Job Description	
Position	Principal Information Security Specialist
Department	CISO Office
Division	Risk & Compliance

SUMMARY OF RESPONSIBILITIES

1. Drive the execution of PayNet's cyber security/information security strategy via an appropriate management forum to achieve cyber security vision and target security capabilities.
2. Review and maintain the strategy to be consistent with overall business direction and in line with PayNet's peers in related cyber security requirements across the industry
3. Establish and enforce directive controls, validate internal detective and preventive security controls.
4. Work together with relevant stakeholders to assess technology risk considering relevant controls.
5. Coordinate and maintain security governance implementation and certification e.g., PCI DSS, ISMS etc which includes collation and analysis of relevant security measures and reporting and monitoring of compliance by PayNet to BNM regulatory requirements such as Risk Management in Technology Guidelines and PayNet's internal IT related policies
6. Drive risk and security aware culture/behavior internally by several key initiatives including targeted information security awareness training program for all employees, contractors, and service providers, and establish metrics to measure the effectiveness of this program for different audiences.
7. Establish continuity on the implementation and monitoring of technical and organizational controls for Data Protection as part of Personal Data Protection requirement (PDPA) as well as complying to the Management of Customer Information and Permitted Disclosures Guidelines issued by BNM. This includes deployment, management and monitoring to safeguard data and manage insider threats via PayNet's Data Loss Protection system and other relevant solutions.
8. Perform any other ad-hoc assignments that is instructed by the management of Risk & Compliance that may be given from time to time

KEY REQUIREMENTS

1. Understanding of cyber security covering both internal PayNet and external payments eco-system.
2. Experience related to information security strategy planning, security architecture design and review.
3. Effective communication, collaboration and presentation skills. Ability to explain complex concepts in plain language and graphics.

KEY AREAS OF RESPONSIBILITIES

1. Coordinate and plan work packages for security governance, risk, compliance and project execution for team members within the department.
2. Provide expert input into the collective information security strategy to ensure that future security investments are aligned appropriately when considering key priorities such as business requirements, industry threat landscape, and risk appetite.

3. Maintain regular engagement and proactive partnership with business and technology teams to ensure cyber/information security strategies align with business and technical needs, requirements, and constraints.
4. Define and maintain security capability catalogues and roadmap to support the information security strategy agenda.
5. Analyse market and industry trends and adjust security strategy accordingly
6. Monitors current and proposed laws, regulations, industry standards, and ethical requirements related to information security and privacy, so that PayNet is warned in advance and ready to be fully compliant with these requirements.
7. Designs, develops, delivers, or oversees the delivery of information security awareness programs (videos, memos, computer-based training, etc.) delivered to users, technical staff, management and relevant third-party personnel.
8. Conceives and proposes new approaches that will allow greater standardization and more effective management of security measures including adoption of automated tools.
9. Participates in periodic information systems risk assessments including those associated with the development of new or significantly enhanced business applications.
10. Establish and fine-tune security governance, risk and compliance metrics, then on develop routine reports in accordance with the metrics.
11. Prepares and periodically updates draft information security policies, architectures, standards, and/or other technical requirement documents needed to advance information security at PayNet.
12. Build IT Compliance competencies and capabilities for the Security Oversight team in understanding, manifesting, governing and conforming to industry standards such as ISMS, PCIDSS, RMIT etc.
13. Work closely and increase cross collaborations between Cyber Intelligence & Threat Response, Security Oversight and IT Risk Team to foster greater and effective collaborations in Cyber and IT related matters.
14. Perform or support any tasks related to the function of the Department as assigned by Director of Risk and Compliance or CISO which may arise from time to time

QUALIFICATIONS

TECHNICAL COMPETENCIES

- Practical understanding on industry frameworks for cyber / information security such as National Institute of Standards and Technology (NIST) Cyber Security Framework, COBIT, Information Security Management System (ISMS), Payment Card Industry Data Security Standard (PCI DSS) and Bank Negara Malaysia's Risk Management in Information Technology (RMiT);
- Thorough understanding of end-to-end IT operations and how IT interfaces with business, risk management and compliance processes and IT Security
- Demonstrate understanding of defense in depth concepts and supporting security technologies, including but not limited to: endpoint protection, network access control, remote access VPN, file integrity monitoring, firewalls, IDS/IPS, SIEM, application security controls, identity management / federated identity services and public key infrastructure.
- Prior experience developing and implementing security solutions.
- Demonstrate knowledge of threat actor Tactics, Technique, and Procedures (TTPs) as well as corresponding mitigation/disruption techniques.
- Prior experience securing public cloud environments (AWS, Azure)
- Demonstrate expertise with addressing zero-day threats, intrusions, malware infection and experience with packet analysis.

MINIMUM QUALIFICATIONS

1. Degree in Information Technology (IT), Computer Science or other related discipline with relevant experience in managing cyber risk in financial market infrastructures, critical national infrastructure, military, security intelligence or equivalent
2. Cyber security expert with 5 to 7 years or more hands-on experience
3. Professional certification such as CISM, CISA, CISSP or equivalent

ADDITIONAL REQUIREMENTS

- Excellent interpersonal, facilitation, and leadership skills along with effective communication (both written and verbal) skills.
- Strong history of external engagement with industry peers, working groups, and cybersecurity communities globally.