PACIS
INSURANCE COMPANY LTD
For Comfort & Peace in Life

+254 730 677 000

Info@pacisinsurance.com

Pacis Centre, 4th Floor off Waiyaki Way,
Westlands - Nairobi

JOB DESCRIPTION

POST TITLE: ICT RISK & CYBERSECURITY OFFICER

DEPARTMENT: RISK & COMPLIANCE

REPORTING TO: HEAD OF RISK & COMPLIANCE

1. JOB PURPOSE

To provide second-line oversight of ICT risks, cybersecurity and data protection, assess control effectiveness and monitor compliance to safeguard the Company's information assets and critical operations.

2. PRINCIPAL ACCOUNTABILITIES.

ICT Risk Management and Governance

- Conduct ICT risk assessments covering infrastructure, applications, technology projects and system changes.
- Review ICT governance arrangements, policies and procedures against the Company's risk appetite and business objectives.
- Maintain the consolidated ICT and cybersecurity risk register and recommend appropriate mitigation measures.
- Monitor ICT Key Risk Indicators, analyse trends and escalate threshold breaches.

Cybersecurity leadership and Risk Management

- Support implementation and review of the Company's cybersecurity strategy, policies and improvement plans.
- Advise ICT and Management on cybersecurity architecture, security controls, emerging threats and mitigation measures.
- Conduct cybersecurity risk assessments covering critical systems, cloud environments, third parties and emerging technologies, including AI.
- Monitor implementation of cybersecurity risk mitigation measures and recommend improvements.
- Review cybersecurity controls, vulnerability assessments, penetration testing, periodic red teaming exercises and remediation actions.
- Review cybersecurity exceptions and risk acceptance requests in accordance with approved governance requirements.
- Coordinate cybersecurity incident preparedness, response assessments and staff awareness programmes.

Data Protection and Compliance

- Coordinate implementation and review of the data protection framework, policies and procedures.
- Conduct privacy compliance reviews and coordinate Data Protection Impact Assessments.
- Support responses to data subject requests, privacy complaints and confidentiality queries.
- Maintain records of processing activities with departmental data owners.
- Review privacy notices, consent arrangements, retention practices and data-sharing arrangements.
- Assess cross-border data transfers and recommend appropriate safeguards.
- Support personal data breach assessments and notifications and maintain privacy incident records.

Third Party Technology Risk

- Conduct ICT, cybersecurity and privacy due diligence on technology vendors, cloud providers and other relevant service providers.
- Review contractual safeguards covering security, confidentiality, incident notification, continuity, data processing and exit arrangements.
- Assess outsourcing, vendor dependency and service concentration risks.

Business Continuity and Cyber Resilience

- Support ICT disaster recovery and cyber recovery planning in alignment with business continuity requirements.
- Review backup and restoration arrangements against approved recovery objectives.
- Coordinate cybersecurity incident simulations and recovery exercises, assess results and recommend improvements.

Reporting and Stakeholder Management

- Prepare ICT risk, cybersecurity and data protection reports for Management and the Board Audit & Risk Committee.
- Monitor cybersecurity performance indicators, analyze trends and escalate significant risks and control weaknesses.
- Coordinate cybersecurity incident notifications, quarterly returns and other regulatory submissions within prescribed timelines.
- Support independent cybersecurity audits, regulatory reviews and monitoring of associated corrective actions.
- Perform any other duties as may be assigned in line with the role and organizational objectives.

3. RELATIONSHIPS

ICT Risk Management and Governance

REPORTING TO: Head of Risk & Compliance
OTHER CONTACTS:
Within the company: All departments
Outside the Company: Office of the Data Protection Commissioner (ODPC),Insurance Regulatory Authority (IRA), ICT Vendors and Service Providers

4. KNOWLEDGE AND EXPERIENCE

Qualifications:

- Bachelor's degree in information technology, Computer Science, Cybersecurity or related field.
- Professional certifications in Data Protection, ISO 27001, CISA, CRISC, CISSP, CISM or related certifications

Experience:

- At least four (4) years' experience in ICT risk, cybersecurity, information security, data protection within a regulated financial institution.

Knowledge:

- Knowledge of the IRA Cybersecurity Guidance Note, the Computer Misuse and Cybercrimes Act, 2018, and the Data Protection Act, 2019.
- Understanding of cybersecurity frameworks and standards, including NIST and ISO/IEC 27001.
- Familiarity with cybersecurity threat intelligence, MITRE ATT&CK, Zero Trust principles and emerging technology risks, including AI.

5. SKILLS AND COMPETENCIES

- **Problem solving**
- **Team player**
- **Analytical skills**
- **Attention to detail**
- **Interpersonal skills**
- **Communication and report writing skills**

Application closing date is 30th November 2026. All applications should be done on www.pacisinsurance.com/careers attaching an updated CV and cover letter.

***Only shortlisted candidates will be contacted.**