Manager Payment System Support (Re-advertised) (1 Position(s))

Job Purpose:

To plan, organize and lead a team of Payments Systems Support Analyst to deliver cost effective and efficient ICT level 2 support services for all Payment Systems which are not Core Banking System To ensure that they meet and exceed business and customers' expectations (availability, recoverability, security and continuous improvement).

Main Responsibilities:

- Implement and co-ordinate an effective Payments systems support
- Plan, supervise, direct, reporting and administration of the second level support team(s) on issues pertaining to Payments systems.
- Supervise, implement, maintain and improve performance of all Payments systems
- Escalate incidents and problems to 3rd level support, follow-up & feedback on the progress made for resolution, conduct weekly meeting with Payments systems vendor to resolve all outstanding issues.
- Plan and conduct simulation of EOM and EOY runs in Collaboration with CBS team in order to eliminate any unforeseen incidents for successful completion of EOD/EOM/EOY batch runs.
- Maintain the Risk Register and controls policy frameworks for all Payments systems applications and ensure they are updated on an annual basis, engage Payments systems staff in Risk policy implementation
- Manage operational costs; perform cost-benefit and return on investment analyses for proposed solutions.
- Manage relationships with all vendors of Payments Systems and ensure effective routine and emergency maintenance of payment systems with no or very rarely downtime and interruption to business operations.
- Provide capacity planning statistics and periodic reports to aid in management decisions.

Knowledge and Skills:

- Payments Systems domain knowledge
- Banking operations.
- Regulatory knowledge in payment systems domain.
- Compliance (AML, Fraud, and sanction screening) knowledge in payment systems domain.

Qualifications and Experience:

- Bachelor's degree in computer science or equivalent qualification
- 5 years' experience in Payments Systems Support or Banking Operations

- Professional Certification in ITIL

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 : 06-Nov-2023
Job closing date : 20-Nov-2023

Senior Specialist Technology Risk; Cybersecurity, Data Analytics and Reporting (1 Position(s))

Job Location :

Head Office, Hq

Job Purpose:

To Ensure that risks related to cybersecurity within the bank are structurally managed so that the bank can make sound decisions in matters that affect the risk posture of the bank.
Manage risk data analytics, reporting and perform the oversight role as the primary contact between Technology Risk and other lines of defence within the bank.

Main Responsibilities:

Cybersecurity Risk Governance

- Using industry cybersecurity standards and frameworks, provide guidance on the governance of cybersecurity risk management at the bank.
- Oversee the establishment and management of cybersecurity risk-related policies and procedures that govern cybersecurity risk management for the bank.

Risk Identification, Assessment & Evaluation

- Drive and support the identification and assessment of cybersecurity threats to the bank's network and computer systems

- Ensure key cybersecurity risks have been adequately documented with relevant controls and key indicators.
- Define, in close co-operation and alignment with the first line, the Risk Appetite statement for cybersecurity within the bank.
- Support the 1LoD to ensure all relevant key cybersecurity risk information are properly and adequately maintained in the risk management system tool, check and validate the risk data quality in the system to support accurate reporting and decision making by management.
- Facilitate and support the 1LoD in conducting thorough risk assessments to evaluate their security, business practices and other factors that may pose risk to the bank.
- Ensure the business conducts Risk and Control Assessments (RCSAs) in accordance with guidelines issued by Operational Risk through training and conformance reviews, including osupporting (advice and guide) the 1st line in their risk and control activities and risk-return considerations (especially provide second-line opinions on new or significant change initiatives)
  oconstructively challenge performance of the first-line risk and control activities.
- Train the first line staff members to understand the defined controls and facilitate them in risk identification and assessment and in executing the controls and performing self-assessments to demonstrate their effectiveness.
- Review risk assessment and analyze the effectiveness of information security control activities, and report on them with actionable recommendations.
- Manage the oversight of cybersecurity risk on vulnerability assessments and penetration testing engagements.
- Serve in an advisory role in application development, major systems implementation projects, technology infrastructure projects etc. to assess relevant security risks requirements and controls; and ensure that security controls are implemented as planned.
- Continuously research and stay abreast of the new industry cybersecurity risks and recommend 1LoD on the respective controls that need to be implemented.
- Manage the oversight of the third-party cybersecurity risks identification and assessment.
- Using various risk management tools and technologies, accurately measure and report cybersecurity risks of the bank.

Risk Mitigation Strategies

- Support the cybersecurity team in the development and implementation of mitigation strategies.
- Ensure the cybersecurity teams have accurately implemented various security controls including but not limited to Firewalls, Endpoint Protection and Encryption capabilities.
- Ensure the cybersecurity teams have established effective response strategies to cybersecurity incidents.
- Develop and support the implementation of relevant cybersecurity frameworks, policies and procedures within the bank.
- Work with relevant teams to resolve security issues that are uncovered by various internal and third-party monitoring tools.
- Work with relevant bank vendors to ensure their products and services meet the banks security requirements

- Oversee and ensure staff are trained and educated on cybersecurity practices including acceptable internet usage, use and protection of logical access information and awareness on phishing and other cyber threats.
- Ensure that relevant new requirements from new policies are implemented and followed bank-wide, by interacting with the risk champions of each of the relevant teams and ensuring related controls are embedded in the banks risk and control framework.

