Risk management

The operations of the SARB continue to evolve in an economic landscape and financial system that are changing rapidly and becoming more complex.

These changes present both risks and opportunities for the SARB as it executes its price and financial stability mandates.

Operationally, the SARB is exposed to significant inherent risks in many of its core functions. These risks include strategic, policy process and operational risks – such as business continuity, cybersecurity, information security and compliance – as well as reputational, project and financial risks.

The SARB's risk management framework governs the full spectrum of these risks and ensures they are effectively managed within the SARB's risk tolerance levels. The risk management approach includes monitoring and responding appropriately to potential and actual political, economic and regulatory risks arising from the global and domestic environments.

Following the adoption of ISO 31000 as the enterprise risk management framework, the SARB has continued to implement this standard across the various business areas, aligning the Group with global best practice.

Specialised cross-cutting risks

The coordinating role of the RMCD extends to the following cross-cutting risk categories.

Compliance

The RMCD provides a centralised management of compliance, ensuring obligations are met by:

- implementing and maintaining a Compliance Policy and framework;
- identifying, assessing and monitoring compliance in line with regulatory requirements;
- monitoring new regulatory developments;
- enabling compliance with various legislation, including environmental, labour, constitutional and anti-money laundering (AML) legislations;
- promoting a culture of compliance and ethics; and
- reporting compliance risks to the RMC and BREC.

Business continuity

The SARB has adopted the Business Continuity Institute's Good Practice Guidelines that are based on the ISO 22301: Business Continuity Management System (BCMS) standard. The SARB and the cash centres have received formal ISO 22301 BCM certification, which places it on par with international best practice.

The SARB's BCM programme is managed centrally and is supported by a policy, framework, incident management plan and annual cycle of technical activities. The BCM Committee is fully operational.

As the SARB matures and develops its consideration of, and approach to, climate change and cybersecurity risks, the BCM team will continue to support the SARB's Climate Change Programme and liaise closely with the Cyber and Information Security Unit, which is responsible for ensuring governance and the management of the Group's Cyber and Information Security Programme.

Risk management framework

Risk governance

GROUP RISK MANAGEMENT POLICY

Heads of Department and Managing Directors

Responsible for strategic, operational and project risk management

Risk Management and Compliance Department

Facilitates and coordinates integrated risk management in the Group and reports to risk oversight committees

Risk Management Committee

Oversees risk management in the Group on behalf of the SARB executive

Board Risk and Ethics Committee

Reviews the status and effectiveness of risk management in the Group on behalf of the Board

Risk universe

RISK ASSESSMENTS

The risk management framework governs the full spectrum of risk, including strategic, policy process and operational risks (such as business continuity, cybersecurity, information security, compliance, OHS, climate change and CSI) as well as reputational, project and financial risks.

CONTINUOUS RISK MANAGEMENT

This includes risk incident management, monitoring action plan implementation, day-to-day risk management activities, key risk indicators, scenario analysis and the monitoring and assessment of external risks, including those that emanate from climate change.

Combined assurance

The SARB has adopted a combined assurance approach, in line with *King IV*™, to increase the effectiveness of assurance activities within the five lines of assurance. The combined assurance model has matured and has been subjected to ongoing enhancements, alignment of assessment methodologies and integrated dashboard-based reporting across the lines of assurance.

The Group's combined assurance approach to risk management and control aims to integrate, coordinate and align processes and optimise the levels of risk, governance and control oversight.

Combined Assurance Forum

The Combined Assurance Forum (CAF) regularly reviews the combined assurance approach, model and processes as well as information sharing and coordination between the respective assurance providers. This contributes significantly towards an effective control environment and supports the integrity of information used for internal decision-making by management, the Board and its committees. Based on reports submitted by the lines of assurance and the CAF, chaired by the Chief Risk Officer (CRO), the forum considers the adopted combined assurance approach to be adequate, effective and aligned to good practices.

Combined assurance providers aligned with the Combined Assurance Model

First level of assurance providers	**Departmental management**	The managers of each department are responsible for the ongoing identification, assessment and management of risks, including designing, implementing and maintaining an adequate and effective system of control.
Second level of assurance providers	**Integrated risk management**	The RMCD performs a centralised and integrated risk management coordination function to ensure risks are managed consistently, within internationally accepted standards and guidelines.
Third level of assurance providers	**Internal Audit**	The IAD is an independent, objective assurance and advisory function that provides a view on whether processes for managing and controlling risks and overall governance are adequately designed and function effectively. The IAD brings a systematic approach to assessing risk management, control and governance processes, advising management in developing control solutions and monitoring management's corrective actions. The IAD works across the Group, covering all operational functions as well as information technology (IT) systems and processes. The work is carried out in accordance with the Institute of Internal Auditors' (IIA) International Professional Practices Framework.
Fourth level of assurance providers	**Independent external assurance service providers:** external audit and other independent assurance providers	Independent external auditors audit the Group's annual financial statements. Where it is deemed necessary, other external assurance providers are used to obtain independent assurance on the adequacy and effectiveness of the internal processes and practices, ensuring they are aligned to international best practice.
Fifth level of assurance providers	**Board**	The Board oversees that the Combined Assurance Model is implemented to cover significant risks and material matters through a combination of the various assurance services and functions for the Group.

2023/24 | Performance highlights

Received the formal BCM certification against the ISO 22301 BCMS international gold standard. The certification was awarded by the British Standard Institute, validating that the SARB is compliant with the requirements for setting up and managing an effective BCM system.

Completed an independent ethics management maturity assessment and an ethics risk assessment in collaboration with the Ethics Institute.

Looking *ahead*

In line with ongoing objectives, the SARB will continue to advance risk management practices that are forward-looking and support business objectives. The organisation will continue to enhance and expand collaboration and integration with internal and external stakeholders.