POSITION DESCRIPTION

Position title:	**IT Governance, Risk and Compliance Analyst**
Location:	**Head Office**
Reports to:	Information Security Manager
Entities:	GMHBA
Organisational level:	Technical Specialist
Reports:	Nil

Job Purpose:

To ensure appropriate testing and ongoing adherence of internal IT security and risk controls is undertaken, and to make recommendations for addressing gaps or developing remediation plans. Develop and review IT Security policies and associated training materials.

Accountabilities:

Policy Development:

- Assist in the development and communication of IT compliance standards and guidelines and provide input into GMHBA-wide policies.
- Conduct reviews of existing information IT security policies, risk processes and documentation, and make recommendations for remediation where required.
- Ensure that all issues and findings across all IT compliance related activities are documented and tracked for remediation, with direct involvement by either facilitation of discussions, or by being directly involved in the process.
- Evaluate general and specific training needs associated with IT security policies.

Compliance

- Provide central oversight to deliver consistency and quality in compliance work across GMHBA – all IT functions and capabilities.
- Measure adherence to ITSG policies.
- Review activities associated with the implementation of previously identified mitigation strategies.

IT Information Security

- Publish corporate ISMS policies and procedures and communicate changes.
- Contribute to continuous improvement of the internal control framework, including the decision-making processes around information security and usability.
- Collaborate with key stakeholders to ensure appropriate remediation planning exists across a range of IT related issues, including disaster recovery, security risks, user access, data protection etc.
- Serve as a subject matter expert on key internal controls, procedures and workflow.

- Drive increased awareness of information security amongst users, working closely with the People and Culture team
- Conduct Threat Risk Assessment in conjunction with the IT Team and updating and maintain the ITSG Operational Risk Register.
- Develop and monitor mitigation strategies for identified risks.
- Develop site-specific policies and procedures in support of the ISMS implementation.

Regulatory and Reporting

- Ensure compliance with the Company's Delegated Authorities, Business Plan, Policies and Standards.
- Keep up to date with regulatory trends and changes, and ensure the company anticipates and navigates changes successfully.

Stakeholders & Advice

- Provide expert advice and recommendations to key stakeholders to facilitate understanding for robust decision making.
- Take opportunities to maintain positive and constructive relationships with regulators, auditors and other external stakeholders.

Other

- Participate in the design, build and roll-out of business change programs designed to strengthen GMHBA's performance
- Embrace the mindset and actively contribute towards embedding the GMHBA Way including working in an Agile environment.
- It is not the intention of this position description to limit the scope or accountabilities of the position but to highlight the most important aspects of the position.
- The accountabilities described within may be altered in accordance with the changing requirements of the role.
- Perform 1st Line of Defence duties by identifying operational risks, investigating their root causes and provide support to mitigate risk through understanding control effectiveness and recommending risk improvement.

Key Relationships:

Internal:

- Information Security Manager
- IT Services Group
- Governance Risk and Compliance team
- People and Culture team
- ITSG Leadership Team

External:

- Auditors
- External consultants and service providers as required
- External Information Security public forums

Skills, Experience and Qualifications:

Mandatory

- IT security and risk experience within a regulatory, internal audit or compliance environment.
- Experience with the development of general controls and/or IT compliance related standards.
- Working knowledge and exposure of IT Governance, Risk and Compliance practices.
- Strong technical and analytical aptitude.

Highly desirable

- Experience in private health insurance
- Experience in developing and rolling out information security compliance programs using ISO 27001
- Experience in developing and rolling out PCI DSS compliance programs
- Certified Information Security Manager (CISM) Certification
- Certified Information System Security Professional (CISSP) Certification