



CAREER OPPORTUNITIES AT EQUITY BANK.

Equity Bank is one of the region's leading Banks whose purpose is to transform the lives and livelihoods of the people of Africa socially and economically by availing them modern, inclusive financial services that maximize their opportunities. With a strong footprint in Kenya, Uganda, Tanzania, Rwanda, DRC and South Sudan, Equity Bank is home to more than 20 million customers – the largest customer base in Africa. Currently the Bank is seeking additional talent to serve in the role outlined below.

General Information about the opportunity

Job Title: Data Protection and IT Risk Manager

Department: Risk Management

Reports to: Head of Risk

Job Purpose

The Data Protection and IT risk Manager will be responsible for overseeing the Bank's data protection strategy, IT risk strategy and their implementation to ensure compliance with Data Protection Laws in the country and ensure IT risk is managed well. The role will work closely with Leadership of IT Security, Legal, Risk and Compliance functions.

Key Responsibilities and Accountability

1. Inform and advise Equity Bank of their obligations pursuant to the Data Protection Laws.
2. Monitor compliance with the Data Protection Laws and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in personal data processing operations, and the related audits.
3. Provide advice where requested as regards the data protection impact assessment and monitor its performance.
4. Cooperate with the supervisory authority and to act as its contact point on issues relating to processing of personal data, including the prior consultation with the supervisory authority, and to consult, where appropriate, with regard to any other matter.
5. Implementing measures and a privacy governance framework to manage data handling and use in compliance with the privacy laws that Equity bank has to be compliant with.
6. Working with key internal stakeholders in the review of projects to ensure compliance with local data privacy laws, and where necessary, complete and advise on privacy impact assessments
7. Serving as the primary point of contact for queries in the business in regards to data Protection and Privacy.
8. Reviewing Equity vendor contracts and consents needed to implement projects in partnership with the Bank's Legal and Information Security functions, and ensuring filing requirements with local regulator are achieved



9. Ensure fulfilment data Subject rights arising from the various touch points the bank has with the customer.
10. Developing policies, standards and procedures that align to the requirements set out in the GDPR, Data Protection Act and any localization requirements in countries of operation
11. Collaborating with the Information Security function to raise employee awareness of data privacy and security issues, and providing training on the subject matter in the bank.
12. Monitoring performance and providing advice on the impact of data protection efforts across the bank.
13. Maintaining comprehensive records of all data processing activities conducted by the bank including the purpose of all processing activities, which must be made public on request.
14. Interfacing with Equity Bank customers to inform them about how their data is being used, their Rights and what measures the company has put in place to protect their personal information.
15. Collaborating with the Bank's Information Security and Legal functions to maintain records of all data assets, ensure data classification and maintaining a data security incident management plan to ensure timely remediation of incidents, security breaches, complaints and claims
16. Conduct risk assessment related to data handling and ensure the risk register is in place and and updated.
17. Serve as the chief point of contact for our Technology Risk Management & Information Security team.
18. Provide support for reviewing technology initiatives with reputational risks and red flags identified during defined intake procedures.
19. Assist in the definition of the client's technology risk appetite statements and monitor Key Risk Indicators (KRIs) against our technology risk appetite.
20. Prepare the Technology Risk Management & Information Security line of business Technology Risk report and track actions to reduce technology risk.
21. Assist with the Technology Risk reporting operations, including scheduling key monthly meetings, monitoring key milestones, escalation of past due activities, problem triage and management, and archiving key monthly artifacts for audit purposes.
22. Develop on-going technology risk reporting, monitoring key trends and defining metrics to regularly measure control effectiveness for own area.
23. Adhere to internal policies and procedures, technology control standards, and applicable regulatory guidelines.
24. Contribute to the review of internal processes and activities and assist in identifying potential opportunities for improvement.
25. Adhere to, advise, oversee, monitor and enforce enterprise frameworks and methodologies that relate to technology controls / information security activities.
26. Influence behavior to reduce risk and foster a strong technology risk management culture throughout the bank



Key Critical Competence

Behavioural Skills

1. Critical thinking and Problem-solving skills with the ability to analyze complex information to identify the key issue/action and drive resolution.
2. Excellent organizational skills with attention to detail.
3. Excellent interpersonal and communications skills, both orally and in written
4. Ethical and moral skills
5. Have good personal values

Technical skills

6. Knowledge and understanding of modern risk management standards, frameworks and practices
7. Knowledge of national and international regulatory environments and key regulatory regimes
8. Understanding of the national financial industry and business environment.
9. Risk intelligence (critical thinking, creativity, and curiosity, research, surveys, interviews, brainstorming, and scenario planning, analysis emerging risk, forward looking)
10. Risk ethics (risk culture, risk appetite, risk governance, and risk accountability)
11. Risk communication (communications skills, good listener, team player, positive attitude is a must , reports preparation, dashboard, presentation and communication about identified risk and control to be implemented)
12. Risk intelligence (critical thinking, creativity, and curiosity, research, surveys, interviews, brainstorming, and scenario planning, analysis emerging risk, forward looking)
13. Risk ethics (risk culture, risk appetite, risk governance, and risk accountability)
14. Knowledge and experience of best practice Governance, Risk management and Compliance frameworks and methodologies
15. Excellent analytical, statistical and math skills with the ability to interpret vast amounts of performance data and be an IT literate
16. Strong understanding of IT coding, IT information security assessment, IT risk management
17. Interpret the Vulnerability assessment report and penetration Testing report
18. Ability to test Incident response plan
19. Ability to conduct IT risk assessment and provide recommendation on identified loopholes
20. Ability to evaluate the IT environment and assess control in place and suggest any improvement
21. Ability to assess adequacy of information security tool

Qualifications:

1. A bachelor's degree with Second Class upper-level majoring in IT and information security
2. Minimum of 5 years' experience in banking, especially in IT risk management.
3. Expert knowledge of IT security and risk disciplines and practices



4. Professional qualification in IT Risk Management and Data protection risk management is a MUST to have (Certified in information system audit, Data protection certified, etc....)
5. Able to operate in a performance driven organization and culturally aware and adept at working within multicultural settings
6. Attended Leadership training

If you meet the above requirements, submit your application quoting the job opportunity you are applying for as subject of your email through the email address below by **22nd September 2025**. Please include detailed Curriculum Vitae, copies of the relevant certificates, testimonials, and daytime telephone contact and email address. Only short-listed candidates will be contacted.

Email to: **jobsrwanda@equitybank.co.rw**

Equity Bank is an equal opportunity employer. We value the diversity of individuals, ideas, perspectives, insights, values and what they bring to the workplace.