



NATIONAL SAVINGS AND CREDIT BANK

JOB OPPORTUNITY

In line with its Strategic ambition to strengthen Digital Banking, Operational resilience, Cybersecurity maturity, and Technology governance within a regulated financial services environment, National Savings and Credit Bank invites applications from suitably qualified, visionary, and high-calibre professionals to fill the following executive position:

Chief Information and Technology Officer (CITO) – NG2

Reporting to: Chief Executive Officer

Location: Head Office, Lusaka

1. Strategic Context of the Role

National Savings and Credit Bank operates within a highly regulated banking environment where technology underpins financial stability, customer trust, and regulatory compliance.

The Chief Information and Technology Officer (CITO) will serve as a key member of Executive Management, providing strategic leadership over the Bank's technology ecosystem, ensuring resilience of mission-critical banking systems, safeguarding information assets, and advancing digital innovation in alignment with prudential guidelines and industry best practice.

The role carries accountability for Enterprise Technology Strategy, Cybersecurity governance, Core banking platforms, Digital banking channels, IT risk management, Regulatory compliance, and Operational IT Business Continuity across the Bank.

2. Purpose of the Role

The CITO is responsible for providing executive oversight and strategic direction of the Bank's information technology function to ensure:

- Secure, reliable, and resilient core banking and payment systems
- Robust cybersecurity and information security governance
- Alignment of ICT strategy with corporate strategy and regulatory requirements
- Effective IT risk management integrated within the Bank's enterprise risk framework.
- Continuous digital transformation to enhance customer experience and operational efficiency.
- Compliance with banking regulatory standards, data protection laws, and industry frameworks

3. Key Accountabilities

A. Technology Strategy & Enterprise Architecture

- Develop and implement the Bank's ICT and Digital Transformation Strategy aligned to the Corporate Strategic Plan.

- Lead enterprise architecture governance to ensure scalable, secure, and future-ready technology platforms.
- Establish multi-year technology roadmaps supporting growth, innovation, and regulatory alignment.
- Provide strategic advisory support to Executive Management and the Board on technology investments and risk posture.

B. Core Banking & Digital Platforms

- Provide executive oversight of the Bank's core banking system, ensuring high availability, integrity, and performance.
- Oversee digital banking channels including mobile banking, internet banking, ATM, and card systems.
- Ensure technology platforms support efficient product development, financial reporting, and customer service delivery.
- Monitor system performance against defined Service Level Agreements (SLAs) and operational targets.

C. Cybersecurity & Technology Risk Governance

- Lead the design and implementation of a comprehensive cybersecurity governance framework.
- Oversee information security operations, incident response, and cyber resilience programmes.
- Ensure integration of ICT risk management within the Bank's Enterprise Risk Management (ERM) framework.
- Provide regular reporting to Executive Management and the Board Risk Committee on technology risks and mitigation measures.
- Ensure effective management of fraud-related technology controls and data protection mechanisms.

D. Regulatory Compliance & Audit Oversight

- Ensure full compliance with applicable banking regulations, prudential guidelines, ICT supervisory frameworks, and data protection legislation.
- Lead ICT engagements with regulators, internal auditors, and external auditors.
- Ensure integrity and reliability of systems supporting regulatory and financial reporting.
- Maintain documented ICT policies, procedures, and governance frameworks aligned to international best practices.

E. Operational Resilience & Business Continuity

- Oversee Business Continuity Management (BCM) and Disaster Recovery (DR) frameworks for all critical banking systems.
- Ensure regular testing of disaster recovery capabilities and system failover readiness.
- Safeguard data resilience and backup integrity in line with regulatory expectations.
- Maintain high system uptime and operational continuity across the Bank's branch and digital network.

F. Vendor & Third-Party Technology Risk Management

- Oversee ICT vendor selection, contract negotiation, and SLA management.

- Ensure effective third-party risk management controls for outsourced technology services.
- Monitor vendor performance and compliance with contractual and regulatory obligations.

G. ICT Financial & People Management

- Develop and manage the ICT budget aligned to strategic priorities.
- Drive cost optimisation while maintaining technology quality and security standards.
- Build, mentor, and retain a high-performing ICT team.
- Foster a culture of innovation, accountability, and continuous professional development.

4. Qualifications & Experience

- Full grade twelve (12) certificate
- Bachelor's degree in Information Technology, Computer Science, Information Systems, or related field (required).
- Master's degree in Information Technology, Business Administration (MBA), or related discipline (preferred).
- Minimum of Ten (10) years' progressive ICT experience, with at least five (5) years at senior management level within a regulated financial institution.
- Must be a member of the Information and Communication Technology Association of Zambia (ICTAZ) with a valid practicing license.
- Demonstrated experience overseeing core banking systems and digital banking platforms.
- Proven track record in cybersecurity governance, IT risk management, and regulatory compliance.
- Experience managing large-scale ICT environments supporting multi-branch banking operations.
- Experience leading technology transformation initiatives and enterprise system implementations.

5. Professional Certifications (Preferred)

- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- COBIT Certification
- ITIL Certification
- ISO/IEC 27001 Lead Implementer or Lead Auditor

6. Required Competencies

- Strategic and innovative leadership capability
- Strong understanding of banking technology risk frameworks
- Proven board-level reporting and stakeholder engagement skills
- Crisis management and decision-making capability
- Strong analytical and problem solving skills.
- High ethical standards and integrity
- Ability to operate effectively within a highly regulated and performance-driven environment.

7. Application Process

If you meet the above requirements and are ready to lead technology transformation within a dynamic banking environment, kindly submit your application letter, detailed Curriculum Vitae, certified copies of academic and professional qualifications, and valid practicing certificate to:

Chief People & Culture Officer

National Savings and Credit Bank
P.O. Box 30067
LUSAKA

Or e-mail your application to:

jobs@ictaz.org.zm

Closing Date: 24th February 2026