Job Description – Information Security GRC Specialist

Department	Information Security
Grade	13
Reporting to	Information Security GRC Manager
Direct reports (yes or no)	No
WTW Code	

Job purpose

As a member of the Information Security - Governance Risk and Compliance team, you will maintain the confidentiality, integrity and availability of MIB's information and information systems. This will primarily be achieved through identification and recommendation of risk mitigation treatment plans and through the ongoing assessment of the efficacy of controls.

You will support the alignment of the Information Security Strategy with business objectives, drive continual improvement, and act as a subject matter expert for security matters.

This will be delivered by:

- Supporting the ongoing alignment of the Information Security Strategy to business objectives
- Cultivating Best Practices: Establish and promote a clear vision of "what good looks like" for technology risk and controls
- Maintaining robust governance processes in the delivery of MIB's Information Security responsibilities
- Operating an effective Information Security Risk Management capability that assesses and where possible supports through communication, education awareness and other activities, the reduction of risk to an acceptable level. Ensure clarity, consistency, and alignment with regulatory, legal, and industry standards (e.g., NIST, ISO 27000, COBIT)
- Implementing and operating an ongoing Information Security Compliance Programme that delivers assurance of control performance and seeks to uplift and transform technology controls, ensuring they are robust, clearly understood, effective, and future-ready.
- Ensuring that the ongoing compliance of baseline industry security standards such as ISO27001/2 are met
- Providing effective assurance through the auditing and assessment of MIB's controls against control frameworks
- Being the first point of contact for Information Security expertise for internal stakeholders. Partner with product, engineering, business, and control owning teams to undertake annual risk and control assessment, agreement of control standards and receiving and responding to

Job purpose

challenge, embedding best practices, facilitate collaboration, and drive adoption of frameworks and standards.

- Facilitating a process of continual improvement in the delivery of Information Security services to MIB

Key accountabilities

Governance

- Support the GRC Manager with the implementation, of the agreed Information Security Strategy
- Develop and review the Information Security Management System (ISMS)
- Create, deliver and maintain an ongoing Information Security Awareness Programme in line with direction from the Information Security GRC Manager
- Ensure Information Security policies, procedures and standards are accessible, communicated and understood by Staff, Contractors, Client Companies and Vendors and reviewed in line with established annual cadence.
- Establish mechanisms, behaviours and culture to encourage the protection of MIB information and information systems. Foster a culture of operational excellence and innovation, driving ongoing enhancement of risk management practices and frameworks.
- Attendance of relevant governance groups (where required) within MIB to ensure complete, transparent and effective risk management is delivered
- Assist in the production of governance, reporting, and issue management for controls and frameworks, feeding directly into the MIB Enterprise Risk Management framework governance structure, including quarterly risk reporting, risk appetite metrics, KRIs and thematic reporting as required by ESSG, ARC and ExCo Establish and maintain a community of Information Security 'Champions' throughout the organisation
- Act as an Information Security subject matter expert (SME) to the business

Risk

- Assist in the management and maintenance of the Information Security Risk Register, ensuring risks are actively identified and managed or exemptions are approved and recorded.
- Ensuring that Information Security risk governance and control frameworks are maintained and that risks/issues are reported and escalated appropriately.
- Completion of Information Security risk assessments and workshops.
- Support the Information Security Incident Response Process as required
- Support the Third Party Risk Management Process (TPRM) including the Information Security Assessment of both prospective and existing third parties.
- Oversee the administrative aspects of Penetration Testing across the MIB estate, including stakeholder engagement, Pen testing organisation, the recording of findings and tracking of remediation efforts.
- Assist in ensuring the consistency and quality of risk assessments performed across the ODT function, setting standards and providing guidance to the ODT functional leaders

Key accountabilities

- Assess and appropriately catergorise any vulnerabilities that may damage the confidentiality, integrity or availability of MIB information or information systems

Compliance

- Work with all teams to track requirements and compliance with relevant Legislation, Regulations, Standards and Frameworks as they pertain to Information Security
- Collation and tracking of Information Security and ODT audit matters, including the review of audit findings, agreement of remediation plans, and tracking of actions through to closure.
- Ensure compliance is maintained with our critical security compliance certification of ISO27001
- Measure the performance and compliance of key MIB controls
- Assist in the development, implementation and maintenance of a rolling 12-month compliance schedule

Role requirements

- The job holder must have a thorough understanding of the Information security Frameworks, Risk Management Methodologies and the creation and maintenance of Information Security Management Systems.
- 3 to 5 years of relevant experience for this role ideally in the insurance sector.
- Experience in effective collaboration, co-creation, coaching and education to support colleagues at all levels across a business.
- Experience in writing Information Security policies, procedures and standards
- Experience in maintaining all aspects of ISO27001/2 compliance
- Working knowledge of standard risk management/control frameworks such as ISF, NIST, ISO and ITIL.
- Excellent written and oral communication skills
- Able to present Security in 'non-technical' business-friendly accessible language and engage effectively with all related stakeholders.
- Ability to effectively prioritise and execute tasks in a high-pressure environment

One or more of the following qualifications are highly desirable.

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Risk and Information Systems Control (CRISC)