|  |  |  |  |
| --- | --- | --- | --- |
| **Role title:** | Information Security Manager | **Responsible to:** | Chief Information Security Officer |
| **Division:** | Member Experience, Digital and Data | **Department:** | Information Security  |
| **Direct Reports and Level:** | 3 Direct reports (Information Security Analysts) | **Scope:** | Information Security Governance, risk, compliance and control frameworks across the MPS Group (MPS) |
| **Scale:** | 3 PeopleNo BudgetN/A income |
| **Regulated Function(s) Held:** | No |
| **Evaluation Level** | tbc | **Role Family** | Digital, Data and Change  |

|  |
| --- |
| **Overall Role Purpose** |
| The Information Security Manager is responsible for overseeing governance, risk and compliance activities within the domain of information security, as part of the wider Information Security function. This role will ensure effective operation of the information security management system that ensures the appropriate policies, controls and assurance procedures are in place across MPS to manage the key cyber, information security and privacy risks in line with industry best practise and frameworks.Where relevant, the manager and team will also operate a number of these controls, as well as measure effectiveness, identify gaps and drive remediation actions as needed. The manager will also support the Chief Information Security Officer in developing and driving information security strategy, and to drive education, awareness and information security culture across the organisation. |

|  |  |
| --- | --- |
| **Accountabilities (RACI)** | **Measures of Success/KPI’s** |
| **Operational Leadership*** Provide leadership across the MEDD Division and the Information Security team to deliver on the overall 2025 goals, business performance, leadership of teams that reinforces the desired culture and delivery of MPS strategic priorities.
* Contribute to the development and delivery of the MEDD strategy to plan, cost and quality
* Implement, maintain and continually improve the information security management system and associated processes
* Support and enable delivery of projects within the Information Security Programme
 | * Corporate Strategic priorities Vs plan
* Division Plan delivery Vs plan
* Delivery of projects to plan
* Stakeholder Feedback
 |
| **Financial*** Recommend solutions which deliver security enhancements that improve the services to our members and ensures business cases supports the desired strategic outcomes.
* Identify and report accurate information security risks and enable resolution to the issues identified across MPS to mitigate impact on MPS, members and colleagues
 | * Operational budget Vs Plan
* Project Quotes v actual cost at end of project
 |
| **Member*** Ensure identification of threats and risks to member or client information, highlighting and facilitating remediation plans as required
* Provide due diligence over supplier and outsourcing arrangements to protect member data handled by our data processors
* Monitor for and provide robust challenge of emerging risks and issues arising from business activities which fail to deliver appropriate and consistent outcomes for members
 | * Net promoter score
* Member feedback
* Member Experience Scores
 |
| **People**  * Provide leadership to deliver exceptional training, competence, performance and engagement of the operational security team ensuring clarity of the team’s accountabilities and compliance to all governance, policy, standards and procedures
* Contribute to a strong pipeline of talent and succession across MEDD for the benefit of MPS which will mitigate workforce planning risks and maximises the performance and potential of colleagues.
* Maintain an ongoing education and awareness programme across the business
* Support the continual education and enhancement of risk and control culture across MEDD and the wider organisation
* Promote an inclusive environment, which aligns with our commitment to celebrate and promote diversity.
 | * MEDD Engagement Index Vs MPS
* MEDD Leadership Index Vs MPS
* MEDD Inclusion Index vs MPS
* Strong Talent and Succession Plan
* HR Metrics – attrition, absence

  |
| **Risk*** Maintain risk management processes in conjunction with the 2nd Line risk function, inline with the Information Security Management System
* Produce regular risk reports and key risk indicators to support management reporting and reporting upwards to the audit and risk committee
* Identify and report risks and issues identified within MEDD and potentially across MPS to enable resolution and mitigation of potential impact on MPS, members and colleagues.
 | * Risk & Control Self- Assessments
* Audit Actions
* Improved awareness and understanding of risk management
* Risk reporting is accurate
* Business areas risks being actively reviewed and challenged
 |

|  |
| --- |
| **Responsibilities (RACI)** |
| * Manage the information security policy framework and associated standards
* Maintain an effective ISMS and control framework
* Oversee information risk management, control exception & remediation processes
* Deliver the supplier risk management process
* Ensure appropriate assurance over technology projects and specification of security requirements
* Maintain the ongoing training and awareness programme
* Ensure correct operation of security controls owned within the team as required
* Support privacy processes and procedures in conjunction with general counsel and data privacy champions
 |

|  |
| --- |
| **Key Governance Responsibilities** |
| * Produce reporting that will be utilised at the Executive and the Council.
* Member of Operational Risk Committee
* Member of Programme Change Boards
 |

|  |  |
| --- | --- |
| **Leadership Framework Competencies** | **Level** |
| Fresh Thinking | Leading Others |
| Building Capability in Self and Others | Leading Others |
| Influencing Others | Leading Others |
| Collaborating for Results | Leading Others |
| Leading Self and Others | Leading Others |
| Commercial and Risk Thinking  | Leading Others |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Knowledge and Qualifications** | **Skills** | **Experience** |
| **Essential** | * Understanding of the cyber security risks associated with various technologies and ways to manage them
* Knowledge of security domains, auditing standards and frameworks, and risk analysis frameworks including ISO 27001, Cyber Essentials, PCI DSS etc
* In-depth knowledge of global technological trends and developments in information security and risk management.
 | * Verbal communication skills, including presentation skills, with an ability to communicate with a range of technical and non-technical team members and other relevant individuals
* Written communication skills, for example to write technical reports
* Excellent attention to detail, analytical skills and an ability to analyse complex technical information in order to identify patterns and trends
* An ability to work under pressure, particularly when dealing with threats and at times of high demand.

  | * Experience of working in an information security role, working with all technical, governance, risk and compliance aspects
* Significant experience of ISO 27001 (Information Security Management System – ISMS)
* Experience of General Data Protection Regulation
* Experience of risk management frameworks and methodologies
* Experience of writing and introducing effective information security and compliance policies/standards.
* In depth understanding of security concepts and ability to articulate these to technical and non- technical audiences
 |
| **Desirable** | * Certified Information Systems Security Professional (CISSP)
* Certified Information Security Manager (CISM)
* Certified Information Security Auditor (CISA)
 | * Experience of leading teams and coaching others
 | * Experience of assurance end to end technical projects from design to implementation
* Experience of privileged access/account management
* 3rd party assurance and Information Security assessments
* Experience of disaster recovery planning
* Experience of Payment Card Industry Data Security Standard (PCI DSS)
* Solid understanding of network and infrastructure security best practice
 |