VACANCY

Postbank Your Bank

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

Purpose of the Job

The Head: IT Operations is responsible for leading production technology operations across infrastructure, integration services, database platforms, cloud services, core banking dependencies, payment services, switching services, channel technology, batch processing and operational technology environments. Direct technology operations teams to maintain availability, performance, capacity, monitoring, recovery, continuity, service management and operational control for services that affect customer access to accounts, balances, payments, cards, withdrawals, deposits, grant payments, digital channels and branch services. Manage operational readiness, production support, vendor accountability, privileged access control, major incident command, disaster recovery and audit evidence to protect transaction integrity, customer data and service continuity. Protect savings services and South African Social Security Agency payment services by strengthening operational resilience, security compliance, recovery capability and evidence-based service control.

Job Responsibilities

Technology Operations Leadership

- Lead infrastructure, integration, database, cloud and production technology operations to maintain stable, secure and responsive technology services
- Set operational priorities, standards and escalation procedures to support agreed availability, performance and recovery targets
- Monitor operational performance, service trends, transaction impact and customer impact to identify root causes and reduce repeat failures
- Coordinate restoration of critical technology services to minimise disruption to customers, employees, partners and operations
- Protect payment services by maintaining effective operational support for critical technology platforms

Production Stability and Availability

- Direct production support activities to maintain availability of critical banking platforms and customer facing technology services
- Monitor core banking availability, channel availability, payment service availability, infrastructure stability and major incident frequency to identify service risks
- Coordinate proactive monitoring of transactions, interfaces, batch services, infrastructure and customer impacting services to improve early detection
- Review service desk queues, support queues and escalation routines to confirm that they support high volume retail banking operations
- Maintain operational readiness for new or changed banking platforms to support safe transition into production

Core Platform and Transaction Integrity Operations

- Direct production technology support for core platform dependencies, transaction processing, batch services, interface monitoring, operational control, core banking production support, customer and account servicing, General Ledger (GL) related interfaces, End of Day (EOD), Beginning of Day (BOD), postings, interest, fees, reversals and reconciliation dependencies
- Monitor transaction flows, failed interfaces, delayed processing, settlement dependencies and reconciliation impacts to identify service risks
- Coordinate technology response where incidents affect balances, postings, payments, reversals, statements, files or settlement processes

- Apply strict operational controls over production scripts, data fixes, privileged actions and emergency changes to protect transaction integrity
- Treat incidents affecting balances, missing transactions, failed payments, reconciliation breaks and audit gaps as high-priority banking integrity matters

Payments Switching and Channel Operations

- Direct operational support for payment services, switching interfaces, card platforms, automated teller machine services, point of sale services, digital channels and file exchanges
- Monitor clearing, settlement, payment files, authorisations, reversals, exceptions and partner interfaces to identify service and control risks
- Coordinate escalation paths with payment partners, processors, card service providers, network providers and service integrators to support timely restoration
- Support operational readiness for payment, card, digital channel and partner channel changes to protect production stability
- Maintain operational evidence for payment and channel incidents to support audit, regulatory and management review

Infrastructure Cloud and Platform Operations

- Direct infrastructure operations across hosting, networks, servers, storage, workplace technologies, cloud services and related platform environments to maintain service reliability
- Oversee capacity, availability, patching, backup, performance, job scheduling and monitoring activities to support resilient technology operations
- Manage infrastructure and cloud incidents, operational risks and service constraints to protect production stability
- Review ageing technology, cloud utilisation, platform performance and operational dependencies to identify modernisation priorities
- Support infrastructure and cloud changes, upgrades and service transitions to improve operational efficiency and service continuity

Integration Database and Information Platforms Operations

- Lead integration services operations across middleware, interfaces, application programming interfaces, managed file transfer and data exchange platforms to maintain reliable system connectivity
- Direct database operations to maintain secure, available and high performing data services across critical platforms
- Monitor integration performance, database performance, transaction flows and interface exceptions to identify failures and service risks
- Coordinate resolution of integration and database incidents with applications, infrastructure, vendors and business teams to restore end to end service
- Maintain integration and database operating standards, support procedures and service documentation to support controlled operations

Incident Problem Change and Service Management

- Lead major incident command and service restoration activities for critical technology failures to reduce customer, financial and regulatory impact
- Coordinate root cause analysis and permanent corrective actions for recurring infrastructure, integration, database, cloud, payment and channel issues
- Manage operational input into incident, problem, change, release, service request, availability, capacity, configuration management processes, and service-level management disciplines
- Review change impact, operational readiness, evidence requirements and rollback plans before implementation of high risk technology changes
- Chair or participate in major incident reviews, root cause sessions and operational service reviews to improve service discipline