Risk Monitoring

- Perform regular security testing and reviews to ensure bank systems are secure and that security measures are working as required.
- Follow up on the progress of actions that are relevant to improve the risk posture of the bank including risk and control remediation action plans, resulting from e.g.
  oRisk and control self-assessment activities;
  oRisk events such as security related risk incidents.
  oRelevant actions arising out of governance committees.
- Build an independent view on the cybersecurity risk posture of the bank by performing
  oIndependent validations of control assessment by the first line;
  oRisk-assessments on new and changed products, services and business,
  oTargeted investigations on specific topics of interest, depending on actual developments within or outside the organisation, in order to provide more clarity in a specific topic of interest.
- Ensure that cybersecurity risks are put on the meeting agenda of all relevant departments in the bank and contribute in the preparation of these meetings and attend in the meetings themselves when necessary.
- Follow up on monthly cybersecurity key risk indicator performance results and challenge the risk owners on unfavorable KRI results (amber and red KRI), establish root cause analysis and report on proper remediation plans to ensure risk levels remain within approved limits.

Risk Communication and Reporting

- Proactively communicate with the Head Technology Risk on cybersecurity and data analytics risk issues. Escalate significant events to relevant stakeholders as appropriate.
- Produce timely and accurate monthly and quarterly (and ad hoc) reports on cybersecurity and products automated systems controls risks exposure to governance committees.
- Report to management concerning residual risk, vulnerabilities, and other security exposures, including misuse of information assets and noncompliance.
- Follow up and gather relevant 1LoD reports for 2LoD view and voice-over for consideration in Technology Risk reporting.
- Plan and concisely prepare all Technology Risk required reports with determination on report objectives, scope and structure that include but not limited to Management and Board Technology Risk reports.
- Create well structured, concise, and clear reports based on data analyses, ensuring logical information organization, finding presentation and evidence-supported conclusions. Ensure the report adhere to the bank's style guidance and formatting requirements.
- Facilitate presentation of complex data in an accessible and understandable manner using data visualization that applies visual elements such as charts, graphs, infographics and tables.

- Ensure the accuracy, integrity and the reliability of the data and information presented in the reports.

Risk Data Analytics

- In consultation with relevant teams within the bank, identify areas that should be subject to risk data analytics and perform data extraction and analytics for those areas covering critical systems of the bank and report findings to RCC and EXCO on month basis.
- Research, recommend and implement relevant data analytics and risk management tools to aid in data analysis and risk management activities.
- Examine and interpret data to identify risk patterns, trends and insights.
- Assess the adequacy and effectiveness of key product related application controls and provide assurance on the risk exposure levels.
- Prepare standard scripts for data analytics for application control testing and all critical systems in the bank, foster the use of robotics in automating the risk data analytics tasks for timely risk exceptions reports.
- Provide data related issue closure validations and assurance for closed risk actions in governance committees within the bank.
- Maintain a database of identified risks and tests to be carried in data analytics from the bank's systems across the network.

Oversight and Coordination

- Serve as the primary contact with the 1LoD and the business stakeholders for streamlined communication with Technology Risk.
- Support and challenge the 1LoD in their risk related activities by managing a streamlined communication with risk champions and risk owners.
- Organize and coordinate meetings between Technology Risk and relevant stakeholders within the bank.
- Collaborate with ICT management and risk champions in the identification, evaluations, reporting and management of their risks, ensuring they are fully aligned with the ERM framework and other relevant policies and procedures of the bank and regulatory requirements.
- Coordinate all interactions between ICT, the business and Technology Risk ensuring availability of information from either direction.
- Facilitate and coordinate communication with internal and external auditors for all matters on Technology Risk.
- Facilitate the identification and correction of risk defective business processes.

Knowledge and Skills:

- Knowledge of security issues, techniques, and implications across all existing computer platforms.
- A practical knowledge and understanding of risks, controls, risk management tools and methodologies.
- Mastery in using data analytics tools such as ACL.
- Cybersecurity frameworks such as ISO/IEC 27001, NIST Cybersecurity Framework (CSF) and CIS Critical Security Controls.
- In-depth understanding of ISO/IEC 2007 Information Security Risk Management.

- Risk & control techniques; Facilitation skills
- High personal credibility and integrity.
- Understanding of database systems such as MongoDB, MySQL, SQL server, Oracle and/or PostgreSQL.
- Ability to use tools for vulnerability management, security monitoring, access & identity management, non-personal/privileged account management and/or multi-factor authentication.
- Ability to use risk management tools, analytical and problem-solving skills
- Team player
- Good written and verbal communication skills
- Time management - ability to juggle priorities and execute at speed individually and as part of a team.

Qualifications and Experience:

- Holder of University Degree in Computer Science, Information Systems or other related field
- Holder of an active professional certification in Information Security including at least one of the following CISSP, CISM or OCSP.
- 3 years of combined IT and security work experience with a broad range of exposure to systems analysis, application development, database design and administration
- Previous risk management experience gained within an auditing, operational risk management or compliance/controls type role.
- Understanding of the core retail and commercial banking product set.

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 : 03-Nov-2023

Job closing date : 17-Nov-2023

To Apply **CLICK HERE**