NCBA

Job Title:	Principal Engineer – Cyber Security Architecture	**Reports to:**	Senior Manager, Cyber Security Architecture
Unit:	Digital Business	**Department:**	Technology Security
Grade:	Band 5	**Date:**	February 2025
Job holder:		**Supervisor:**	
Signature:		**Signature:**	

Job Purpose Statement

Reporting to the Senior Manager, Cyber Security Architecture, the role holder is responsible for designing and implementing cyber security systems in line with best practices to ensure they meet all requirements including adequate security, capacity, and performance.

The role is also in charge of the day-to-day running of the Cyber Security solutions and services to ensure 99.999% uptime. They will provide technical security expertise and 2nd level support to staff and external partners to ensure the efficient use of systems and tools.

Key Result Areas

Perspectives unique to the role	**% Weighting** *(to add up to 100%)*	**Output**
Architecture Governance	30%	• They will develop security architecture best practices and ensure they incorporated in the implementation of technology systems. • Periodically benchmark and review the security architecture in line with best practice and business strategy. • Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems, and services.
Security Engineering	40%	• Architect and design cyber security systems in line with best practices to ensure they meet user requirements including adequate security, capacity, and performance. • Define cyber security requirements and acceptance criteria for new systems. • Do the technical evaluations and PoCs on Technology and Security solutions. • Recommend major upgrades where required and liaise with the operations team when doing the upgrades especially if it affects the design/architecture of the system.

		• Conduct research and development on new areas in security and present on them for sensitization and knowledge transfer to other team members/staff. • Ensure all security systems implemented have high availability and disaster recovery in accordance with best practices.
Research and Development	25%	• Research on emerging technologies such as cloud, AI, and Quantum computing to identify applicable threats and their mitigations. • Automate cyber processes and risk mitigation. • Ensure attendance of research & innovation sessions with other teams such as Digital Engineering and Enterprise architecture.
People leadership	5%	• Direct and supervise the team members and vendors assigned to the department.

Job Dimensions

Reporting Relationships: jobs that report to this position directly and indirectly	
Direct Reports	• None
Indirect Reports	• None

Stakeholder Management: key stakeholders that the position holder will need to liaise/work with to be successful in this role.	
Internal	**External**
• ICT Risk • Digital Engineering • Technology Infrastructure • Technology Architecture • Loop DFS Projects Management: Project management of all the projects delivered by Loop DFS. • NCBA Bank Group Technology	• Technology security vendors

Decision Making Authority /Mandates/Constraints: the decisions the position holder is empowered to make *(Indicate if it is Operational, Managerial or Strategic)*
• Strategic: security engineering strategy • Operational: Continuous monitoring & system implementation.

Work cycle and impact: time horizon and nature of impact (Planning) *(e.g. Less than 1 week, 2 weeks, 2 weeks – 1 month, 1month – 3 months, 3-6 months, 6-12 months, above 1 year)*
• 1 year and above.

Ideal Job Specifications

Academic:

- University degree, in Computer Science or technical field.

Professional:

- Information security certifications e.g. CISSP/CISM/CISA/CEH
- Information Technology certifications are desirable: ITIL, COBIT, TOGAF, PRINCE2, ISO, Cloud technology.
- Strong understanding of common best practices, frameworks, and regulations (ISO 27001, ISO22301, OWASP, MITRE ATT&CK, CIS, etc).
- Experience in implementing security solutions such as IPS, SIEM, DLP, AD, DAM, PKI etc.

Desired work experience:

- At least 3 years’ experience in Information Technology management.

Ideal Job competencies

• **Technical Competencies**	
Information, Technology	• Knowledge and experience in IT technology platforms across the IT domains. • Knowledge and application of modern IS security management practices in financial services industry to proactively define and implement security quality improvements in line with technological and product changes.
Project Management	Inculcates a culture of project management excellence – project leadership, accountability, high-performance teams, customer and market focus, robust solutions, alignment, discipline, speed, and quality. Implements incentives and metrics to support such agility.