MANAGER IT RISK

REPORTING TO: CHIEF RISK OFFICER

Job Purpose:

The Manager ICT risk is responsible for establishing, implementing, and maintaining the Bank's ICT Risk Management Framework in compliance with the Central Bank of Kenya (CBK) Guidelines and global standards which include ISO 27001, NIST CSF, COBIT, Basel Accords and other best practices.

This role provides oversight of ICT risk, cybersecurity, vendor/third-party risk, and operational resilience. It ensures effective risk governance, regulatory compliance, and supports the Bank's digital transformation agenda while safeguarding customer data, systems, and reputation.

The Manager ICT risk closely with ICT, Cybersecurity, Operations, Internal Audit, ExCo, and the Board Risk Committee to ensure technology risk exposures are identified, mitigated, monitored, and reported effectively

Key Responsibilities:

1. ICT Risk Framework & Governance

- Develop, implement, and maintain the ICT Risk Management Framework aligned to CBK/PG/08, Prudential Guidelines, and ISO/NIST/COBIT standards.
- Review ICT policies, procedures, and controls across the Bank.
- Define and monitor ICT risk appetite, Key Risk Indicators (KRIs), and emerging risks, reporting to ExCo and the Board Risk Committee.
- Prepare and present ICT risk dashboards, incident reports, and governance updates to ICT Steering Committee, Service Council, Risk Champions, and Board Risk Commitee.
- Drive ICT risk awareness and training to embed a risk-aware culture across the Bank.
- Align the IT Risk Framework with the Banks overall strategy.

2. ICT Risk Identification, Assessment & Mitigation

- Ensure ICT risk assessments are conducted, Risk Control Self-Assessments (RCSAs), and control testing for systems, infrastructure, and digital platforms.
- Ensure identification of risks across core banking, mobile/internet banking, agency, card systems, fintech integrations, and cloud solutions.
- Ensure update the ICT risk register, dashboards, and heat maps.
- Work with ICT Security to review cyber threats, vulnerabilities, and incident responses.
- Track closure of ICT risk issues, regulatory findings, and internal/external audit recommendations.
- Provide assurance on IT resource adequacy, capacity, and allocation, ensuring resourcing decisions do not expose the Bank to operational or compliance risks

3. Technology Projects & Change Risk Advisory

- Provide ICT risk advisory for new products, core banking upgrades, and new systems implementation.
- Support the Change Advisory Board (CAB) by reviewing risks in major system changes.

4. Cybersecurity & ICT Oversight

- Oversee penetration test and vulnerability assessment results, ensuring timely remediation.
- Monitor privileged access controls and cyber incident logs for risk exposures.
- Ensure compliance with PCI DSS, ISO 27001, and CBK directives.
- Safeguard confidentiality, integrity, and availability of data in compliance with the Data Protection Act 2019**.**

5. Business Continuity & Resilience (BCP & BIA)

- Lead Business Impact Analysis (BIA) to identify critical ICT systems, processes, and dependencies.
- Drive regular Business Continuity (BCP) and Disaster Recovery (DR) testing**,** scenario simulations, and ensure results are documented, tracked, and reported to CBK, ExCo, and the Board Risk Committee.
- Monitor resilience gaps and ensure corrective actions are closed.

6. Vendor & Third-Party Risk Management

- Conduct risk assessments for outsourced ICT services, fintech partners, and third-party service providers.
- Ensure vendor contracts and SLAs include regulatory, ICT security, and resilience obligations.
- Monitor vendor performance and escalate significant risks to management.

7. Fraud Risk & Revenue Assurance Oversight

- Review fraud-related ICT incidents, ensuring root cause analysis and closure of control gaps.
- Evaluate **revenue assurance risks** such as failed billing, duplicate reversals, or leakage, and recommend remediation.
- Report fraud/revenue assurance risk trends to CRO to facilitate reporting to Executive Commitee and Board Risk Committee.

8. Monitoring, Reporting & Regulatory Liaison

- Conduct compliance reviews against CBK Prudential Guidelines, Risk Management Guidelines, and other ICT-related regulations.
- Provide ICT risk regulatory reporting to CBK, including posture, incidents, and BCP/DR test outcomes.

- Prepare ICT risk dashboards, KRI reports, and heat maps for senior management, Executive Commitee and Board governance committees.
- Liaise with Internal/External Audit and CBK inspectors on ICT risk matters, ensuring timely closure of findings.
- Continuously scan the external environment to for emerging risks and new regulations impacting ICT Risk Framework.

9. Leadership & Capacity Building

- Supervise and mentor ICT Risk staff to deliver departmental objectives.
- Build capacity across the Bank in ICT risk management, fraud risk awareness, and resilience practices.
- Recommend tools, systems, and automation to enhance ICT risk monitoring and reporting.
- Support the CRO in managing broader IT, operational and reputational risks as required.

Qualifications & Experience

- Bachelor's degree in information technology, Computer Science, Cybersecurity, or Risk Management.
- Master's degree preferred.
- Professional certifications: Either CRISC, CISSP, CISM, CISA, CISSP, IRMCert, ISO 27001 Lead Implementer/Auditor, PCI DSS lead implementor/Auditor, ITIL, PrinceII/PMP,
- 6–8 years' ICT risk, audit, or security experience in banking/financial services.
- Strong knowledge of CBK Prudential Guidelines, CBK/PG/08 ICT Risk Guidelines, Data Protection Act 2019, Basel II/III, PCI DSS.
- Experience with ICT project risk advisory, BCP/DR testing, vendor risk management, and fraud/revenue assurance oversight.

Key Competencies

- Deep understanding of ICT systems and banking technologies (CBS, payments, cards, mobile/internet banking, fintech integrations).
- Ability to link ICT risks to business, financial, and regulatory impacts, and articulate at EXCo/Board level.
- Strong stakeholder engagement with regulators (CBK), auditors, EXCo, and vendors.
- Analytical, problem-solving, and reporting skills with attention to detail.
- High integrity, independence, and professional judgment.
- Leadership ability to foster a risk-aware culture across the Bank.

ALL applicants MUST apply online to the email; **recruitment@familybank.co.ke**; closing date is **7th February 2026.**
Canvassing will automatically disqualify the candidate. Only shortlisted candidates will be contacted.

"We are an equal opportunity employer"