



# Job Description

9th Floor Tanzanite Park, Victoria, Dar es Salaam, Tanzania | +255 758 778 886 | info@empower.co.tz

|                                                                |                                      |                                      |
|----------------------------------------------------------------|--------------------------------------|--------------------------------------|
| <b>Job Title</b><br>Cybersecurity Control Officer              | <b>Job Location</b><br>Dar es Salaam | <b>Category</b><br>-                 |
| <b>Job Type</b><br>Full Time                                   | <b>Job level</b><br>Intermediate     | <b>Industry</b><br>Telecommunication |
| <b>Open to Expatriates</b><br>Only Open to Tanzanian Nationals |                                      |                                      |

## Minimum Requirements

|                                |                              |                                                       |
|--------------------------------|------------------------------|-------------------------------------------------------|
| <b>Min Budget</b><br>-         | <b>Max Budget</b><br>-       | <b>Primary Industry</b><br>Telecommunication: 4 Years |
| <b>Secondary Industry</b><br>- | <b>Primary Category</b><br>- | <b>Secondary Category</b><br>-                        |
| <b>Certificate</b><br>-        | <b>Qualification</b><br>-    |                                                       |

## Summary

The Cybersecurity Control Officer is responsible for providing independent oversight and control assurance over company's cybersecurity environment. The officer will assess whether appropriate cybersecurity controls are designed, implemented and operating effectively to protect company systems, customer information, financial data and digital services.

The role will monitor cybersecurity risks, access controls, vulnerabilities, security findings and remediation activities while maintaining independence from teams responsible for day-to-day IT and cybersecurity operations.

## Responsibilities

### Cybersecurity Control Oversight

- Independently review cybersecurity controls implemented across Company systems and technology environments.
- Assess whether cybersecurity controls are appropriately designed and operating effectively.
- Identify weaknesses and control gaps that may expose the company to cybersecurity threats.
- Monitor corrective actions and ensure identified weaknesses are addressed within agreed timelines.
- Escalate critical cybersecurity-control weaknesses to management.
- Support implementation of cybersecurity governance requirements.

### User Access & Privileged Access Control

- Conduct periodic reviews of user access to critical systems.
- Verify that system access is based on approved business requirements.
- Review privileged and administrator accounts.
- Identify excessive, unauthorized, dormant or inappropriate access.
- Review segregation of duties within critical systems.
- Monitor timely removal or amendment of system access following staff transfers, role changes or separation.
- Follow up identified access-control exceptions until closure.

### Vulnerability & Security Finding Oversight

- Review vulnerability assessment and security-testing results.
- Monitor outstanding vulnerabilities based on severity and business impact.
- Maintain an independent tracker of cybersecurity findings.
- Follow up responsible Technical teams on remediation activities.
- Verify evidence provided for closure of significant cybersecurity findings.
- Escalate overdue critical and high-risk vulnerabilities.
- Monitor recurring security weaknesses.

### **Cybersecurity Risk Assessment**

- Conduct cybersecurity risk assessments on systems, applications and technology processes.
- Participate in risk reviews for new systems and significant technology changes.
- Assess cybersecurity risks relating to new products and integrations.
- Identify potential threats and control gaps before implementation.
- Recommend appropriate cybersecurity risk-mitigation measures.
- Coordinate cybersecurity risk information with the Risk Management Officer.

### **New Systems, Products & Integration Review**

- Participate in control reviews before implementation of significant systems, products and integrations.
- Review security requirements for new technology solutions.
- Verify that important cybersecurity controls are considered during system development.
- Review access, authentication, data protection and security-monitoring requirements.
- Track cybersecurity findings identified before system or product launch.
- Escalate unresolved critical security-control matters before implementation where necessary.

### **Security Incident Oversight**

- Independently review significant cybersecurity incidents.
- Monitor whether security incidents are properly investigated and documented.
- Review root-cause analysis and corrective actions.
- Track implementation of agreed actions following incidents.
- Identify recurring cybersecurity incidents or control weaknesses.
- Provide independent reporting on significant cybersecurity events to management.

### **Information Protection Controls**

- Review controls designed to protect sensitive company and customer information.
- Assess access and handling controls for confidential information.
- Review controls relating to data sharing and transfer where required.
- Identify weaknesses that may result in unauthorized disclosure, modification or loss of information.
- Work with responsible teams to ensure identified information-security weaknesses are addressed.

