MANAGING OUR RISKS

We aim to instil conscious risk-taking across the group. We take a holistic and forward-looking view of the risks we face by continually assessing current and emerging risks. Our risk appetite is regularly reviewed, in response to changes in our operating context, and our exposures are managed accordingly.

Our key risk types, shown in our shared value model on page 14, are those that are foreseeable, continuous and material. They are inextricably linked to the nature of our business and what we do for our clients. Managing these risks effectively, which is done within the parameters of our board-approved risk appetite, is essential to protecting the interests of our stakeholders and creating shared value.

AIR 92 – 97 Our risk report sets out our enterprise risk management approach and outlines the key developments in managing our key risk types.

The constant change in our industry and operating environments gives rise to emerging risks. The potential impact of these emerging risks on the group's strategy and operations must be understood and managed. We have processes in place to adequately prepare for and respond appropriately to these emerging risks in our longer-term strategic decision-making.

Our top emerging risks are identified through our enterprise risk management framework and operational risk processes, specialist expertise within the group and a survey across the three lines of defence. This collaborative effort aligns our financial planning and provides a combined risk assurance view.

These risks are discussed at management and governance committees, allowing us to act to mitigate their long-term impact on our shared-value outcomes and reputation. The table below shows the key drivers and mitigants of our emerging risks, but do not represent all the activities which are being pursued to manage them.

Going forward, we will continue to improve the robustness of the emerging risk identification process. Specifically, we will aim to improve our ability to transform risk knowledge into actionable steps to further embed the enterprise-wide risk culture, and to identify opportunities for the group in the long term by effectively responding to emerging risks.

EMERGING RISKS	RISK DRIVERS	MITIGANTS
1 ***TECHNOLOGY*** *The inability to manage, develop and maintain secure, agile technology assets to support strategic objectives.*	• A multi-channel digital experience means more technology to keep relevant, up-to-date and safe from cyber fraud attacks. • New types of devices span an extremely wide range of security requirements and have very different security postures.	• Dedicated combined development, security and operational teams focus on speeding up implementation of projects and changes. • Continual testing of technology and applications to identify and rectify potential weaknesses that can be exploited by cybercriminals.
2 ***CYBER*** *The risk of financial loss, disruption or damage to reputation from breaches or attacks on transaction sites, systems or networks.*	• Remote presence technologies may increase the avenues for attack. • Increasing number and sophistication of cybercrime incidents globally.	• Use of adaptive cybersecurity which uses a combination of artificial intelligence and other methods to dynamically shift tactics and detect and remove threats as quickly as possible. • Multi-factor authentication integrated into all critical payment applications and end-user devices. • 24/7 cybersecurity operation centres have improved monitoring capabilities to address evolving cyber vulnerabilities and attacks.
3 ***REGULATORY IMPACT*** *The risk of reputational and financial losses due to the inability to comply with or keep abreast of regulatory requirements.*	• Changing regulatory and supervisory requirements are resource intensive and costly. • Public interest, social drivers and consumerism may initiate legislative change, requiring appropriate response strategies.	• Ongoing engagement with government and regulators to support evidence-based policy-making and dialogue between public and private sectors. • Monitoring of international developments, learnings and benchmarks to identify future supervisory focus areas.

EMERGING RISKS	RISK DRIVERS	MITIGANTS
4 ***FRAUD*** *The risk of regulatory sanction and reputational and financial losses due to fraud, crime and misconduct from staff or syndicates.*	• Increasingly advanced cyber and malware attacks are expected, which may result in increased fraud. • Aggressive advancements in technology may cause unforeseeable fraud threats.	• Enhanced digital detection capability covering people, processes and technology. • Development of predictive fraud detection and prevention capabilities using agile methodologies.
5 ***INFORMATION*** *The risk of loss due to inaccurate data, data breaches or being unable to protect client information.*	• Perpetrators and events will continue to evolve. • There may be increased demand for processing of information from data subjects.	• Ongoing awareness encourages a consistent information protection culture. • Ongoing research and threat intelligence to stay abreast of developments and to ensure the protection of information assets.
6 ***PEOPLE*** *The risk of failure of the workforce to adequately and efficiently serve clients, support operations and deliver business strategy.*	• The multi-generational workforce has different needs, expectations and aspirations, increasing complexity in the workplace. • A rise in digitisation and automation will deliver efficiencies and reduce demand for certain skillsets.	• A range of learning and development solutions ensure that employees can adapt and remain relevant in the changing work environment through continuous learning. • Recognition programmes support a culture where success is celebrated and employees feel valued for their contribution to the business.
7 ***BUSINESS DISRUPTION*** *The risk of infrastructure/change failure or environmental impacts disrupting the services to and of the group.*	• Voluminous and/or significant system changes always pose the risk of unforeseen consequences or disruption to clients and business activities. • Reliance on infrastructure such as water and power utilities, and network service providers.	• Continue to improve our system production stability and reliability to minimise disruption of digitally enabled services to our clients. • Business continuity plans are prepared for all business areas. • Simplify our IT landscape to improve agility, enhance customer experience and ensure the relevance of services we offer to our clients.
8 ***THIRD-PARTY*** *The risk of losses or disruptions due to ineffective management of third-party relationships.*	• Emergence of third-party partnerships and outsourcing as business enablers, for example, partnering with fintechs. • The potential for unknown fourth- and fifth-parties supporting third-party providers.	• Predictive profiling of suppliers to drive improved supply chain management. • Increased visibility into fourth- and fifth-parties to ensure accountability and preparedness to avoid potential incidents.
9 ***CONDUCT*** *The risk of harm being caused to the group, its clients and markets due to inappropriate execution of business activities.*	• Cultural misalignment due to inappropriate ethics, behaviours and values being applied that result in poor business practices. • Growth in the complexity of regulatory frameworks.	• By driving a culture of doing the right business the right way, we will continue to embed our desired values, ethics and behaviours. • Continuing to refine our approach to training through the rollout of more interactive and digital methods of training that are standardised across the group. • Working to embed and monitor conduct-related metrics in business units and corporate functions across the group.