdivided into areas with specific focus per asset type and/or region, which rigorously monitor the markets and make investment decisions supported by our proprietary research. ➤ The investment team is predominantly based at our Cape Town headquarters, which facilitates continual in-person engagement, further entrenched by a daily morning meeting of all investment team members. ➤ Investment analysts have deepened their research and understanding of ESG factors. ➤ Extensive insights and thought leadership on markets and Coronation strategies are made available to clients, as well as the general public, via client communications, our website, conferences and our thought-leadership articles.

Risk	Definition	Management and mitigation
OPERATIONS AND INFRASTRUCTURE RISKS		
Human resources risk 	Inability to attract, motivate and prevent the departure of top talent.	<ul style="list-style-type: none"> ▶ Our people are our most valued assets. ▶ Accordingly, our work environment, culture and Remuneration Policy are designed to attract, retain and motivate great talent (→ refer to page 72). ▶ Our high-performance culture, employee ownership and personal career development opportunities are defining characteristics of our business. ▶ We maintain a bursary and internship programme (→ refer to page 77), which serves the dual purpose of developing the nation's youth and providing a workforce pipeline.
Cybersecurity risk 	Ineffective preparation for, and management of, cyber threats that may significantly disrupt core operations, cause financial loss and damage our reputation.	<ul style="list-style-type: none"> ▶ 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.
Data protection risk 	Policies and processes do not adequately ensure protection of client data, including sufficient oversight of data at our service providers.	<ul style="list-style-type: none"> ▶ A cross-functional Information Management Steering Committee actively identifies and manages information-related risks and improves information management processes. ▶ Focus areas over the period have included improving the maturity of information management processes and systems, reviewing and enhancing systems that proactively protect against common data breach vulnerabilities, managing third-party access to data stores and emphasis on employee awareness and training. ▶ Subject matter experts have been engaged to assist with our improvement programme and to test the effectiveness of information technology security at various intervals throughout the year.
Data quality risk 	The inability to maintain accurate, complete, consistent and reliable data.	<ul style="list-style-type: none"> ▶ 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 – see Information Technology and Information Systems Report (→ refer to page 103).
Information technology/information systems risk 	Obsolescence of infrastructure, deficiency in integration, failures/inadequacies in systems/networks that may significantly disrupt core operations.	<ul style="list-style-type: none"> ▶ Technology (information technology systems and data) is viewed as a key enabler of the Group's strategic objectives and, as such, a robust information technology and systems governance framework has been implemented (→ refer to page 103). ▶ The Board-approved framework sets out the objectives of technology, which includes ensuring high integrity and availability of technology and information to meet business needs in a timely manner.

Risk	Definition	Management and mitigation
OPERATIONS AND INFRASTRUCTURE RISKS (CONTINUED)		
Client fraud risk 	Coronation's clients are exposed to, and may potentially become the victims of fraudulent activity.	<ul style="list-style-type: none"> Business processes and controls are continuously improved and designed to prevent or detect potentially fraudulent activity. Regular independent assurance over the control environment. Implemented voice recognition software to further enhance the control environment. Participate in industry forums focused on fraud prevention. Ongoing employee awareness training.
Risk of operational failure 	Operational processes and controls may be inadequate and/or operating ineffectively, resulting in operational errors and financial loss.	<ul style="list-style-type: none"> Our Combined Assurance Model, including the annual Operational Risk Assurance Plan, delivers an ongoing assessment of the design and operating effectiveness of our control environment (<i>→ refer to page 53</i>).
OUTSOURCING		
Outsourcing risk 	The inability or unwillingness of an outsourced key service provider to discharge its contractual obligations.	<ul style="list-style-type: none"> A Service Provider Management Framework has been implemented which includes: <ul style="list-style-type: none"> robust oversight controls of key outsourced providers on a real-time and ongoing basis, including daily, weekly and monthly transaction reviews; monitoring adherence to service level agreements, implementation of formal communication channels and escalation procedures to manage and resolve issues identified; and conducting periodic, formal due diligences.
Outsourced providers continuity risk 	An event or system failure that could inhibit an outsourced provider's ability to perform core activities.	<ul style="list-style-type: none"> The business continuity plans of key outsourced providers are reviewed periodically as part of the formal due diligence process. Key systems are tested as part of Coronation's Disaster Recovery Testing.

Risk concentration

A representation of the types of risks within the business and the likelihood of the risk materialising. In the diagram below, the closer to the centre, the likelihood of the risk increases. The further away it is, the less likely it is to occur.



● Common ● Likely ● Moderate ● Unlikely

Nothing has come to the attention of the Board to indicate that there has been any material breakdown in the risk management function, processes or systems during the year.