VACANCIES – DEPARTMENT OF ICT

BACKGROUND
CRDB Bank Plc is inviting applications from qualified and experienced candidates to fill the vacant positions existing in the Department of ICT.

The Bank seeks to recruit highly competent, self-motivated and professional individuals to fill the following positions:

1. **Configuration Application Security Officer.**
2. **Specialist; Network and Cyber Security.**
3. **Specialist; Card System- (3 positions).**
4. **Network Operation Centre (NOC) Analyst- (3 Positions).**
5. **Specialist; Office Application Support.**
6. **Service Desk Analyst.**
7. **Specialist; Supplier Relationship Management.**
8. **Specialist; Business Applications.**
9. **Logical Access Management (LAM) Analyst.**

Remuneration:
CRDB BANK PLC offers competitive remuneration and benefits. Successful candidates will receive attractive and competitive packages commensurate with demands of the position.

Mode of Application & Closing Date
Interested candidates who meet the above criteria should submit an Application Letter accompanied with a detailed up to date CV with two work-related referees addressed to the below email with a ***clear subject of the position applied for*** not later than **30th March 2020.** Hard copies will not be accepted.

Email: career.career@crdbbank.com

1. **Configuration Application Security Officer.**

Job Summary

Daily monitoring of the IT Infrastructure using security technical expertise and looking for patterns and potential issues, this includes working in close connection with Senior ICT Management.

Key responsibilities:

- Ensure provision of relevant IT documents and procedures for use as evidence toward the commitment to meeting full compliance with Information Governance and data security requirements.
- Responsible for the technical IT security strategy, proposing and implementing systems and processes to continuously reduce the risks and effects of hacking and cyber-crime.
- Responsible for the subsequent hardening of IT systems based on results of regular tests.
- In control of monitoring, analysis and escalation of incidents through logs review.
- Administrate and monitor using specific IT Network Security applications including [but not limited to] the company -wide antivirus, email encryption, file encryption, firewall logs, file screening, server audit, and host protection systems. This requires continuous re-assessment of suitability for purpose and making or recommending any required changes.
- Implementing and maintaining security policies, standards and procedures, consistent with industry best practices, to protect against unauthorized access, modification and destruction of data, systems, networks and service.
- Enhance physical security access to sensitive IT Assets.
- To prepare and undertake acceptance test plans for each component of the infrastructure delivered also ensuring compliance of these systems with the security requirements of the bank.
- Hardening of all IT assets before promotion to production environment. Formal checklist will be used for installation/changes of any configuration in the banks environment this is for a new/existing setup.
- Monitoring of all IT assets on configuration integrity in order to proactive manage the bank's environment.
- Work with different units in the department to reduce application configurations risk.
- The SMIS, HISG, DICT, and Executive Management may assign other assignments as needed.

Experience, Knowledge and Skills Requirements

- Bachelor Degree in Information Systems(IS), Computer Science, Computer Systems Technology or related academic field.
- Minimum of 2 years working experience in Configuration Application Security.

- IT Security professional certifications, CISA, CISSP, CEH etc. will be an added advantage.
- Extensive IT knowledge across many of the below areas:
    - IT desktop applications, Computer technology.
    - Operating systems (Windows, LINUX, Red hat, AIX).
    - Networking & Database technology.
    - IT Security & Virtualization.
    - Microsoft Server and Supporting Services.
- Strong interpersonal, written and oral communication skills.
- Report writing skills and procedure /policy development.
- Good time management.
- Ability to organize self and others and to work on own initiative.
- Up to date knowledge of technical applications.
- Ability to think ahead and anticipate problems, issues and solutions.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.

2. **Specialist; Network and Cyber Security.**

Job Summary.

To manage and lead an internal Cyber security team on implementation of cyber security framework, protection of network, data and applications against cyber threats that may lead to a loss of confidential information.

