IT security and risk management

Our vision is to continuously deliver efficient and effective information technology that enables business and excellent client service, within acceptable risk tolerance.

We continue to build information security and technology risk management capabilities across the group. Our strategy supports business resilience, protects information assets, and safeguards personal data by proactively identifying and mitigating risks to people, processes, systems and data. This approach is underpinned by three core principles – defence in depth, security by design, and role-based access – with an emphasis on group-wide coordination and efficiency.

Policies and procedures are in place, which govern the sound management of digital and technology resources. This includes comprehensive acceptable IT usage policies.

Intelligent security and data loss prevention controls protect against system compromise and unauthorised access or disclosure of information. These are supported by data breach monitoring and response processes in line with privacy laws.

Key infrastructure-related developments

Infrastructure-related developments aim to reduce our environmental footprint whilst improving efficiency. During the 2020 financial year we:

- Continued consolidating databases, reducing hardware footprint and power requirements
- Adopted containerisation, resulting in less physical servers required for business applications
- Accelerated digitalisation initiatives to reduce physical paper requirements
- Migrated from traditional spinning disk to solid-state storage with lower power and cooling requirements
- Adopted modern technologies, including energy efficient laptops instead of PCs
- Increased adoption of cloud services to reduce the reliance on on-premise data centres.

Key business application-related developments

Our business application-related developments are focused on consolidation and automation. During the 2020 financial year we:

- Continued to consolidate technology and support teams across divisions and geographies
- Standardised the use of security and service management applications across the group
- Increased the use of online software solutions that require little to no local server resources
- Drove automation through emerging technologies such as machine learning and robotics to improve efficiency.

In addition to these developments, a strategic decision was made to reduce our building footprint in the UK operations. The office space in which the central IT, information security, and networking teams were based was released. These teams were successfully moved into existing, energy-efficient offices.

Board oversight

The board of directors regularly oversee the technology and cybersecurity strategies. There are governance structures in place that meet regularly to review how technology and security risks are managed and report back to the board with relevant updates. Lyndon Subroyen, the global head of digital and technology, forms part of the group executive team. In addition, Laurel Bowden, an independent non-executive director, has relevant enterprise software and fintech expertise. Periodic directors' training takes place to educate and enhance awareness around digital, technology and cybersecurity matters.

Strategy

Investec recognises that information and technology resources are critical business assets which need to be appropriately managed and secured. Strategic roadmaps enhance capacity, scalability, security, and reduce reliance on legacy systems. We continue to drive innovation in line with business objectives – integrating people, processes, systems and information, and leveraging technology to sustain and enhance intellectual capital.

Fundamental to this is monitoring appropriate response to developments in the technology landscape, including the capturing of potential opportunities and the management of disruptive effects on the organisation. We strive to make ethical use of technology, protect client and employee privacy, and responsibly dispose of obsolete infrastructure and data.

The key principles underpinning our IT strategy are:

- Aligned technology architecture across the group
- Simplified application and data footprint
- Flexible and scalable technology environment
- Rapid delivery of new products and services
- Strategic and responsible use of data.

GOVERNANCE, RISK AND COMPLIANCE

6

Information security training

Security awareness is an ongoing activity and provided to all employees to ensure high levels of vigilance.

Information security training provides insight into the risks of data compromise, and arms staff with the knowledge they need to safeguard our data and their personal information. Awareness campaigns educate staff on potential threats and reinforce their responsibilities in protecting information.

The training, mandatory for all new starters and refreshed annually, covers a broad range of topics including:

- **Data protection:** The different classifications of information based on confidentiality and business criticality, and the importance of protecting these assets
- **Cybersecurity:** The dangers that are prevalent online, tricks and techniques used by cyber criminals, and how to guard against these
- **Mobile devices and social media:** The risks associated with using mobile devices and social media, and how to keep devices and personal data safe
- **Beyond the office:** The importance of being vigilant and how to protect information when out of the office, such as while working at home, in public places, or travelling
- **Security essentials:** The fundamentals of information security, social engineering, and secure use of technology resources to safeguard both corporate and personal data.

In addition to interactive security training, ad-hoc focused awareness takes place as needed through various channels including face-to-face, email, and the corporate intranet.

Information security training

In the 2019 financial year, a modular information security awareness campaign was rolled out to all employees to educate staff about the threats to our information, provide insight into the potential risks of data compromise, and arm them with the knowledge they need to safeguard our (and their) data. In the 2020 financial year, we continued to promote the existing training by enrolling all staff that had joined Investec after the initial campaign had ended, to ensure complete coverage. In addition, the security awareness training was made mandatory for all new starters, who are automatically enrolled upon joining Investec and are required to complete the training within five weeks.

76% of the 4 513 enrolled staff completed all five modules (2019: 81%; 3 945 enrolled staff)

Systems availability

Continuity capabilities are in place to maintain business operations during adverse events, and to minimise impact to clients and the broader financial system.

Fit-for-purpose resilience strategies are defined and tested per critical service and application. This includes relocation to alternate processing sites, implementation of high-availability technology solutions, and ensuring physical redundancy for critical infrastructure components.

Recovery strategies are validated at least annually to ensure they remain effective and appropriate. Resilience is further enhanced through alignment of security incident response, crisis management and business continuity processes.

Cybersecurity

Cyber risk remains a board-level agenda item. Periodic updates to the board keep them abreast of industry developments and informed on the group's security position.

We maintain a risk-based strategy incorporating prediction, prevention, detection and response capabilities. A mature security architecture, research, and threat intelligence ensure the group is adequately protected against advanced attacks.

Continual monitoring provides visibility and enables proactive response to evolving cyber threats. Cyber controls are stress tested through security assessments and attack simulations, run both internally and in conjunction with independent specialists.

We maintain active participation in the global cybersecurity industry to remain current and relevant.

Testing of our cyber defences is complemented by desktop exercises involving the board and senior leadership, to evaluate and improve cyber incident response and crisis management.

Targeted simulation attacks

Real-world cyberattack simulations are performed by external specialists to measure and improve our cyber defences. These are complemented by non-technical exercises involving the board and senior leadership to evaluate and improve cyber incident response and crisis management. In the 2019 financial year, a target simulation attack was performed by an independent cybersecurity firm to assess the group's defenses against potential cyber threats. In the 2020 financial year, our focus was on addressing previously identified weaknesses, and improving consistency and coverage of baseline cyber controls. We also enhanced our group-wide cyber maturity and incident coordination. In the year ahead, we aim to strengthen our cyber monitoring capabilities and automate incident response, to enhance our security visibility and resilience as a business.

Delivering against the SDGs

Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels