VACANCY

JOB TITLE : **SENIOR AUDIT MANAGER: IT AUDITS**

BUSINESS UNIT : **INTERNAL AUDIT**

LOCATION : **HEAD OFFICE_PRETORIA**

POSITION STATUS : **FIXED TERM CONTRACT (6 MONTHS)**

Purpose Statement

To lead and manage the Information Technology (IT) Audit function within Postbank by providing independent, objective assurance and advisory services over the organisation's technology environment, digital banking ecosystem, operational technology processes, cybersecurity framework and IT governance structures.

The Senior Audit Manager: IT Audits is responsible for developing and executing a risk-based IT audit strategy and annual audit plan that provides assurance on the adequacy and effectiveness of IT governance, risk management, cybersecurity, digital transformation initiatives, operational systems and internal controls across Postbank.

The role supports the Chief Audit Executive in strengthening governance, operational resilience, regulatory compliance, information security and technology risk management in alignment with Postbank's mandate of delivering accessible, secure, transparent, and customer-centric financial services to South Africans.

The role provides strategic oversight across IT General Controls (ITGC), Application Control Reviews (ACR), Computer Assisted Audit Techniques (CAATS), Cybersecurity and Security Reviews, Project Management and Programme Assurance, Digital and Self-Service Channels, Payments and Interbank Systems, PMO and Operational Technology Audits, IT Governance and Infrastructure Audits.

Job Responsibilities

IT Audit Strategy and Leadership

- Develop and implement the IT Audit strategy and operational plans.
- Lead the delivery of the annual risk-based IT Audit Plan.
- Provide strategic assurance over technology and digital risks.
- Support the CAE in strengthening governance and control maturity.
- Develop and maintain a risk-based IT audit universe and audit strategy aligned to Postbank's strategic objectives and risk profile.
- Lead the development and execution of the annual IT audit plan.
- Identify emerging technology, cybersecurity, operational and digital banking risks.
- Ensure alignment between IT audit activities and enterprise risk management objectives.
- Provide strategic insight into Technology governance, Digital transformation risks, Cybersecurity maturity, Operational resilience, Data governance, Systems reliability
- Advise the CAE and leadership on technology risk exposures and control effectiveness.
- Ensure IT Audit coverage remains responsive to Banking sector developments, Cybersecurity threats, Regulatory changes, Digital banking innovation, Operational risks
- Lead continuous improvement initiatives within the IT Audit function.
- Support Internal Audit quality assurance and improvement programmes.

IT Audit Execution and Assurance

- Oversee and ensure the delivery of high-quality IT audit engagements.
- Provide assurance over technology governance, systems, infrastructure, applications and operational controls.
- Ensure audit conclusions are risk-based, practical, and value-adding.
- Oversee and review audits relating to IT General Controls (ITGC), Application Control Reviews (ACR),

Cybersecurity and Security Reviews, CAATS and Data Analytics, Infrastructure and Network Audits, Cloud and Digital Platform Audits, Payments and Interbank Systems, PMO and Project Assurance Reviews, Self-Service and Digital Channel Audits, Business Continuity and Disaster Recovery

- Review audit scopes, testing approaches, findings and reports.
- Ensure that appropriate audit methodologies and standards are applied.
- Evaluate the effectiveness of IT governance frameworks, Information security controls, Change management processes, Access management controls, Systems development lifecycle (SDLC) controls, IT operations controls, Data integrity and interface controls, Incident and problem management processes
- Ensure that audit findings are supported by sufficient and appropriate evidence.
- Review and approve audit reports prior to submission to the CAE and governance structures.
- Monitor the implementation of agreed management actions and remediation plans.
- Escalate significant technology and cybersecurity risks appropriately

Cybersecurity and Information Security Oversight

- Provide strategic assurance over cybersecurity and information security risks.
- Support the strengthening of cyber resilience and information protection controls.
- Oversee security reviews and cybersecurity audits across the organisation.
- Assess cybersecurity governance, policies, and operational controls.
- Evaluate: Identity and access management, Privileged access controls, Vulnerability management, Patch management, Security monitoring, Incident response processes, Third-party cybersecurity risk management, Cloud security controls
- Monitor emerging cyber threats and regulatory expectations.
- Assess the adequacy of controls protecting customer and financial information.
- Provide insight into cybersecurity maturity and resilience capabilities.
- Support assurance over digital banking and self-service channel security.

Project Management and Programme Assurance

- Provide assurance over strategic technology projects and programmes.
- Assess project governance, risk management and implementation controls.
- Oversee project and programme assurance reviews for strategic initiatives.
- Evaluate governance structures and oversight mechanisms within projects.
- Assess Project risk management, Budget and resource controls, Delivery timelines, Change readiness, Systems implementation controls, User acceptance testing (UAT), Data migration and deployment controls
- Provide assurance over PMO governance and project delivery effectiveness.
- Identify risks that may impact operational stability, compliance, customer experience or strategic objectives.

