JOB DESCRIPTION

Job Title:	ICT Risk Officer	**REFERENCE INDICATOR:**	ERM/Risk Measurement
DIVISION:	Risk Management	**DEPARTMENT/ UNIT:**	Risk Management

JOB OBJECTIVE(S)

The ICT Risk Officer is responsible for developing, implementing, and managing the bank's information security strategy to protect systems, networks, and data. The role ensures alignment with the bank's risk management framework, regulatory requirements, industry and group best practices.

INFORMATION SECURITY STRATEGY & GOVERNANCE

- Develop and implement the bank's information security strategy aligned with enterprise risk management.
- Establish security policies, standards, and procedures.
- Ensure compliance with regulatory requirements (e.g., central bank regulations, data protection laws).
- Report on security posture and risks to senior management and risk committees.

RISK MANAGEMENT

- Identify, assess and mitigate IT and cybersecurity risks.
- Conduct regular risk assessments and vulnerability analyses.
- Integrate IT security into the bank's overall risk management framework.
- Maintain risk registers and track remediation action

SECURITY OPERATIONS & INCIDENT MANAGEMENT

- Oversee security operations including monitoring, detection, and response.
- Lead incident response and investigation of security breaches.
- Ensure timely resolution and reporting of incidents.
- Coordinate disaster recovery and business continuity planning.

COMPLIANCE & AUDIT

- Ensure compliance with standards such as ISO 27001, PCI DSS, and regulatory guidelines.
- Coordinate internal and external security audits.
- Address audit findings and implement corrective actions

SECURITY ARCHITECTURE & CONTROLS

- Design and implement secure IT infrastructure and systems.
- Manage identity and access management (IAM), encryption, and network security controls.
- Oversee third-party/vendor security risk management

AWARENESS & TRAINING

- Promote security awareness across the bank.
- Conduct training programs on cybersecurity best practices.
- Foster a culture of security and risk awareness.

KEY PERFORMANCE INDICATORS

- Reduction in security incidents and vulnerabilities.
- Compliance audit results and regulatory adherence.
- Incident response time and resolution effectiveness.
- Risk mitigation effectiveness.
- User awareness and training completion rates.

JOB REQUIREMENTS

Education:

- Bachelor's degree in Information Technology, Cybersecurity, or related field.
- Master's degree is an added advantage.
- Professional certifications such as:
- CISSP (Certified Information Systems Security Professional)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control).

Experience:

- Minimum 5–10 years of experience in IT security, preferably in banking or financial services.
- Experience in risk management and regulatory compliance.

KEY COMPETENCY REQUIREMENTS

- Strong knowledge of cybersecurity frameworks and standards.
- Risk assessment and analytical skills.
- Leadership and stakeholder management.
- Incident response and crisis management.
- Excellent communication and reporting skills.
- High integrity and attention to detail.

Key Relationships

Internal: Risk Department, IT Department, Internal Audit, Compliance, Business Units

External: Regulators, Auditors, Vendors, Security Consultants

Reporting Relationships

Functionally and administratively reports to: Chief Risk Officer (CRO)