Job Description – Client Company Information Security Manager

Department	Information Security
Work level	3
Reporting to	Head of Information Security
Direct reports (yes or no)	No
WTW Code	

Job purpose

The Client Company Information Security Manager is responsible for providing specialist information security guidance, oversight, assurance and project support to MIB's client companies. The role helps client companies understand, develop and maintain proportionate information security policies, standards, procedures and control frameworks that support their own contractual and business requirements.

This role provides support and specialist guidance to the client companies, ensuring that information security responsibilities, risks and control expectations are clearly understood, consistently managed and embedded into day-to-day client company operations.

The Client Company Information Security Manager will act as a subject matter expert for the client companies, supporting them to protect the confidentiality, integrity and availability of their own information and information systems. The role is advisory and assurance-focused and does not own or manage MIB's internal information security controls. This will be achieved by:

- Providing a focal point within MIB for client company information security guidance, assurance and subject matter expertise.
- Supporting the alignment of client company information security activity to agreed client company objectives and obligations.
- Supporting an effective information security risk management approach for client companies, helping assess information security risks, agree proportionate treatment plans and track progress to closure.

Key accountabilities

General

- Support the Head of Information Security and the Information Security GRC Manager by providing client company insight to inform the wider security strategy where relevant.
- Share knowledge, guidance and good practice with colleagues supporting client company information security activity.
- Work with Security Operations, Engineering and Architecture functions to ensure client company requirements are understood and appropriately reflected in advice, assurance and control recommendations.
- Provide client company teams with security-focused support, training and consultancy to help them understand and meet applicable security standards, policies and legislation.
- Engage with ODT leadership, supporting functions and business stakeholders to support the delivery of effective information security practices within client companies.
- Produce and share management information on the performance of client company information security controls, providing assurance on maturity, risk exposure and control effectiveness.
- Recommend improvements to client company information security standards, guidance and control expectations through continuous improvement activity.
- Develop and maintain procedures and guidance that help client companies understand and respond to relevant threats and vulnerabilities.
- Support client companies to embed appropriate information security behaviours and practices that help protect their information and information systems.
- Review and advise on information security clauses, obligations and controls within client company contracts.
- Keep up to date with emerging trends, technologies and legislation relevant to client company information security and assurance.

Key Role Requirements

- Act as the client company point of contact for information security governance, risk, assurance and compliance matters.
- Support client company governance forums by providing clear reporting, insight and challenge on key information security risks, audit outcomes, control maturity and remediation progress.
- Support the development, review and alignment of client company information security policies, standards, procedures and guidance.
- Maintain a proportionate client company information security risk and compliance approach, including information security risk assessments, treatment plans, escalation, tracking and a rolling compliance schedule.

Key accountabilities

- Review, challenge and track client company control actions, vulnerabilities and information security incidents to ensure appropriate mitigation and management focus.
- Coordinate client company audit and assurance activity, including audit readiness, evidence quality, audit findings, remediation plans and action closure.
- Measure and report on the performance and compliance of key client company information security controls, including policy, process and relevant technical control expectations.
- Support client company initiatives, solutions and services where information security advice, assurance or oversight is required.

Role requirements

- A thorough understanding of the information security threat landscape, significant risks, technical developments and regulatory expectations as they apply to client company environments.
- Strong interpersonal and stakeholder management skills are essential, as the role must influence and support client company teams and stakeholders without direct ownership of their operational delivery.
- Extensive experience as an information security practitioner, ideally within a complex supplier, client or multi-stakeholder environment.
- Direct experience of supporting information security governance, risk and compliance activity in a stakeholder-facing or advisory capacity.
- Experience and knowledge of supporting information security risk assessments, including review, challenge and assurance of risk treatment plans.
- Proven experience of developing or supporting information security policies, procedures, standards and guidance.
- Experience supporting ISO27001-aligned controls, assurance activity or equivalent information security frameworks.
- Ability to harness the commitment and contribution of colleagues outside the direct span of control.
- Excellent written and oral communication skills.
- Ability to research, assess and recommend improvements to governance, risk and compliance capabilities and maturity.
- Ability to present ideas in non-technical, business-friendly and accessible language.
- Ability to effectively prioritise and execute tasks in a high-pressure environment.

Role requirements

Qualifications

One or more of the following qualifications are highly desirable:

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in the Governance of Enterprise IT (CGEIT)