Type:	Policy Summary
Name:	Information Risk Policy Summary
Keywords	Data Management/ Information Management/ Data Security /Information Security /Cyber Security /Cyber Security Risk/Data Privacy Risk/ Technology Risk

1 Policy Statement

- Standards Bank Group (Group) has issued a formal Information Risk Governance Standard (IRGS) which outlines the Group's highlevel policy objective. SBG is committed to information risk management and information security practices.

- Information Risk is defined as the risk of accidental or intentional unauthorized use, access, modification, disclosure or destruction of information resources, which would compromise the confidentiality, integrity and availability of information and which would potentially harm the business. This policy summary provides the necessary principles and minimum requirements to manage the risk to information assets.

2 Policy Scope

- This policy summary applies to Standard Bank Group, including all Business Units (BUs), Corporate Functions (CFs), Legal Entities (LE), all employees and third parties, including Independent Service Providers.
- This policy summary applies to both data (the representation of facts as text, numbers, graphics, images, sound or video); and information (data in context).
- This policy summary applies to 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.

3 Purpose of this policy

- This policy provides the necessary principles and minimum requirements to manage the risk to information assets. This summary is to govern accidental information exposure or unauthorized use, access, modification, disclosure or destruction of information resources, which would compromise the confidentiality, integrity and availability of information and which would potentially harm the business.
- The summary ensures alignment between the following risk types:
- Cyber security risk, Technology risk and Data Privacy risk

- 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.
- Principle 2: Access to information assets must be managed on a Need-to-know and Need-to-have basis.
- Principle 3: Risks to information assets must be assessed and managed in accordance with the established information risk profile.
- Principle 4: All information risk incidents must be reported, escalated, and handled in accordance with Group defined policies related to incident management.

4 Roles and Responsibilities

- The following roles and responsibilities are applicable to ensure that the Standard is managed, implemented, executed, and complied with:

- The Group Board is accountable for ensuring that prudent and reasonable steps have been taken with respect to fulfilling its responsibilities for Information Risk Governance and Management. This includes the overall responsibility for managing Information Risk.
- The Group Board delegates approval authority for the Standard to the Group Risk and Capital Management Committee (GRCMC), a subcommittee of the Board, which delegates the review and recommendation thereof to the Group Risk Oversight Committee (GROC) and its subcommittee Group Operational Risk Committee (GORC).
- The Group Head Information Risk is the owner of the Standard and responsible for implementation and oversight.
- The Group Information Risk Office (GIRO) maintains the Standard and ensure that it is reviewed at least once every two years for applicability and alignment to the Operational Risk Governance Standard.
- The Group Information Risk Management Steering Committee (IRM SteerCo) provides governance and oversight on all matters relating to Information Risk.
- Operational Risk Integration (ORI) promotes awareness and communication related to this Standard, in line with the defined engagement model and flight plan.
- Embedded Operational Risk Managers are responsible for governance and oversight of the Standard, which includes making Business aware of the content and to ensure that the principles are considered in the Risk Control Self Assessments (RCSA) and business as usual activities.