VACANCY

Postbank Your Bank

JOB TITLE	**:**	**Head: Data Management**
REPORTS TO	**:**	**General Manager: IT Optimisation**
BUSINESS UNIT	**:**	**IT**
LOCATION	**:**	**HEAD OFFFICE: PRETORIA**
POSITION STATUS	**:**	**Permanent**
POSITION GRADE	**:**	**D5**

Purpose of the Job

The Head: Data Management is responsible for leading data management practices that support reliable, secure, governed and compliant information across the bank's technology platforms, operational systems, retail banking data flows and reporting environments. Define and manage data governance, data ownership, data stewardship, data quality, data lineage, metadata, master data, reference data, data access, data lifecycle and operational data control practices to protect customer, account, transaction, payment, card, social grant and business information assets. Direct the management of critical banking data across core banking, payments, switch, card, digital banking, finance, General Ledger, fraud, Anti-Money Laundering, complaints, regulatory reporting and analytics environments to improve traceability from source system to report. Provide evidence of data lineage, access control, data changes, ownership, quality, reconciliation and remediation progress to support audit readiness, regulatory assurance and operational decision making. Coordinate data management activities across technology, operations, finance, risk, compliance, security, analytics and vendor teams to improve data reliability, reconciliation integrity, reporting quality, service continuity and the bank's financial inclusion mandate.

Job Responsibilities

Data Management Strategy and Governance

- Define the data management framework to guide data ownership, data stewardship, data quality, data control and operational data practices across the bank
- Set data standards, data definitions, metadata requirements, naming conventions, reference data standards and control procedures to support accountable management of information assets
- Establish data governance forums and reporting routines to review data risks, quality issues, remediation progress and control effectiveness
- Define critical data elements for customer, account, balance, transaction, General Ledger, payment, card, switch, channel, Know Your Customer, sanctions, complaints, regulatory and reporting data to strengthen data accountability
- Report material data risks, unresolved quality issues and control gaps to management forums to support informed decision making
- Maintain an inventory of critical data elements and priority data flows across core banking, digital banking, payments, switch, cards, General Ledger (GL), reconciliation, fraud, Anti Money Laundering (AML), regulatory reporting and analytics platforms

Banking Data Quality and Integrity Management

- Lead data quality management across core banking, payment, switch, card, digital channel, finance, reconciliation, reporting and analytics environments to improve information reliability
- Monitor data completeness, accuracy, timeliness, validity and consistency to identify defects that affect service delivery, reconciliation, regulatory reporting or decision making
- Coordinate data quality remediation with technology, operations, finance, business, analytics and vendor stakeholders to resolve root causes
- Track duplicate, missing, inconsistent, stale, orphaned or unreconciled data to drive permanent corrective action
- Maintain data quality dashboards, exception reports and remediation records to support audit and assurance reviews

Reconciliation Data and Operational Control

- Coordinate data reconciliation, validation and control checks to confirm integrity across critical banking processes

- Support reliable reconciliation between customer records, account records, sub ledgers, General Ledger records, transaction stores, switch records, payment files, settlement files, finance records and reporting outputs
- Monitor data breaks, unmatched items, missing transactions, unusual postings, suspense trends and operational anomalies to identify service and control risks
- Support data related incident, problem and change processes to protect production stability and transaction integrity
- Protect payment services by maintaining effective data controls over relevant operational and payment information

Data Architecture Integration and Platform Support

- Coordinate data architecture and lineage practices with enterprise architecture, solution architecture, operations, analytics and platform teams to improve transparency of data flows
- Maintain data ownership records, data definitions, data lineage, metadata, master data and reference data to support traceability and accountability
- Support resilient and auditable data pipelines across core banking, payment, switch, card, channel, reporting and analytics environments
- Provide data management input into Integrated Banking Management System (IBMS), digital banking, data warehouse, data lakehouse, metadata catalogue, master data, reporting and analytics platform modernisation
- Review data integration, application programming interface, streaming, batch, extraction and transformation practices to identify risks in data movement, quality and reporting reliability

Data Protection Regulatory and Audit Compliance

- Apply data protection, retention, privacy and security requirements to data management activities to support responsible information use
- Support Financial Intelligence Centre Act (FICA), Financial Intelligence Centre (FIC), South African Reserve Bank (SARB), Prudential Authority, National Payment System (NPS), Protection of Personal Information Act (POPIA), Anti Money Laundering (AML), audit and forensic evidence requirements through controlled extracts, lineage and retained proof
- Maintain data control evidence, data access records, data handling records and governance decisions to support internal audit, external audit and regulatory review
- Identify data access, data extraction, data movement and data handling risks to support timely remediation
- Coordinate data related responses to audit findings, regulatory observations and assurance requests

Retail Banking Analytics and Decision Support

- Enable trusted reporting for customer growth, account activity, deposits, balances, payment volumes, channel usage, fraud trends, failed transactions, reversals, complaints, operational incidents and financial performance
- Partner with business and analytics teams to deliver dashboards, data marts and insights that support retail banking performance and service improvement
- Improve customer view, segmentation, campaign, financial inclusion, product usage and service quality analytics through controlled and approved data sources
- Review analytics outputs to confirm that reporting is based on reconciled, traceable and approved data sources
- Support data driven decision making by improving the reliability, usability and business relevance of operational and customer data