Key responsibilities:

- Monitor all ICT operations and infrastructure. This includes but not limited to daily review of logs and alerts (which are computer security) in order to keep an eye on your organization's digital security footprint.
- Responsible for information security awareness and training program that informs and motivates workers on cyber-security matters.
- Monitor internal and external policy compliance and cybersecurity framework is being compiled by both vendors and employees.
- Work with different units in the department to reduce cyber security risk. From technical controls to policies (and everything in between).
- Implement new technology. If your organization is looking at a new technology, as the cybersecurity manager, you will be evaluating it and helping implement any controls that might mitigate the risk of its operation.
- Implement and Ensure compliance of Cybersecurity framework amongst the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every high-level manager knows his or her duties during such an incident.

- Prepare and report all security incidents to the Manager Network & Cyber Security.
- The SMIS, HISG, DICT, and Executive Management may assign other assignments as needed.

Experience, Knowledge and Skills Requirements

- Bachelor degree in Computer Systems Technology or related academic field.
- ICT Security professional certifications, CISA, CISSP, and CEH etc. will be an added advantage.
- At least 3 years of general ICT Security experience in the banking environment.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.
- Technical handling interaction with vendors, contractors, and other stakeholders.
- Technical knowledge of Information Security.
- Strong interpersonal, written and oral communication skills.
- Strong knowledge in Cyber Security Framework and Security operating Center.

3. Specialist; Card System (3 positions)

Job Summary.

To provide level 2 support for Card Systems: ATM / POS switch, HSM, Card Management system, Card Production systems, International Payment Schemes, Integration with Third Party systems, Incident & problems escalations and follow-up resolution of issues with vendors.

Key responsibilities:

- Administration, configuration and maintenance of ATM /POS switch and card management system.
- Maintain card systems portfolio by monitoring the status and challenges of existing systems, on-going projects and future/prospective projects.
- Monitor / Support interfaces between CRDB Bank's card systems and third party vendors.
- Provide enhancement and support for card management switch, e-transaction services/applications.
- Support Alternative Banking Channels and E-Fraud on card related transactions.
- Interact professionally with various departments.
- Liaise with Card production vendors for 2nd level support issues.
- Generate periodic E-channel reports.
- Liaise with Alternative Banking Channels unit on new card business requirements.
- Perform integrations with card management systems.
- Leading in implementation, testing and certification of the switch, International Card scheme, device certification i.e. ATM, POS.
- Participating with other duties and projects as assigned and deemed necessary to meet the business need.

Experience, Knowledge and Skills Requirements

- Bachelor degree in Computer Systems Technology or related academic field with ICT Service Management ITILv3 certifications.
- 3 Years experience in working in a banking IT environment.
- Experience in issue analysis and resolution.
- Experience and ability to work effectively in a dynamic, collaborative and fast-paced atmosphere.
- Experience in managing Backup / Recovery processes and Systems / Business Continuity.
- Be a team player that motivates and trains other team members.
- Knowledge on Oracle database management.
- Operating System: Working knowledge of MS Windows and UNIX (HP-UX, Linux) Operating Systems.
- Good understanding of network technologies.
- Knowledge of ATMs, POS and card production lifecycle.
- Basic knowledge of Visa, MasterCard and Union Pay International technologies, operation and trends.
- Knowledge of card management systems, switches and HSM.
- Strong interpersonal, written and oral communication skills.
- ICT Service Management skills.
- Troubleshooting and ICT problem solving skills.
- Excellent Interpersonal and relationship skills.

4. Network Operation Centre (NOC) Analyst- (3 Positions)

Job Summary.

To ensure that services run efficiently without interruption and ensure timely service restoration from service incidents when service issues occur.

Key responsibilities:

- Provide timely response to all incidents, outages and performance alerts. Categorize issues for escalation to appropriate technical teams and between ICT Department and stakeholders (internal and external) with respect to service performance and availability. This includes Branches, Business units, Aggregators, MNOs, third-parties, who are linked to the Bank's payment systems among others.
- Monitor Services, Applications, Servers and Network Communication link nodes, ATMs, POS on the monitoring tools and are monitored adequately.
- Support multiple technical teams in 24 x 7 environment operational environments with high uptime requirements. Varied shift schedules may include day or evening/odd hours.
- Maintain and meet the demand and respond in a timely manner to network and service anomalies and outages.
- Working with flexibility in different shifts for the NOC operations and performance in an efficient and effective manner to ensure maximum possible service availability and performance.
- Recognize, identify and prioritize incidents in accordance with customer business requirements, organizational policies and operational impact.
- Monitor and Report daily, weekly and monthly critical system metrics including trends.

