|  |  |  |  |
| --- | --- | --- | --- |
| **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 carrying out technical assessments and remediation of activities across the MPS network, systems and software applications to ensure MPS maintains a stable, robust, secure and reliable IT environment underpinning core business processes and to ensure MPS data is robustly protected.The role will assist in the highlighting and ensuring the reduction of information security risks across the organisation, by driving the delivery of consistent, high quality security assurance and controls. The role will advocate and support a security first culture across the organisation |

|  |  |
| --- | --- |
| **Accountabilities (RACI)** | **Measures of Success/KPI’s** |
| **Operational** * Support the design and maintenance of Information Security policies and supporting standards to ensure MPS meet business and legislative and/or regulatory requirements.
* Support the delivery of systems to protect the confidentiality, integrity and availability of MPS networks and data to prevent security concerns that are likely to have a material adverse effect on the Group, its operation or financial security and/or reputation
* Contribute to the design and delivery of controls which mitigate risks identified against numerous Information Security frameworks to enable MPS to remain compliant
* Support the development and delivery of both the Information Security strategy and the Digital and Change strategy to plan, cost and quality
 | * 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 and consistent outcomes for members
* Provide support to the D&C division to ensure fair treatment and outcomes for colleagues and the organisation ensuring compliance with associated policies.
 | * Net promoter score
* Policy compliance audit results
 |
| **People**  * 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
* 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
* Act as a role model for best practice in demonstrating Information security to MPS
* Take an active role in promoting a more inclusive environment, which aligns with our commitment to celebrate and promote diversity.
 | * Improved colleague understanding and awareness risk
* Delivery of Personal Development Plan to plan
* One to one / performance review meetings Vs Plan
* Colleague feedback
 |
| **Risk*** 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.
* Review daily security monitoring output from security monitors and tools and escalate or take appropriate action to mitigate any security incidents.
* 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)** |
| * 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 vulnerabilities and inappropriate 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.
* Perform day-to-day operational monitoring and remediation of security threats and vulnerabilities via logical security tools and products. Escalate any security concerns to the Information Security Manager for consultation.
* 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
* Excellent IT skills, including knowledge of computer networks, operating systems, software, hardware and security
* 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 General Data Protection Regulation
* Experience of Payment Card Industry Data Security Standard (PCI DSS)
* Experience of disaster recovery planning
* Experience of managing technical projects from design to implementation
* Experience of leading teams and coaching other staff members.
* 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
 |