Job Title:	Principal Engineer, Cyber Security Assurance	**Reports To:**	Head of Technology Security
Division:	Digital Business	**Department:**	Technology - Engineering
Grade	Band 5	**Date**	May-24

JOB PURPOSE STATEMENT

The Principal Engineer, Cyber Assurance will be responsible for conducting security reviews on new and existing systems, products and services in compliance with the NCBA Digital Business security policies and industry best practices such as ISO27001, CIS, PCI DSS among others. They will also be responsible for providing timely security assurance reports and advice to the business when required even with very tight timelines.
The role will lead and coordinate all cyber security assurance activities in 5 markets (Kenya, Tanzania, Rwanda, Ghana and Ivory Coast). They will manage external Penetration testing activities periodically for key systems.

KEY RESPONSIBILITIES & PERCENTAGE (%) TIME SPENT

- **Conducting Security Reviews for new and existing NCBA Digital systems:** Perform security assessment on new and existing systems to identify cyber risks and ensure the necessary controls are in place. (40%)
- **DevSecOps Implementation:** Drive the culture of implementing built in security controls end to end in the software development lifecycle and automate the security testing processes. (20%)
- **Research:** Stay up to date with new trends in technology and cyber by continuously researching on emerging technologies and threats to ensure necessary controls are in place. (20%)
- **Leadership:** Manage and coordinate cyber assurance initiatives by both internal and cyber security external teams. Define and report on key cyber metrics to senior management to measure return of investment in Cyber. (20%)

MAIN ACTIVITIES

- Perform design reviews and provide cyber security input to ensure the necessary security controls are included from the beginning of new projects.
- Perform threat modelling for the Digital Business systems to ensure threats are identified and mitigated.
- Perform vulnerability assessments and penetration testing across NCBA Digital Business systems.
- Perform compliance hardening reviews for the NCBA Digital Business systems.
- Provide timely and quality security assurance reports to the business.
- Do regular follow ups with system custodians to ensure identified risks are addressed within the agreed timelines.
- Implement cyber assurance testing tools within the CI/CD pipeline to automate security testing.
- Research on new technologies, threats and vulnerabilities to inform the necessary security controls and investments in cyber.
- Continuously review and improve cyber processes to ensure efficient support to the agile process of software development.

Decision Making Authority /Mandates/Constraints: What decision/s is the position holder empowered to make based on the key result areas of the position?
• Security approval for system go-live. • Security approval for solution designs and architectures. • Technical Decisions for security testing tools.

Type of Planning	Duration of Planning
Long Term Planning	One year
Short Term Planning	Quarterly and Annually for Performance Plans

Financial Responsibility: What financial responsibilities are applicable to the role?
N/A

Responsibility for stocks, equipment etc (non – cash resources).	
Resources, equipment, stocks etc.	**Approximate value (Kshs)**
N/A	

Responsibility for generating revenue
None

Relationship Management: The departments/organizations/companies etc that the position holder will need to relate/liaise with as part of this role
All business units

Project Management	
Type of projects	**Nature of responsibility**
Cyber security tools	Supplier

Process Management	
Type of Processes	**Nature of Responsibility**
Solution architecture and design reviews. Implementation of security testing tools. Change Approval	Responsible Responsible Responsible

COMPETENCE REQUIREMENTS

Excellent Interpersonal Skills

- The candidate relates easily and naturally with executives, business managers, technical teams and customers. Has excellent listening skills and understands the desires and challenges of all our leaders and customers.
- Candidate forms trusted relationships with technical teams and customers

Commercial Acumen

- The ideal candidate has broad knowledge of business and has an interest in market trends.
- With this knowledge, the candidate has researched and possessed an intricate knowledge of our business: its vision, mission, strategy, values and how it operates. They easily see how our business model compares with *trending local & world-wide* consumer demands.

Leadership & Communication Skills

- The ideal candidate can clearly communicate and share the planned cyber initiatives, reports, and risks with executives, business leaders, and stakeholders across the organization - in a manner that leaves them all touched, moved and inspired.

Innovative & Adaptable

- The ideal candidate is passionate about innovation.
- Loves technology and possesses both a deep and broad understanding of the technology market and cutting-edge technology and Cyber trends.
- Continuously listening to our stakeholder's feedback and coming up with new architectures and enhancing existing ones to leverage these *cutting-edge technologies*.

Self-Driven & Results Oriented

- Self-motivated and self-managing.
- Their work has had a material impact in attracting new customers, delighting existing customers, increasing our market share and enhancing our organizations efficiency and profits.
- Delivery model is organized around delighting our customers, increasing our profitability, and increasing the businesses efficiency.

Others

- Knowledge and experience in modern practices for Cyber security, Application Development and Agile Project management in medium to large Financial Institutions.
- Technical skills to effectively perform security testing activities/tasks across various technologies in a manner that consistently produce high quality of results.
- Knowledge and effective application of all relevant banking policies, processes, procedures and guidelines to consistently achieve required compliance standards or benchmarks.
- Self-empowerment to enable development of open communication, teamwork and trust that are needed to support performance and customer-service oriented culture.

QUALIFICATION AND EXPERIENCE REQUIREMENTS

- A Bachelor's degree in Computer Science, Information Technology or related field.
- Minimum of 5 years' working experience in Information Systems Security – e.g. Ethical Hacking, Penetration Testing, Vulnerability Assessments, ICT Audits, Pre-and-Post Implementation System Reviews
- Information security certifications e.g. CEH/CISSP/CISM/CISA/GIAC/CPTP/OSCP
- Minimum of 2 years' working experience in Networking and Operating Systems e.g. Cisco, Huawei, Windows (All) and Linux.
- Demonstrate competency in the use and administration of ethical hacking tools e.g. KALI Linux, Metasploit, Nexpose, Nessus, Nmap, BurpSuite etc.
- Hands on experience in software development with major languages Java, C++, C# and practical experience using relation RDBMS e.g. Oracle and MS SQL etc.
- Working knowledge of Cloud technologies in at least one of the following: AWS, Azure, Google and Huawei.
- Working knowledge and experience in DevSecOps technologies and practices i.e. AGILE, Jenkins, Jira, Github, Gitlab etc… will be an added advantage
- Excellent analytical, problem solving and reporting skills
- A good knowledge of the systems and processes within Financial Services industry.
- Experience in leading teams of security analysts will be an added adavantage.