- Work with internal and external technical and service teams to create and/or update knowledge base articles.
- Provide timely response to all incidents, outages and performance alerts. Categorize issues for escalation to appropriate technical teams.
- Collect and review performance reports for various systems, and report trends in hardware and application performance to assist senior technical personnel to predict future issues or outages.
- Document all actions in accordance with standard company policies and procedures.
- Perform basic systems testing and operational tasks (installation of patches, network connectivity testing, script execution, etc.)

Experience, Knowledge and Skills Requirements

- Bachelor's Degree in Computer Science, Information Technology or equivalent from an accredited institution.
- Basic Microsoft and/or Cisco certifications (CCNA, MCITP, etc.) will be an added advantage.
- Minimum of 2 years' experience working in a banking IT environment.
- Minimum of 3+ years of knowledge and understanding of ITIL processes.
- Knowledge of ICT environment and broad experience using a variety of monitoring tools.
- Basic Knowledge of Banking/ Branch Operations.
- Excellence in interpersonal, communication and team skills.
- Strong rapport and relationship building skills.
- Good level of business awareness and problem solving.
- Courtesy and customer focused attitude.

5. Specialist; Office Application Support.

Job Summary.

Responsible for providing timely support to the daily operation in the company and support applications which are directly used by the users on their daily activities like Corporate Email, Active Directory, workflows. The candidate must possess excellent interpersonal skills, and the ability to work well in a diverse, multicultural environment. The candidate should also have a sense of ownership over all applications and should ensure smooth daily operation of all applications in the position's purview.

Key responsibilities:

- To Monitor and provide technical support to all applications and ensure that necessary help is provided to the end-users and allots work to the staff.
- Responsible for resolving critical issues of the system which is used by normal users in their daily operations.
- Provide timely and high-quality L1 and L2 support for AD, Corporate email, and all other office application systems, leveraging specialized knowledge and training in aforementioned applications.

- Author and oversee all technical documentation necessary to facilitate usage and adoption of applications, including user and admin guides; routinely review documentation to ensure accuracy.
- Administer all upcoming patches, plugins, new service packs and versions and ensure effective implementation to provide better services.
- Collaborate with Manager Office Application to administer applications to meet business needs.
- Testing new products, running regular maintenance checks and keeping up-to-date with information security issues.
- Plan and host ad-hoc webinars, tele-conferences, and/or in-person meetings to better train and support application users.
- The application support specialists also participate in the research and system application needs to visualize any problems for users. They also provide assistance to the customers or clients regarding the use of various software applications.
- Coordinate with vendors and other business users and provide technical assistance for all applications.
- Prepare management reports to review for precision and totality of contents and document the reports obtained from the team members and present them to the Manager Office Application Support.

Experience, Knowledge and Skills Requirements

- Bachelor degree in Computer Systems,Technology or related academic field.
- At least 3 years of experience in Office Application Support in any financial institution.
- At least 1 certification from Microsoft.
- Minimum of 3 years experience as an IT technician.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.
- Technical handling interaction with vendors, contractors, and other stakeholders.
- Technical knowledge in System Administration and support.
- Technical knowledge on Client and Servers Operating Systems.
- Strong interpersonal, written and oral communication skills.
- Security operating Control.
- Ability to explain complex ideas to those with limited IT and systems knowledge.
- Technical knowledge in System Administration and support.
- Technical knowledge on Client and Servers Operating Systems.

6. Service Desk Analyst.

Job Summary.

Responsible for managing calls, emails and tickets raised by users regarding ICT service requests, queries and complaints. A primary contact point for users, so the analyst will login requests and incidents, and then follow up with support teams for resolution within agreed service level targets.

