Type:	*Policy Summary*
Name:	Information Risk
Keywords	Information risk, information security, information assets, information lifecycle, PCI DSS, Card data, Records management, Mobile device, Information classification, End User Self Developed Applications, Privacy, Personal data, Data Governance, data quality, metadata, master data and reference data.

1 Policy Statement

Standard Bank Group (Group) has issued a formal Information Risk Governance Standard (IRGS) which outlines the Group's high-level policy objectives and commitment to implement good information risk management, information security and data privacy risk management practices.

Information Risk is defined as the risk of accidental or intentional unauthorised use, access, modification, disclosure, dissemination or destruction of information resources, which would compromise the confidentiality, integrity and availability of information and which would potentially harm the business.

Data Privacy Risk is the accidental or intentional compromise and/or unlawful processing of Personally Identifiable Information at any point during its lifecycle, which would potentially cause harm to the business and/or data subject.

Data Privacy Risk is a sub-risk type of Information Risk and is by default included where Information Risk is referred to in this document.

2 Policy Scope

The policy applies to:

- the Group, including all Legal Entities (LEs), Business Units (BUs), and Group Functions (CFs)
- both data (the representation of facts as text, numbers, graphics, images, sound, or video), and information (data in context); and
- information in audible (spoken in conversation), physical and electronic format (including the Group's intellectual property) owned by or entrusted to the Group throughout the information lifecycle, including information in motion, information in use and information at rest.

Policy Owner: Group Head: NFR. Approved by Group Non-Financial Risk Committee. Approval Date: October 2024. Next Review Date: October 2025

3 Purpose of this policy

The policy provides the necessary principles and minimum requirements to manage the risk to all types of information assets and compliance with applicable statutory and regulatory obligations.

Key principles to be adhered to by the Group:

- Principle 1: Information is a valuable asset to the Group and must be protected according to its value, sensitivity, and purpose. This includes information asset identification, ownership, classification, records management, lifecycle management and protection throughout its footprint through established data governance practices to enhance the value of the information assets.
- Principle 2: Data Privacy Risk must be managed proactively and holistically (privacy-by-design) according to legislative requirements. This includes the appointment of Information/ Data Privacy/ Data Protection Officers and the identification and embedment of both legislative and regulative requirements per jurisdiction whilst adhering to the Group's minimum data privacy principles.
- Principle 3: Access to information assets must be managed on a need-to-know and need-to-have basis. This includes logical, physical, and privileged access management and implementation of full accountability for all high-risk profiles and roles.
- Principle 4: Risks to information assets must be assessed and managed in accordance with the established information risk appetite. This includes the implementation of people, process, and technology controls to mitigate information risks within risk appetite.
- Principle 5: All information risk incidents must be reported, escalated, and handled in accordance with Group defined policies related to incident management. This includes the reporting, recording and remediation of all information risk incidents and data privacy breaches in accordance with legislation and regulations where applicable.

4 Roles and Responsibilities

- The Three Lines of Defense model is followed to ensure roles and responsibilities are effectively cascaded in the management of information risk.
- Lines of Business are overall accountable for setting the tone from the top to promote a transparent culture of accountability, where all employees are encouraged and committed to their information risk responsibilities and ensure that Third Parties acknowledge and comply with the minimum requirements set out. This includes ensuring that all information is processed and stored in accordance with compliance requirements and all significant information risks and control weaknesses are managed and reported.
- Non-Financial Risk Managers provide the necessary oversight and guidance to managing the risks to information and implementation of the policy.
- Technology (including IT Security) ensures policy principles are embedded in operations and technology and that technical solutions and infrastructure for internal and external (e.g., cloud) systems and associated security controls enable and give effect to the policy.
- Group Information Risk enables and continuously improves the governance of Information Risk, oversees compliance, provides subject matter guidance, oversight, ongoing assurance and reporting on policy implementation, and ensures awareness and training on information risk is available on Group level.
- Group Data Privacy Officer sets the Group's approach to data privacy by developing, maintaining, monitoring and overseeing the implementation of the Group Data Privacy Operating Standard and providing guidance to Data Privacy Officers in all Group LEs.

- Data Privacy Officers in jurisdictions and LEs support the maintenance of the data privacy regulatory universe for the relevant jurisdiction, identifies compliance obligations and integrates these into existing frameworks, policies, and procedures in alignment with Group Information Risk governance.
- Internal Audit provide an independent assessment of the adequacy and effectiveness of the Information Risk Management control environment.
- Other key stakeholders play a significant role in the holistic approach to Information Risk management, e.g., Procurement, Compliance, Legal, Business Resilience, Third-Party Risk Management and employees.