Information Access Lifecycle and Security Control

- Define data lifecycle controls for creation, use, storage, retention, archiving and disposal of information assets to reduce data risk
- Review data access and usage practices to support appropriate handling of customer, account, payment, card and operational information
- Coordinate controls over privileged data access, data extraction, masking, encryption and secure disposal to reduce exposure risk
- Support the use of authorised or masked data in development, testing and reporting environments where applicable
- Maintain data continuity and recovery requirements to support access to critical information during disruptions
- Prevent uncontrolled extraction of customer, account, transaction, card, Know Your Customer (KYC), Personal Identification Number (PIN) adjacent or sensitive banking data and confirm that testing and reporting environments use masked or approved data where required

Data Operating Model and Service Management

- Define the data management operating model to clarify data ownership, stewardship, issue management, service levels and escalation routines
- Maintain a data issue register with accountable owners, closure dates, risk ratings and executive escalation for unresolved high-risk data issues
- Establish data management service levels, issue resolution routines, control dashboards and executive reporting to improve delivery discipline
- Support operational resilience of data pipelines, batch processing, beginning of day feeds, end of day feeds, failure recovery and production support routines
- Drive skills transfer, documentation and reduced dependence on individual key persons or vendors to strengthen continuity

Stakeholder Vendor and Service Coordination

- Engage business, technology, finance, operations, risk, compliance, security, analytics and audit stakeholders to clarify data management priorities and issues
- Coordinate vendor inputs where external service providers support data platforms, data processing, reporting or data remediation activities
- Provide specialist data management input into projects, system changes, service improvements and operational reviews
- Communicate data risks, control gaps and remediation progress clearly to support transparent stakeholder management
- Build effective working relationships across teams to improve accountability for data outcomes

Financial Management

- Compile data management budget inputs and forecasts to support planned service delivery, data control and remediation requirements
- Monitor data management expenditure against approved budgets to manage costs within allocated financial parameters
- Review vendor cost drivers, support demand, data platform usage and remediation effort to identify optimisation opportunities
- Track benefits from data management improvements to demonstrate improved reliability, reduced incidents and stronger control

People Management

- Clarify role expectations, priorities and standards for direct reports to align delivery with data management objectives
- Lead performance planning, review and feedback processes to support accountability and delivery
- Coach and mentor direct reports to build capability in data management
- Allocate work, manage capacity and monitor delivery timeframes to maintain effective functional performance and ensure the correct shift coverage
- Support recruitment, onboarding, development and succession planning to maintain a capable and sustainable data management team
- Address conduct, performance and attendance matters in line with Human Resources policies and labour legislation

Qualifications and Experience

- Bachelor's Degree in Computer Science, Information Systems, Data Management, Data Science, Statistics,Commerce, Finance Systems or related discipline (NQF Level 7)
- Certificate in Data Management, Data Governance, Data Quality, Database Management, Data Protection or Information Technology Service Management (NQF Level 6)
- Leadership Development Programme
- 10 Years Experience in the Information Technology industry
- 8 Years Experience in data management, data governance, data quality, database management or data operations

- 5 Years Experience in banking technology, payments, customer data, account data, transaction data or regulated financial services data environments
- 5 Years Experience in data control, data risk, data protection, audit support or regulatory compliance environments

Ideal

- Post Graduate Degree in Computer Science, Information Systems, Data Management, Data Science, Statistics, Commerce, Finance Systems or related discipline (NQF Level 8)
- Advanced Certificate in Data Governance, Data Architecture, Data Engineering, Data Protection, Data Analytics or Information Technology Governance (NQF Level 6)
- Advanced Certificate in Banking Risk, Regulatory Reporting, Data Privacy, Information Security or Audit Management (NQF Level 6)

Advantageous

- 5 Years Experience in core banking data, payment data, card data, social grant data, reconciliation data,data platforms or operational reporting environments
- 3 Years Experience in vendor management, service management, data remediation, data lineage, data platform modernisation or information risk environments
- 3 Years Experience in Know Your Customer data, Anti Money Laundering data, fraud data, complaints data, General Ledger data, switch data or regulatory reporting data

Special requirements

May be required to provide specialist support for critical data incidents, regulatory reviews, audit requests, major system changes, data remediation activities, production incidents, disaster recovery tests, batch failures, data pipeline failures or urgent service restoration events

How to Apply

If you wish to apply and meet the requirements, please forward your Curriculum Vitae (CV) to recruitmentNM@postbank.co.za Please indicate in the subject line the position you are applying for. To view the full position specification, log on to www.postbank.co.za and click on Careers.

Closing Date

11 November 2026

Disclaimers

The South African Postbank SOC Limited is committed to the achievement and maintenance of diversity and equity in employment, especially with regard to race, gender and disability. In compliance with the banks employment equity plans, first preference will be given to candidates from designated groups. Correspondence will be limited to short listed candidates only.

If you do not hear from the South African Postbank SOC Limited or its Agent within 3 months of this advertisement, please accept that your application has been unsuccessful. The South African Postbank SOC Limited reserves the right not to fill the positions or to re-advertise the positions at any time.

POPIA provides that everyone has the right to privacy and it includes a right to protection against the unlawful collection, retention, dissemination and use of personal information. By applying for employment you consent to the processing of your personal information with Postbank. Your personal information and any attached text or documentation are retained by Postbank for a period in accordance with relevant data legislation.