Key responsibilities:

- Support the activities in the ICT Service Management System as required by ISO 20000 requirements.

- Participate in ISO 20000 internal audits and improvement initiatives.
- Recording incidents on Service Desk and ensuring ICT Department members properly record incident information on Service Desk.
- Closing incidents on Service Desk and verifying users and business units have resumed normal operations.
- Monitoring the status and progress towards resolution of assigned incidents as well as keeping users and ICT Department informed about incident progress.
- Recording all incidents tickets on Service Desk tool.
- Routing incidents to support specialist groups within the ICT Department.
- Analyzing for correct prioritization, classification and providing initial support.
- Providing resolution and recovery of low level incidents not assigned to support specialist groups.
- Closing incidents all incidents tickets on Service Desk tool.
- Monitoring the status and progress towards resolution of assigned incidents.
- Keeping users and ICT Department informed about incident progress.
- Escalating incidents as necessary per established escalation policies.
- Providing a single point of contact and end-to-end responsibility to ensure submitted service requests and service incidents have been processed.
- Providing initial assessment of service requests to determine which IT resources should be engaged to fulfill them.
- Communicating service requests to other IT resources that will be involved in fulfilling them.
- Escalating service requests in line with established service level targets.
- Ensuring service requests are appropriately logged on Service Desk,follow up for fulfillment and closing the tickets as required.
- Providing data to other ICT department teams from Service Desk.
- Conducting Service Desk customer satisfaction surveys.
- Monitoring progress on the resolution of known errors and advising ICT Department staff on the best available workaround for incidents.

Experience, Knowledge and Skills Requirements

- Bachelor's Degree in Computer Science, Information Technology or their equivalent from an accredited institution.
- More than 3+ years of knowledge and understanding of ITIL processes.
- Minimum of 2 years' experience working in a banking IT environment.
- Excellence in interpersonal, communication and team skills.
- Strong rapport and relationship building skills.
- Good level of business awareness and problem solving.
- Courtesy and customer focused attitude.

7. Specialist; Supplier Relationship Management.

Job Summary.

Provide leadership in building and managing relationships with ICT suppliers and internal stakeholders, to ensure the achievement of business objectives and outcomes, performance criteria and targets are achieved and also ensuring that the Bank's obligations to suppliers are executed with all due diligence and within the agreed SLAs.

Supplier Relationship Management Specialist is also the process owner for ICT financial management practice.

Key responsibilities:

Relationship Management

- Act as a single point of contact (SPOC) and accountability for escalation point for ICT supplier issues, identify the causes and facilitate the amicable resolution of disputes, engaging all subject matter experts such as Legal, Technical, and Finance, Business and Procurement partners as appropriate in the resolution process.
- Develop excellent working relationships with all ICT suppliers.
- Facilitate joint meetings between ICT stakeholders and suppliers.
- Coordinates with senior business leaders who serve as Executive Sponsors for key ICT suppliers to oversee and manage their relationship with the suppliers.
- Negotiate service provision that will deliver greater efficiencies for services delivered to ICT.
- Ensure ethical and professional communication with all ICT suppliers and other stakeholders.
- Define, document and implement an approved annual engagement/Service review plan for ICT suppliers, especially the strategic ones to measure their performance, and establish plans for continuous improvement on a regular basis.

Budgeting & Cost Management

- Prepare and control the annual budget (CAPEX & OPEX) of the section.
- Collate Annual Collate OPEX budget data for ICT Department and prepare Annual Budget.
- Submit ICT Annual OPEX Budget to ICT Management for review and concurrence.
- Ensure that inputs from all stakeholders are considered in preparing Annual ICT budget and obtain extra budgetary approvals where required.
- Maintain a detailed record of all payments made to each supplier to support annual budget forecasting exercises.
- Manage, monitor and control ICT costs in line with the approved budget and produce periodic performance reports.
- Re-negotiate cost of Service Level Agreements in a timely manner and with cost optimization, cost avoidance, savings or equal contract value in line with the Bank's cost containment drive.
- Process the payments to ICT suppliers based on their performance reports.
- Prepare monthly progress update reports of the section.
- Setup and implement cost saving initiatives.
- Develop & update policies, procedures and processes to improve efficiency & productivity of the section.
- Comply with principles and policies in the information security handbook.
- Conduct Risk Control Self-Assessment (RCSA) of the section.

