CRDB BANK

*The bank that listens*

## 1. SPECIALIST CYBER SECURITY SYSTEMS (1 YEAR CONTRACT)

| | |
|---|---|
| Reporting Line: | MANAGER CYBER SECURITY |
| Location: | Tanzania Head Office |
| Department: | CYBERSECURITY UNIT |
| Number of openings: | 1 |

Job Purpose

Responsible for 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.

Principle Responsibilities

- To implement and enforce Cybersecurity 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 Cybersecurity strategy – proposing and implementing solutions and processes to continuously reduce the risks and effects of hacking and cybercrime.
- Responsible for forensic investigation of Cybersecurity 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 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 Cybersecurity 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 reassessment of suitability for purpose and making or recommending any required changes.
- Run various assessment tools to obtain insight on 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 in order to proactively 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 results of regular tests.
- Hardening of all IT assets before promotion to the 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. This includes but is not limited to servers, workstations, databases, audio-visuals, 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.
- Review configuration APIs and PKIs of the bank to ensure compliance with the established standard on a regular basis.
- Responsible for the information security awareness and training program that informs and motivates workers on cybersecurity matters as per the SAT program.
- Monitor internal and external policy compliance and ensure the 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 of the Cybersecurity framework across the organization.
- Participate in the incident response program, ensuring that the program is tested throughout the organization and that every staff member knows their duties during such an incident.
- Prepare and report all security incidents to Management or as directed by the line manager.
- Real-time monitoring of network and systems user activities.
- Work with different units in the department to reduce systems configuration risk.
- The CRDB Bank Management may assign other responsibilities as needed.

Qualifications Required

- Bachelor’s degree in computer science, Cyber Security, Software engineering or related academic field.
- At least one security professional certifications such as CISA, CISSP, CEH, CISM are a plus.
- At least 3 years of general ICT security experience in banking environment.
- Expert knowledge of current IT cybersecurity issues.
- Management of a complex IT infrastructure within 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.
- Experience of working in a deadline-oriented incident management environment managing multiple issues simultaneously.

CRDB Commitment

*CRDB Bank is dedicated to upholding Sustainability and ESG practices and encourage applicants who share this commitment. The Bank also promotes an inclusive workplace, hence applications from women and individual with disabilities are encouraged.*

*It is important to note that CRDB Bank does not charge any fees for the application or recruitment process, and any requests for payment should be disregarded as they do not represent the bank’s practices.*

*Only Shortlisted Candidates will be Contacted.*

| | |
|---|---|
| Deadline: | 2025-10-12 |
| Employment Terms: | CONTRACT |
| Contract Duration: | 1 YEARS |

**APPLY HERE**

## 2. MANAGER AGENCY & SECURITY TRUSTEE

| | |
|---|---|
| Reporting Line: | Senior Manager; Agency & Security Trustee |

| | |
|---|---|
| Location: | Tanzania Head Office |
| Department: | DEPARTMENT OF CORPORATE BANKING |
| Number of openings: | 1 |

## Job Purpose

Responsible for managing the bank's role as agent in loan administration and serving as the primary liaison between the borrower and the lending syndicate. Manages key activities such as loan disbursements, repayments, and reporting in line with agreements between the syndicate members and the borrower, ensuring efficient operations and full compliance with the loan terms.

## Principle Responsibilities

### Loan Administration

- Manage the day-to-day administration of syndicated loans, including processing drawdowns, repayments, and interest payments.

- Ensure timely and accurate execution of all loan-related transactions.

### Communication Hub

- Serve as the central liaison between the borrower and the syndicate of lenders, ensuring efficient and transparent communication.

- Collaborate effectively with internal departments (Legal, Credit, Treasury, Operations) and external stakeholders such as legal counsel and auditors.

- Coordinate and facilitate lender meetings, consent solicitations, amendments, waivers, and other corporate actions.

### Compliance

- Ensure all loan activities adhere to the loan agreement terms and comply with relevant regulatory requirements.

### Reporting

- Prepare and distribute periodic reports to lenders, providing updates on loan status, performance, and key developments.

### Monitoring

- Continuously monitor the loan for risks, including covenant breaches or changes in the borrower's financial health.

- Oversee borrower compliance with covenants and take appropriate actions in case of defaults or breaches, including prompt submission of incident reports.

- Stay updated on legislative changes, market trends, and emerging risks impacting the agency function.

## Relationship Management

- Foster and maintain strong, professional relationships with both borrowers and syndicate members.
- Ensure smooth, efficient, and compliant operations throughout the syndicated loan lifecycle.

## Dispute Resolution

- Support in facilitating resolution of disputes between borrowers and lenders when they arise.

## Qualifications Required

- Education: Bachelor's degree in Finance, Business, or a related field.
- Experience: 5 years of experience in corporate banking, syndication, or a related field, with at least 3 years in lending practices.
- Technical Expertise: Strong understanding of corporate finance, credit analysis, risk management, and corporate banking products, services, and delivery channels.
- Market Knowledge: Well-versed in competitive market structures, industry practices, and regulations for business banking, with a minimum of 3 years' experience in the local environment.
- Skills:
    - Excellent negotiation, selling, and communication skills.
    - Strong analytical and problem-solving capabilities.
    - Proven ability to manage multiple projects simultaneously and meet tight deadlines.
    - Ability to quickly acquire and apply new knowledge effectively.
    - High level of cultural awareness and adaptability.

## CRDB Commitment

*CRDB Bank is dedicated to upholding Sustainability and ESG practices and encourage applicants who share this commitment. The Bank also promotes an inclusive workplace, hence applications from women and individual with disabilities are encouraged.*

*It is important to note that CRDB Bank does not charge any fees for the application or recruitment process, and any requests for payment should be disregarded as they do not represent the bank's practices.*

*Only Shortlisted Candidates will be Contacted.*

| | |
|---|---|
| Deadline: | 2025-10-03 |
| Employment Terms: | PERMANENT |

**APPLY HERE**