Stakeholder and Governance Management

- Build effective relationships with senior stakeholders.
- Support governance committees and executive management.
- Promote trust, transparency and collaboration.
- Engage with executive management, technology leadership, risk functions and governance committees.
- Present audit outcomes, emerging risks and control concerns to management and relevant committees.
- Provide advisory support on IT governance, Cybersecurity, Digital transformation risks, Technology controls
- Promote the awareness of audit, governance and cybersecurity best practices.
- Build collaborative relationships while maintaining audit independence.
- Ensure that stakeholder expectations are managed effectively.
- Support the CAE with Board and Audit Committee reporting where required.

People Management and Leadership

- Lead and develop a high-performing IT Audit team.
- Promote a culture of accountability, innovation and continuous learning.
- Manage the performance and development of IT Audit Managers.
- Provide coaching, mentoring and technical guidance.
- Allocate resources effectively across audit engagements.
- Ensure that team capability aligns with evolving technology and cybersecurity risks.
- Support succession planning and talent development initiatives.
- Foster collaboration, inclusion and employee engagement.
- Promote ethical conduct, professionalism and accountability.

Quality Assurance, Compliance and Professional Standards

- Ensure compliance with professional standards and methodologies.
- Maintain high-quality audit practices and governance.
- Ensure compliance with IIA Standards, ISACA Standards, Internal Audit Methodologies, Regulatory requirements
- Maintain quality assurance processes and review mechanisms.
- Ensure complete and accurate audit documentation.
- Promote consistency in audit execution and reporting.
- Maintain confidentiality, independence and professional ethics.
- Monitor adherence to agreed audit timelines and quality standards.

Innovation and Continuous Improvement

- Drive innovation and operational improvement within IT Audit.
- Promote technology-enabled auditing practices.
- Drive the adoption of CAATS, Data analytics, Continuous auditing techniques, Automation tools
- Identify opportunities to improve audit efficiency and effectiveness.
- Monitor global trends in Cybersecurity, Artificial Intelligence (AI), Cloud computing, Digital banking, Emerging technologies
- Promote a culture of innovation and continuous improvement.
- Participate in industry forums and professional development initiatives.

Role Requirements:

Qualifications:

- An NQF Level 8 qualification in Information Technology / Information Systems / Computer Science / Internal Auditing / Accounting / Risk Management / Commerce or related field
- Certified Information Systems Auditor (CISA)

Ideal

- Masters' in Business Administration (MBA)
- Certified Internal Auditor (CIA) / Certified Information Security Manager (CISM) / Certified in Risk and Information / Systems Control (CRISC) / Certified Ethical Hacker (CEH) / COBIT Certification / ISO 27001 Lead Auditor / Project Management Certification (PMP/Prince2) will be preferred

Experience and Knowledge of:

- 8-10 years' experience in IT auditing, information systems auditing, cybersecurity auditing or technology risk management
- 3-5 years management experience within Internal Audit or IT Risk environments
- Experience conducting and overseeing ITGC audits, ACR reviews, cybersecurity audits, CAATS and data analytics reviews, project and programme assurance reviews, digital banking and payments audits
- Experience within banking, financial services, public sector, or regulated industries

- Experience engaging with executive management and governance committees
- Knowledge of IT General Controls (ITGC), Application Control Reviews (ACR), Cybersecurity governance and controls, Information systems auditing. Banking systems and digital banking platforms
- Knowledge of Payments and interbank systems, COBIT framework, ISO 27001 standards, IT governance and technology risk management, Cloud computing and cloud security, Data analytics and CAATS
- Project management and PMO assurance, Business continuity and disaster recovery
- Information security management, Systems development lifecycle (SDLC)
- Infrastructure and network controls, Regulatory frameworks applicable to banking and financial services
- Internal auditing standards and methodologies, PFMA and King IV / V governance principles

Advantageous

- Experience within a banking institution or state-owned entity
- Exposure to cloud computing, digital transformation, and AI-related risks
- Experience leading high-performing audit teams
- Experience implementing continuous auditing or automated audit solutions

Skills and Attributes

Strategic leadership and management, IT audit planning and execution, Cybersecurity risk assessment, Analytical and critical thinking, Stakeholder engagement and influencing, Decision-making and problem-solving, Report writing and presentation skills, Project and programme assurance, Team leadership and coaching, Communication and interpersonal skills, Risk assessment and governance review, Negotiation and conflict resolution, Planning and organising, Data analysis and interpretation, Adaptability and resilience

How to Apply

If you wish to apply and meet the requirements, please forward your Curriculum Vitae (CV) to RecruitmentJM@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

19 June 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 bank's employment equity plans, we encourage and welcome applications from diverse groups from the South African Employee active population. 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.