Service Level Management, Monitoring & Enforcement

- Ensure all ICT Services, products and infrastructure are supported by valid Service Level Agreement at all times.
- Establish key metrics for monitoring the performance of each supplier to measure and assure quality of services delivered to the Bank.

- Perform periodic monitoring and management reporting on the performance of ICT suppliers to ensure delivery is in line with their obligations and performance metrics.
- Ensure that all of the terms and conditions of an agreement are thoroughly reviewed, documented, and mitigate risks to the Bank while adhering to internal and external compliance.
- Drive standardization of Service Level Agreement across all ICT suppliers.
- Enforce SLA penalties on ICT Suppliers where service levels are not met.
- Ensure all Service Level Agreements are compliant with the Bank's internal controls.
- Manages the lifecycle of each SLA such as initiation, variation, renegotiation, renewal and termination.
- Ensure the correct appropriate terms and conditions are applied to each SLA over the lifecycle of the agreement, and track funds expended to ensure compliance.
- Define and document annual deliverables of strategic vendors and monitor delivery through performance management.

Experience, Knowledge and Skills Requirements

- Bachelor degree in Business, ICT or related academic field.
- Minimum of 5 years of managing ICT supplier relationships.
- Experience of successfully conducting a range of negotiations across a variety of ICT categories.
- Background in third party/vendor management and governance, procurement, or regulatory compliance is preferred.
- Experience in effective and successful vendor negotiations to optimize, reduce costs and keep ICT budget on track.
- Strong interpersonal, written and oral communication skills.
- ICT Service Management skills.
- Project Management skills.
- Strong follow-through and initiative to stay with issues until they are resolved, along with discipline and tenacity to meet deadlines.
- Strong dispute resolution and mediation skills to handle issue escalation and to drive win-win outcomes for both parties.
- Microsoft Office, especially Excel, Word and Power Point.
- Strong ability to build relationships across functions.
- Ability to aggressively take the lead on implementation of savings opportunities that affect numerous lines of business.
- Demonstrated high level organizational and time management skills.
- Strong sense of accountability and business partnership.
- Financial Management skills.

8. Specialist; Business Applications.

Job Summary.

Responsible for providing operational support and maintenance of healthcare of business automation applications which includes but not limited to SAP SuccessFactors (Cloud-based HRMIS), SAP ERP System, Back-Office Operations System, End-to-End Credit Management System, CISCO Unified Contact Center Express (Cisco UCCX), Customer Relationship Management system (CRM), Anti Money Laundering system (AML),

Operational Risk Management system (OPRISK), Document Management System (DMS), etc. This position will address business automation applications issues to sustain application functionality and identify process improvement opportunities across the business applications systems.
Required to work closely with the business departments and key vendors to resolve any technical deficiencies, assist with integration needs, implement and test new functionality and generally, to ensure that business applications unit deliver a quality banking experience through systems automation as well as contributing to the strategic direction of the Bank's banking systems and services.

Key responsibilities:

- Facilitate automation of new and existing business applications.
- Ensure infrastructure systems and services are operating at optimal level to ensure business functions, high availability and recoverability.
- Implement and/or upgrade applications and provide second line support for Production, Disaster Recovery site and Tests environments.
- To research and recommend innovative ideas, and where possible automation for system administration tasks. Identify approaches that leverage our resources and provide economies of scale.
- Work with Change/Release Management process stakeholders for successful change execution.
- Ensure systems performance tuning and results experience and constantly review of application logs to ensure no suspicious alerts of system issues.
- Daily systems and server's health checkup (Running processes, CPU utilization, Memory utilization, Load average etc.)
- The use of formal issue trackers or ticket management software to track progress on issues until resolution and closure.
- Respond rapidly to and resolve help desk requests.
- Monitor the system daily and respond immediately to security or usability concerns.
- Ensure that backups of all administering applications are being performed daily and are tested on a regular basis.
- Working with vendors in the process of troubleshooting escalated incidents. This may involve gathering technical information requested by them, and discussing and challenging their findings. Be available 24/7 when needed.
- Participate in appropriate in-service and workshop programs and attend any required meetings.
- Collaborate with other systems administrators on implementing new server technologies and new computer technologies.
- Define, document, maintain best practices, and support procedures (configuration, operational etc.)
- Support and provide guidance to Bank's employees on issues related to business applications.
- To create, amend and delete/disable system's user accounts as per requests and procedure.
- Coordinate with all relevant departments with regards to training and testing on new and existing and upgraded business applications.

