JOB TITLE: Specialist; Technology Control (1 Position(s))

Job Location : Head Office, Hq

Job Purpose:

Responsible for identifying, assessing, mitigating, and monitoring technology-related risks across all technology functions and ensuring compliance with relevant regulations and internal policies.

Main Responsibilities:

- Establish and maintain a comprehensive technology risk management framework that aligns with the banks risk appetite, industrial best practice, and regulatory requirements.
- Coordinate the identification, assessment, and analysis of all technology-related risks across the organization.
- Plan and execute cybersecurity assurance reviews and assessments across various domains.
- Contribute to the development, testing, and maintenance of business continuity and disaster recovery plans for IT systems.
- Evaluate the design and operating effectiveness of cybersecurity controls following relevant frameworks, standards (e.g., ISO 27001, NIST CSF), and regulatory requirements.
- Ensure the timely closure of all audit findings and prevent recurring issues.
- Develop, implementing, maintaining, and regularly reviewing essential technology policies, procedures, standards, guidelines, and practices.
- Collaborate with internal and external auditors by providing requested documentation, evidences, and facilitating walkthroughs. Track and follow up on implementing audit/risk reviews, recommendations, and management action plans to address control weaknesses and compliance gaps.
- Assist in the management of technology-related compliance initiatives and projects.
- Maintain accurate and up-to-date documentation related to technology controls, risk assessments, and compliance activities.
- Prepare regular reports on the status of technology controls and identified risks Collaborate with IT teams and other stakeholders to ensure that privacy compliance requirements are integrated into technology processes and systems.
- Support the organizations efforts to comply with specific standards such as ISO 27001, PCI DSS, or other relevant certifications.

Knowledge and Skills:

- Understanding of IT control frameworks and methodologies (e.g., COBIT, ITIL, ISO 27001).
- Strong knowledge of Cybersecurity risks and controls.
- Knowledge of Technology Risk Management.
- Good understanding of IT processes and technologies.
- Knowledge of data privacy regulations and best practices.
- Strong planning and organizing skills
- Time management skills
- Ability to communicate pleasantly and confidently with change management stakeholders both orally and in writing.
- Demonstrates strong analytical, problem-solving, coordination, and decision-making abilities.
- Be a team player who motivates and educates other team members/stakeholders.
- Ability to interact with all levels of management, staff, and vendors

Qualifications and Experience:

- Degree in Computer Science / Information Technology/Computer Engineering.
- Certification in Technology risk management, preferably CISA
- Certification on CRISC, CDPSE, CGEIT, CompTIA Security is added advantage.
- Other Project and Change management certifications.
- 2 years of experience in Risk Management.
- 2 years of experience in IT risk audits in a major Financial or professional institution

NMB Bank Plc is an Equal Opportunity Employer. We are committed to creating a diverse environment and achieving a gender balanced workforce.
Female candidates and people living with disabilities are strongly encouraged to apply for this position.

NMB Bank Plc does not charge any fee in connection with the application or recruitment process. Should you receive a solicitation for the payment of a fee, please disregard it.

Only shortlisted candidates will be contacted.

Job opening date : 05-May-2025

Job closing date : 19-May-2025