|  |  |  |  |
| --- | --- | --- | --- |
| **Role title:** | Information Security Analyst | **Responsible to:** | Information Security Manager |
| **Division:** | Digital & Change | **Department:** | Digital & Change |
| **Direct Reports and Level:** | No direct reports  | **Scope:** | Information Security Governance, risk, compliance and control frameworks across the MPS Group (MPS) |
| **Scale:** | N/A PeopleN/A BudgetN/A income |
| **Regulated Function(s) Held:** | No |
| **Evaluation Level** | Implement 2 | **Role Family** | Group Corporate Functions |

|  |
| --- |
| **Overall Role Purpose** |
| The purpose of the Information Security Analyst role is to support the Information Security Manager in implementation of the Information Security Governance, risk and compliance framework, and to deliver the associated risk and control assessments track remediation of activities across the MPS business environment. The analyst will help to design, implement and monitor information security controls in line with industry requirements to ensure MPS maintains a stable, secure and compliant environment.As part of the information security function, this role will :* Assist with highlighting and ensuring the reduction of information security risks across the organisation, in line with the MPS group risk appetite and methodology
* Monitor, report and remediate on control or policy deviations across the organisation
* Support and deliver processes within the Information Security function, including third Party Risk assessments, project and change assurance, information security awareness and management reporting as needed
 |

|  |  |
| --- | --- |
| **Accountabilities (RACI)** | **Measures of Success/KPI’s** |
| **Operational** * Support the design and implementation of Information Security policies and standards to ensure MPS meet business and legislative and/or regulatory requirements.
* Identify and support the implementation of controls to protect the confidentiality, integrity and availability of MPS networks and data
* Drive compliance to industry standards and frameworks as adopted by MPS
* Perform day to day activities within the team, including various technical assurance and risk reviews and supporting business change projects
* Support the development and delivery of both the Information Security strategy and the Digital and Change strategy
 | * Corporate Strategic priorities Vs plan
* Division Plan delivery Vs plan
* Delivery of projects to plan
* Delivery of Information Security activity - actual v plan
 |
| **Financial*** Recommend security enhancements and purchases for MPS to minimise related threats to MPS infrastructure and Networks
* Ensure activities assigned are completed within agreed time and budget governance constraints to drive both cost and process efficiency
* Support the production of reporting on findings, make recommendations for corrective action and support regulatory and compliance certifications to GDPR and Cyber Essentials+.
 | * Operational budget Vs Plan
 |
| **Member*** Monitor for and provide robust challenge of emerging risks and issues arising from business activities which fail to deliver appropriate outcomes for members
* Identify and work to resolve non-compliance to regulation, contractual obligations and laws where they relate to our member facing activities
 | * Net promoter score
* Policy compliance audit results
 |
| **People**  * Support colleagues with Information Security related elements of their role, advocate security first culture and promote an environment in which colleagues are comfortable discussing information security related topics and understand associated risks
* Support awareness and communications campaigns as appropriate
* Take an active role in promoting a more inclusive environment, which aligns with our commitment to celebrate and promote diversity.
* Take personal accountability for own training, competence, performance and engagement of self and colleagues ensuring clarity on own accountabilities and comply with all governance, policy standards and processes
 | * Improved colleague understanding and awareness risk
* Delivery of Personal Development Plan to plan
* One to one / performance review meetings Vs Plan
* Colleague feedback
 |
| **Risk*** Support and implement risk management processes and procedures in line with MPS risk appetite and information security policy
* Identify and report information security risks, and issues identified within information security and across MPS to enable resolution and mitigation of potential impact on MPS, members and colleagues
* Appropriately inform and advise the business on incidents and incident prevention through the correct actions to mitigate further instances occurring.
* Support development and embedding of monitoring and metrics to monitor effectiveness of security controls to ensure MPS information assets are kept secure.
* Drive and coordinate remediation of vulnerabilities/risks identified to enhance weakness in MPS security controls.
* Contribute to reporting dashboards designed to inform colleagues of MPS security posture
 | * Risk & Control Self- Assessments
* Audit Actions
 |

|  |
| --- |
| **Responsibilities (RACI)** |
| * Support key processes with the information Security Functions:
	+ Provide security assurance of projects and identification of controls and non-functional requirements
	+ Support third party risk management and supplier assurance activities
	+ Contribute to development and implementation of security policies and standards
	+ Support technical risk management related procedures and activities within the team
* Work on and drive security-related projects, to ensure security requirements have been met and call out any risks identified against MPS risk appetite.
* Proactively identify and implement security controls with a remediation plan to bring back within MPS risk appetite.
* Liaise with relevant teams in specialist areas to manage security, and ensure contractual and regulatory requirements a are met.
* Assist the conduct of security audits detailing recommendations, improvements and corrective actions.
* As the compliance and information security landscape continually changes, keep abreast of evolving legislation and best practice; identify and recommend opportunities for MPS to become more efficient and effective in managing compliance and information security risk.
* Deputies for the Information Security Manager for assigned areas of responsibility.
* Undertaking other duties and tasks that from time to time may be allocated to the role holder that are appropriate to the level or role.
 |
|  |

|  |
| --- |
| **Key Governance Responsibilities** |
| * Facilitate reporting that will be utilised at the Executive and the Council.
 |

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Knowledge and Qualifications** | **Skills** | **Experience** |
| **Essential** | * Purposes and principles of information security and data protection
* Demonstrable Information Technology background, including knowledge of networking, application security and general IT delivery best practises (eg. ITIL)
* An understanding of the cyber security risks associated with various technologies and ways to manage them
* Working knowledge of security domains, auditing standards and frameworks, and risk analysis frameworks including ISO 27001, Cyber Essentials, etc
 | * 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.
 | * Significant experience of information security from a technical and compliance perspective
* Experience of Privacy regulation and best practise
* Experience of Payment Card Industry Data Security Standard (PCI DSS)
* Experience of managing technical projects from design to implementation
* Working knowledge of deploying and managing security solutions
* Solid understanding of network and infrastructure security best practices
* Experience of privileged access/account management
* Experience of dealing with escalations, both service and technical
 |
| **Desirable** | * CompTIA Security +
* CompTIA Network +
* (ISC)² System Security Certified Practitioner (SSCP)
 |  | * Experience of working to embed risk frameworks across an organisation
 |