Experience, Knowledge and Skills Requirements

- Minimum Bachelor's degree in Information Technology or Computer Science or Computer Engineering.
- Information Technology Infrastructure Library (ITIL).
- Best practices SAP System Administration Certifications is an added advantage.
- Minimum of 3 years of general ICT Systems support experience in banking environment.
- Ability to handle numerous concurrent tasks under time constraints, effectively prioritize and execute tasks in a highly dynamic environment.
- Technical interaction with vendors, contractors, and other stakeholders.
- Knowledge of Enterprise Resource Planning Systems.
- Understanding of Infrastructure technologies including networks, servers and databases.
- Understanding the core functions of the business unit, policies and procedures of assigned systems.
- Knowledge of system vulnerabilities and security issues.
- Team player who exhibits effective interpersonal skills with a collaborative style.
- Ability to create and deliver results in a highly collaborative environment.

9. Logical Access Management (LAM) Analyst.

Job Summary.

Performing activities around Logical Access Management (i.e. creation of user IDs, assigning of access rights to system users, resetting users passwords, activating and disabling of user IDs, etc) in accordance with the established policies, processes and procedures.

Key responsibilities:

- Perform Logical Access Management tasks (creation of new user IDs, assign access rights to users, resetting users passwords, activating user IDs, disabling user IDs, etc) in accordance with relevant Logical Access Management processes and procedures.
- Ensure Logical Access Management requests have proper approvals before addressing them.
- Communicate feedback to users in case there is any delay in addressing their requests.
- Ensure that password and any other sensitive information related to user login credentials is communicated to the right people.
- Track status of any request initiated by anyone in the SLAM system.
- Generate and/or prepare user's profiles reports that detail their access rights for different systems.
- Forward user profiles reports to business units for their reviews within agreed timelines.
- Forward exceptions picked during the user access reviews including access rights that violate the segregation of duties (SoD) principle.
- Document user access reviews and ensure signed off review sheets are properly filed for future reference.
- Continually devise ways of improving processes and procedures around reviews of user access.
- Provide information related to user access rights issues as requested by auditors.
- Address audit and Management Assurance findings by performing actions under area of responsibility.

- Ensure controls defined in audit finding closures or management assurance reports related to area of responsibility are embedded in daily operations.
- Get a daily report of leavers and transfers from the HR system.
- Disable all user IDs of leavers and transfers as necessary.
- Disable user IDs of interdicted members of staff immediately upon receiving interdiction notice from HR or any other reliable sources (e.g. line manager of the interdicted staff members).
- Ensure all Logical Access Management requests from the SLAM system are properly filed and approved by relevant authorities to ensure easy reference and retrieval in future.
- Ensure any deviation from normal processes and procedures gets prior approval from relevant authorities and evidence for that is kept for future reference should such need arise.

Experience, Knowledge and Skills Requirements

- Bachelor's Degree in Computer Science, Information Technology or their equivalent from an accredited institution.
- A certificate in IT security or information systems audit e.g. CISSP, Security+ etc. (preferred) is an added advantage.
- Minimum of 3+ years of knowledge and understanding of ITIL processes, at least 2 years' experience working in a banking IT environment.
- Basic Knowledge of Banking/ Branch Operations
- Knowledge in core banking applications.
- Strong rapport and relationship building skills.
- Good level of business awareness and problem solving.
- Courtesy and customer focused attitude.