**Specialist: Governance, Risk & Controls**

**Key Accountabilities of the GRC Specialist role:**

**Role purpose:**

* Defining Cyber Governance, Risk & Compliance in order to:
* To lead ongoing evaluation of security policies, relevant standards and supporting the continuous improvement of the security governance program
* To ensure that comprehensive Information Security Risk management programs are established.
* Ensure the alignment of Information Security Risk management with the enterprise risk management framework.
* To lead in the risk management of cyber security risks while collaborating with other departments to identify, recommend, develop, implement, and support a risk-informed decision and action framework
* To provide Management with assurance covering controls across the Business environments that there are adequately designed and operating effectively
* To support Management during audits as well as implement and track Management audit actions to closure
* Assist in the management and rollout of cyber Training & Awareness initiatives
* Provide Management with status update reports as well as insight reporting

**Key accountabilities and decision ownership:**

* Take a proactive approach to ongoing evaluation of cyber security policies to ensure security policy adherence
* Promote awareness of security policies, training, and the governance strategy amongst all levels of the organization to ensure sound security governance is reflected across the organization
* Assess policy needs, train stakeholders in the policy lifecycle and clearly communicate expectations, collaborate with stakeholders from subject matter experts to senior leaders to develop and manage security content
* Maintain and further develop the Cyber Risk Management Program
* Actively manage risks on the Cyber Risk Register from intake to resolution
* Communicate risk assessment findings with key stakeholders to develop and monitor risk remediation plans
* Develop cyber risk portfolios to provide a more holistic view of teams’ risks
* Conduct regular compliance assessments with the Business to ensure that current and emerging risks are being monitored and managed
* Proactive Control design and implementation guidance provided to the Business
* Process and Control Compliance Monitoring and Reporting
* Cyber audit SPOC to the business with guidance on all audit submissions
* Cyber audit report reviews and guidance to Management on the recommended actions
* Tracking and monitoring of audit remediation action implementation
* Deploying cyber security awareness training collateral with innovative approaches
* Design of status reports as well as insight reporting as and when required by Management
* Lead reporting development with the use of automation and reporting tools to generate Cyber Risk metrics, i.e. KPI’s, KRI’s, KGI’s (KxI)

**Qualifications and Experience:**

* 3-year Technical Diploma/Degree in Information Security, Computer Science or Engineering
* 3 years of experience