Job Description – InfoSec GRC Specialist

Department	IS, Information Security
Grade	13
Reporting to	InfoSec GRC Manager
Direct reports (yes or no)	Yes
WTW Code	AFY637P3 12

Job Purpose

As a member of the Information Security - Governance Risk and Compliance team (InfoSec GRC), you will maintain the confidentiality, availability and integrity of MIB's information and information systems. This will primarily be achieved through identification and recommendation of risk mitigation treatment plans and as a subject matter specialist to support the needs of the organisation.

This will be delivered by:

- Supporting the ongoing alignment of Information Security strategy to business objectives
- Maintaining a robust governance processes in the delivery of MIB's Information security responsibilities
- Operating an effective information security risk management capability that assess and reduces risk to an acceptable level
- Implementing and operating an ongoing information security compliance programme that delivers assurance of control performance
- Ensuring the ongoing compliance of baseline industry security standards such as ISO27001/2 are met
- Providing effective assurance of MIB's controls and control frameworks
- Providing a focal point within for information security expertise

Key accountabilities

Governance

- Support the GRC Manager with the development, alignment of an Information Security Strategy
- Development, review and alignment of Information Security Policy
- Create, deliver and maintain and ongoing information security awareness programme
- Ensure InfoSec policies, procedures and standards are accessible, communicated and understood by staff, contractors and vendors. Where required this will include delivering training
- Attendance of relevant governance groups within MIB to ensure complete, transparent and effective risk management is delivered
- Producing management information (Dashboard) that clearly reflects MIB's information security risk profile
- Establish and maintain a community of Information Security 'Champions' throughout the organisation
- Act as an Information Security subject matter specialist to the business
- Establish mechanisms, behaviours and culture to encourage the protection of MIB information and information systems

Risk

- Management and maintenance of the ISS Risk Register, ensuring risks are actively identified and managed or exemptions are approved and recorded.
- Completion of InfoSec risk assessments and workshops.
- Ensuring that InfoSec risk governance and control frameworks are maintained and that risks/issues are reported and escalated appropriately.
- Review, challenge and track the implementation and effectiveness of controls and risk mitigation treatment plans as a result of a risk assessment
- Ensure appropriate management focus for any vulnerability that could damage the confidentiality, integrity or availability of MIB information or information systems.
- Track and record information security incidents and to ensure risk mitigation controls are appropriate and proportionate and that exposure is minimized.
- Support the Information Security Incident response process as required
- Facilitate a process of continuous improvement in the delivery of information security services to MIB

Compliance

- To work with all teams to track requirements and compliance with relevant Legislation, Regulations, Standards and Frameworks as they pertain to Information Security
- Ensure compliance is maintained with our critical security compliance certification of ISO27001

Key accountabilities

- Measure the performance and compliance of key MIB controls which include (but are not limited to):
  - MIB information security policies
  - Delivery governance gateways
  - Technical controls
- Develop, implement and maintain a rolling 12-month compliance schedule

Role requirements

- The jobholder must have a thorough understanding of the Information security threat landscape, significant risks, technical developments and strategies
- Extensive experience in the IT marketplace, as a security practitioner
- Experience and knowledge of leading information security risk assessments
- Proven 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.
- Demonstrable experience in creating a sustainable compliance capability
- Excellent written and oral communication skills
- Able to present risk in 'non-technical' business-friendly accessible language
- Ability to effectively prioritise and execute tasks in a high-pressure environment

One or more of the following qualifications are highly desirable.

- o Certified Information Systems Security Professional (CISSP)
- o Certified Information systems Auditor (CISA)
- o Certified Risk and Information Systems Control (CRISC)