Payments Network Malaysia Sdn Bhd
200801035403 (836743-D)

Job Description	
Position	Principal Risk Specialist (IT and Cyber Risk)
Department	Risk Management
Division	Risk & Compliance Management

SUMMARY OF RESPONSIBILITIES

- To lead the implementation and continuous improvements in the areas of Cyber Risk Framework, IT Risk Management and Data Protection, including any other new areas that will be set up to meet business strategy and organisational needs.

- To collaborate with Business and ISD in ensuring that risks are identified and considered in the development of PayNet's strategic vision, and proactively manage to balance both the risk and rewards of the business.

- Coordinate and review risk assessments, identify the operational and strategic risks, facilitate the prioritisation of risks and identification of risk owners, and develop and communicate risk reports to the Management and Risk, Board Committee.

KEY AREAS OF RESPONSIBILITIES

1. IT Risk Management and Data Protection

- Review IT risk related assessments including but not limited to Change Request Risk Assessment (CRRA), Project Risk Assessment (PRA), Risk and Control Self Assessments (RCSA), exceptions requests to established IT policies and procedures
- Review, improve and implement enterprise-wide data leakage prevention strategies and processes and compliance to regulator requirements including but not limited to BNM Management of Customer Information and Permitted Disclosure (MCIPD), Financial Services Act (FSA), Risk Management in Technology (RMiT) and etc
- Provide consultations and level 2 reviews to Business and ISD on areas relating to IT risk, cyber resilience and data protection
- Recommend improvements and mitigations on current systems, policies and strategies and take the necessary actions to mitigate IT, cyber and data protection related risks
- Perform special reviews on regulators' requirements and or as required by the Management, GARC and BOD

2. Cyber Risk Framework

- Perform regular Participants' cyber resilience monitoring i.e. ensure timely and complete submission of the compliance reports and mitigations action plan updates by all Participants
- Report on Participants cyber resilience to PayNet's Group Management Committee (PGMC), Group Audit Risk Committee (GARC), Group Board Rules Committee (GBRC) and Board of Directors (BOD)

- Review and update existing as necessary PayNet's cyber resilience controls, including but not limited to the following:
  - PayNet's Cyber Resilience Framework
  - Cyber Resilience Guidelines for Participants of PayNet's Services
  - Participants monitoring process and procedures
  - Data protection policies, processes and procedures

3. On-boarding Due Diligence and Continuous Assessments

- Perform on-boarding due diligence on prospective third-party acquirers (TPA) and Non-Bank Participants (NBP). The on-boarding processes include but not limited to pre-admission assessment, interview, off-site due-diligence, on-site due-diligence and system audit review
- Perform review on system audit report submitted by the TPA and NBP

4. Perform Overall Risk Management Department Operational Functions

- Maintain relevant documentations for audit and inspection
- Maintain a close working relationship with the all large value and retail payments product owners with respect to IT, cyber and data protection matters
- Inculcate organisation-wide culture i.e. risk awareness and management
- Keep abreast with the latest risk management practices and/or standards and proactively adapt these practices and/or standards where appropriate
- Perform any other assignments as directed by the Risk Manager, Head of Risk Management and/or Director of Risk & Compliance

QUALIFICATIONS

Minimum Qualifications

- Degree in Information Technology (IT), Computer Science or other related discipline
- 6 or more years of working experience in IT, cyber security, risk management, internal or external audit
- Good interpersonal and communications skills (both verbal and written) in English and Bahasa Malaysia

Additional requirements

- Experience in regulatory requirements such as BNM GPIS, ISO27001, MAS Technology Risk Management Guidelines, National Institute of Standards and Technology (NIST), Centre for Internet Security (CIS), FMI Cyber Resilience Guidelines or equivalent would be an added advantage
- Understanding of IT security and operations and how IT interfaces with business, risk management and compliance processes would be an advantage
- Relevant professional certifications such as CISA, CISSP, CEH, GPEN, CISM, ISO27001 auditor would be an advantage
- Demonstrate effective working knowledge and understanding of the PayNet products, with the ability to apply said knowledge for effective and efficient execution of the assignments
- Demonstrate ability to effectively apply knowledge of Project Management for efficient execution and management of assigned tasks
- Acts as an agent of change and stimulates others to change. Paves the way for needed changes; by taking calculated risks to derive maximum benefit
- Strong conceptual, strategic and analytical thinking skills
- Good written, presentation and communication skills; able to prepare statistical and narrative reports
- Must be flexible and be able to participate in multiple projects simultaneously
- Able to work under broad direction but is a self-motivated individual who is able to work independently. Has technical responsibility and accountability for work performed and decisions taken
- Must possess excellent interpersonal skills and able to communicate and manage relationship at all levels with business users, financial institutions, vendors as well as team members.