Resilience Continuity and Recovery Management

- Support disaster recovery, continuity planning, failover testing, backup restoration and service recovery exercises for critical technology services
- Confirm that recovery time expectations, recovery point expectations and recovery evidence are understood, tested and maintained for critical banking systems
- Drive resilience improvements across cloud, data centre, network, application, database, integration and third party dependencies
- Maintain runbooks, recovery documentation, incident records, change records and lessons learned to support audit and assurance reviews
- Report recovery gaps, resilience risks and unresolved service continuity issues to governance forums to support informed decision making
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) achievement, backup restore success, failover testing, runbook currency and evidence of recovery testing for critical banking systems

Operational Risk Compliance and Access Control

- Apply information technology service controls, security requirements and compliance obligations to technology operations processes
- Strengthen controls over privileged access, service accounts, audit logs, production data, script execution and change approval to reduce operational risk
- Support compliance with Payment Card Industry Data Security Standard, Protection of Personal Information Act and applicable payment requirements through controlled operational practices
- Identify operational, security, vendor and compliance risks in technology operations to drive timely remediation
- Maintain operational evidence, access review records, control records and audit remediation evidence to support regulatory and assurance review
- Information Technology General Controls (ITGC) evidence, access reviews, privileged access controls, service account controls, audit log completeness, unauthorised change prevention and vulnerability remediation tracking

Vendor Partner and Stakeholder Governance

- Manage vendor and service provider performance to confirm delivery against agreed support, escalation and service restoration commitments
- Challenge vendor performance where recurring incidents, poor response or weak root cause analysis affects banking operations
- Maintain support obligations, escalation contacts, service evidence packs and operational review records to support vendor accountability
- Engage business operations, payments, cards, digital channels, risk, compliance, audit, cyber security, data protection, project delivery and technology teams to resolve operational dependencies
- Escalate vendor or internal support failures where service risk requires senior intervention

Operational Acceptance and Production Readiness

- Define operational readiness gates and minimum evidence requirements before new systems, major changes or service transitions move into production
- Review support models, monitoring arrangements, runbooks, access controls, escalation paths and recovery requirements before operational acceptance
- Recommend suspension, rollback, deferral or rejection of production changes or go-lives where readiness, control or service risk is unacceptable
- Require root cause analysis, permanent corrective action and control remediation for recurring service issues
- Support project teams with production readiness input to protect stable transition into live operations

Financial Management

- Compile technology operations budget inputs and forecasts to support planned infrastructure, database, cloud and integration service requirements

- Monitor technology operations expenditure against approved budgets to manage costs within allocated financial parameters
- Review vendor cost drivers, platform utilisation, support demand and recovery requirements to identify optimisation opportunities
- Track benefits from operational improvements to demonstrate improved reliability, reduced incidents and better value from technology spend

People Management

- Clarify role expectations, priorities and standards for direct reports to align delivery with technology operations objectives
- Lead performance planning, review and feedback processes to support accountability and delivery
- Coach and mentor direct reports to build capability in infrastructure, integration services, database operations, cloud infrastructure and operational resilience
- Allocate work, manage capacity and monitor delivery timeframes to maintain effective technology operations performance
- Support recruitment, onboarding, development and succession planning to maintain a capable and sustainable operations 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, Computer Engineering, Network Engineering or related discipline (NQF Level 7)
- Certificate in Information Technology Service Management, Infrastructure Management, Cloud Infrastructure, Information Technology Operations or Business Continuity Management (NQF Level 6)
- Leadership Development Programme
- 12 Years Experience in the Information Technology industry
- 10 Years Experience in infrastructure operations, systems operations, cloud operations, database operations, applications operations or integration services
- 5 Years Experience in banking technology, payments, digital channels, core platforms, card services or customer facing technology environments
- 5 Years Experience in leading technology operations teams, vendors, service restoration, major incidents and operational governance

Ideal

- Post Graduate Degree in Computer Science, Information Systems, Computer Engineering, Network Engineering, Technology Management, Risk Management, Governance or related discipline (NQF Level 8)
- Advanced Certificate in Information Technology Service Management, Cloud Architecture, Infrastructure Management, Information Technology Governance, Disaster Recovery Management or Business Continuity Management (NQF Level 6)
- Advanced Certificate in Payment Operations, Change Management, Release Management, Cyber Resilience or Financial Services Risk Management (NQF Level 6)

Advantageous

- 3 Years Experience in cloud infrastructure, database platforms, middleware, application programming interfaces, networks, data centre operations, Job scheduling or monitoring tools
- 3 Years Experience in regulated financial services operations, information technology risk, audit, disaster recovery, operational resilience or compliance environments
- 3 Years Experience in core banking production support, payment systems, switching, card systems, batch processing, interfaces or operational readiness environments

Special Requirements

May be required to provide standby or incident support for critical technology failures, payment incidents, card incidents, major infrastructure changes, integration failures, cloud service issues, database failures, batch failures, disaster recovery tests, audit requests, major incident command 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.