1.JOB TITLE: ICT SUPPORT (1 year Contract)

Job Reporting To Manager: Manager Open Banking Technologies

Location: CRDB HQ

Job Purpose

The purpose of the job is to effectively be responsible for Open Banking Technologies System administrator, first level support and provide details to second level support day to day for Open Banking Technologies/ESB, Enterprise Service Bus services; GePG Services, BOT/TIPS Services, Channels services, Partner Services and API Integrations

Responsibilities

- Provide technical support and monitoring of the Open Banking Technologies.
- Provide 24-hour on-call support and supervise day-to-day support of these systems.
- Document and analyze technical specifications for changes and projects.
- Review updates, test and implement changes and/or enhancements in compliance with the Change Management Policy.
- Execute System integration testing and subsequent implementation of system upgrades, hotfixes, and patch releases.
- Coordinate interventions by vendors.
- Communication with all key stakeholders
- Provide end-user support; investigate, troubleshoot, document, and resolve hardware and software issues.
- Perform daily system monitoring, verifying the integrity and availability of all hardware, server resources, systems, and key processes, reviewing system and application logs, and verifying completion of scheduled jobs such as backups.

- Perform backup operations, ensuring all required file systems and data are successfully backed up to the appropriate destination(s).
- Perform regular file archival and purge as necessary.
- Repair and recover from hardware or software failures; coordinate and communicate with impacted users.
- Team player and able to work with minimum supervision.
- Innovative and enterprising in identifying and accepting change opportunities effectively forecasting the impact of change and advising/implementing interventions to mitigate risk.

Knowledge, Skills, Qualifications and Experiences Required for The Role

- Degree or equivalent degree in Computer Science, Software Engineering, Telecom Engineering, Electrical Engineering, or equivalent relevant IT degree from a university with a reputable curriculum.
- At least one professional qualification in ITSM related area (i.e. ITIL)
- Experience Required
- Experience an ICT role in a bank of similar size and scale.
- At least 1 years of experience in supporting integrations in organizations of similar size and scale.
- Experience and ability to work effectively in a dynamic, collaborative.
- Knowledge required.
- Technical knowledge of Open Banking solutions
- Good knowledge of operating systems such as Windows, Launcher and Linux.
- Good knowledge of Databases; Oracle, SQL Server, and PostgreSQL
- SLA and vendor Management skills.
- Interactions with vendors, contractors, and other stakeholders
- Strong interpersonal, and communication skills.

Deadline 30th Dec 2023

APPLY HERE

2.JOB TITLE: Specialist cyber security (1 year Contract)

Job Reporting To Manager: Cyber Security (1 year Contract)

Location: CRDB HQ

Job Purpose

The purpose of the job is to be Responsible for the protection of system boundaries, keeping computer systems and network devices hardened against attacks and securing highly sensitive data. This includes designing and managing systems security architecture and developing cyber security designs as per the established security requirements. Ensuring security minimum requirements and best practices are applied consistently across existing and new systems.

Responsibilities

- To implement and enforce Cyber Security Policies to ensure alignment with related corporate policies.
- To understand and provide expert advice on the cybersecurity risks facing information assets.
- Responsible for the technical Cyber security strategy – proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- Responsible for forensic investigation of Cyber security incidents/breaches, providing regular reporting using the appropriate assurance framework.
- To coordinate regular security testing with high-quality reporting. Responsible for the subsequent hardening of IT systems based on the results of regular tests.
- Implement technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
- To administrate and monitor the infrastructure using specific Cyber security applications including [but not limited to] the company-wide antivirus, email encryption, Data Loss prevention, file screening, server audit, and host protection systems. This requires continuous re-assessment of suitability for purpose and making or recommending any required changes.
- Run various assessment tools to obtain insight into security posture and create various reports for management and stakeholders.
- Provide remediation consultation to global teams to support enterprise risk reduction efforts.
- Monitoring of all IT assets on configuration integrity to proactive manage the bank's environment.
- Engineer, implement and monitor security measures for the protection of computer systems, networks and information assets.
- Identify and define system security requirements standards of the bank.
- To be responsible for regular security testing with high-quality reporting. Responsible for the subsequent hardening of IT systems based on the results of regular tests.
- Hardening of all IT assets before being promoted to production environment. A formal checklist will be used for installation/changes of any configuration in the bank's environment for a new/existing setup.

- Help enhance and maintain current hardening standards for all information assets including but not limited to servers, workstations, databases, audiovisuals, and network devices.
- Support penetration testing activities and exercises, including self-capacity to perform penetration testing.
- Recommend assessment-based findings, outcomes, and propositions for further system security hardening enhancement.
- Reviewing configuration APIs and PKIs of the bank to ensure its compliance with the established standard regularly.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters as per the SAT program.
- Monitor internal and external policy compliance and cybersecurity framework is being complied with by both vendors and employees.
- Implement new technology on the network security and ensure security hardening and effectiveness of the control. Implement and Ensure compliance with the Cybersecurity framework within the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff knows his or her duties during such an incident.
- Prepare and report all security incidents to Management or as directed by line manager.
- Real-time monitoring of network and systems user activities.
- Work with different units in the department to reduce systems configuration risk.

Knowledge, Skills, Qualifications and Experiences Required for The Role

- Possession of a bachelor's degree in computer systems technology or related academic field.
- At least 1 ICT Security professional certifications, CISA, CISSP, CEH, CISM, etc.
- Knowledge of the laws as they apply to cybersecurity and recommended standards as applied by appropriate bodies.

- Software development skills
- Penetration testing skills
- Systems Integrations and the use of APIs
- Projects Management
- IT desktop applications, Computer technology
- Operating systems (Windows, LINUX, Red hat, AIX)
- Networking and database technology
- IT Security & Virtualization
- Interpersonal, written, and oral communication skills.

- Knowledge of security Issues and products so that complex security issues can be quickly diagnosed and resolved.
- Report writing and procedure /policy development.
- Good time management.
- Ability to organize self and others and to work on own initiative.
- Expert knowledge of current IT cyber security issues
- Management of a complex IT Infrastructure within a large enterprise-level organization.
- Contingency and Disaster Recovery Planning.
- Up-to-date knowledge of technical applications
- Ability to think ahead and anticipate problems, issues, and solutions.
- Experience providing IT-focused Enterprise Architecture and strategy.

- Windows Operating systems and Active Directory Management
- Anti-Virus domain infrastructure
- At least 3 years of general ICT Security experience in the banking environment.
- Experience working in a deadline-oriented incident management environment managing multiple issues simultaneously.
- Technical handling interaction with vendors, contractors, and other stakeholders

Deadline 30th Dec 2023

APPLY HERE