### **Third-Party Cybersecurity Risk**

- Support cybersecurity risk assessments for critical technology vendors and service providers.
- Review relevant cybersecurity requirements before onboarding key technology partners.
- Assess security risks arising from third-party system access and integrations.
- Monitor remediation of significant third-party cybersecurity findings.
- Escalate significant third-party cybersecurity exposures.

### **Cybersecurity Policies & Control Standards**

- Review cybersecurity policies, procedures and standards from an independent control perspective.
- Monitor compliance with approved cybersecurity requirements.
- Identify areas where controls or policies require strengthening.
- Support periodic cybersecurity-control self-assessments.
- Monitor implementation of cybersecurity-related audit and control recommendations.

### **Cybersecurity Awareness & Compliance**

- Support implementation of cybersecurity awareness programmes.
- Monitor staff compliance with key cybersecurity requirements.
- Identify recurring cybersecurity awareness weaknesses.

- Provide control recommendations based on observed risks and incidents.
- Support periodic cybersecurity compliance reviews

## Cybersecurity Reporting

- Prepare regular cybersecurity control and risk reports.
- Maintain dashboards covering:
  - o Critical vulnerabilities
  - o High-risk findings
  - o Access-control exceptions
  - o Cybersecurity incidents
  - o Remediation status
  - o Outstanding audit findings
- Highlight overdue corrective actions.
- Immediately escalate critical security-control weaknesses to management.
- Provide independent cybersecurity-control updates to the Head of Internal Control.

## KEY PERFORMANCE INDICATORS (KPIs)

Performance will be measured against:

- Percentage of scheduled cybersecurity-control reviews completed.
- Percentage of critical system access reviews completed on time.
- Number of overdue critical and high-risk cybersecurity findings.
- Percentage of cybersecurity findings closed within agreed timelines.
- Timeliness of critical risk escalation.
- Percentage of new critical systems/products reviewed before implementation.
- Number of unresolved privileged-access exceptions.
- Recurrence rate of previously identified cybersecurity weaknesses.
- Timeliness and quality of cybersecurity-control reports.
- Completion rate of cybersecurity incident corrective actions.
- Accuracy and completeness of cybersecurity findings trackers.

## EXPECTED RESULT

The Cybersecurity Control Officer is expected to provide management with independent assurance that company's critical cybersecurity risks and controls are properly monitored and addressed.

## Education & Qualifications

---

- Bachelor's Degree in Cybersecurity, Information Security, Information Technology, Computer Science, Information Systems or a related field.
- Certifications such as CISA, CISM, CISSP, CEH, ISO 27001 or equivalent cybersecurity qualifications will be an added advantage.

## Requirements

---

- Minimum of 2–4 years of relevant experience in cybersecurity, information security, IT audit, technology risk or IT controls.
- Experience in financial services, fintech, mobile money, telecommunications or banking will be an added advantage.
- Experience in access-control reviews, vulnerability management or technology-risk assessments is desirable.

## Characteristics

---

### KNOWLEDGE & SKILLS

The job holder should have:

- Strong understanding of cybersecurity controls and information-security principles.
- Understanding of identity and access management.
- Knowledge of vulnerability and patch-management controls.
- Knowledge of cybersecurity risk assessment.
- Understanding of network, application, database and infrastructure security concepts.
- Good understanding of IT general controls.
- Knowledge of cybersecurity incident-management processes.
- Strong analytical and investigative skills.

- Ability to assess technical issues from a risk and control perspective.
- Good report-writing and presentation skills.
- Strong documentation and follow-up skills.

#### **CORE COMPETENCIES**

- High integrity and confidentiality.
- Independence and professional judgement.
- Strong analytical thinking.
- Attention to detail.
- Cybersecurity awareness.
- Risk-based thinking.
- Problem-solving.
- Accountability.
- Strong follow-up.
- Effective communication.
- Ability to challenge control weaknesses professionally.
- Ability to work under strict deadlines.

#### **Reporting To**

---

Head of Internal Control

#### **Driving Licence**

---

Not Required

To Apply for This Job [Click Here](#)