

Role Profile: IT Security Analyst

Role Levelling

P2

PEOPLE

Purpose	Key Relationships
<ul style="list-style-type: none">Providing secure and compliant technology, solutions and services to protect Member, Customer, Colleague and Society data and minimise risk to the Society	IT Security Manager Business Risk Lead Security Suppliers and Third Parties IT Architects IT and CTO teams

Key Accountabilities	Measures of Success	Experience/ Qualifications Required
<ul style="list-style-type: none">Supporting the IT Security Manager in the operation of IT Security standards and processes across the Society, achieving compliance standards relating to IT Security by managing threats, breaches, ensuring resolution and continuous improvementActing as the key IT Security contact for projects and new initiatives, reviewing changes made to the Societies live IT environment to ensure security protocols are maintained, ensuring that new systems have sufficient security applied prior to moving into the live environmentOn an ongoing basis:<ul style="list-style-type: none">Maintain and communicate the IT security standards, based on ITIL standards for the SocietyWork with the Security suppliers to ensure that the IT Security tools are utilized to reduce vulnerabilities within Society systemsEnsure alerts are investigated and escalated when requiredProvide detailed event / incident management of security service incidentsMonitor and investigate unauthorised access to Society systemsAct as part of the Society Incident Response team related to cyber or security major incidentsCarry out a continuous audit of current systems looking for opportunities for improving security measuresPerform analysis and threat / breach identification, responding to events and performing investigation / managementMaintain the IT security Incident logEnsure that policy and compliance requirements are being metMeasure the adherence of policy and standards and review gaps providing the IT Security Manager with appropriate risk information and follow up activity / actionsAssist in achieving the regulation compliance required, covering such areas as PCI, GDPR – working directly with internal and external auditors and PEN testers as requiredDesign and carry out internal led vulnerability and penetration assessments for new & established services including the technology and colleague awareness – maintaining the security first ethos	<ul style="list-style-type: none">Operationally critical systems available, recoverable and secureMember, Customer, Colleague and Society data is available, recoverable and secureBusiness continuity and disaster recovery plans to meet agreed SLAs and tested regularlyDeliver Society's Profit, Membership and Colleague Engagement targets annually	<ul style="list-style-type: none">CompTIA Security+CompTIA NetworkISO27001/2 (Desirable)CIS Controls (Desirable)Experience of developing Security Policy Framework (SPF)Experience of managing external parties to deliver Audit, Security Certification, or Compliance related activityExperience of demonstrating and embedding a security first ethos is essentialA working knowledge of IT applications, tools, processes and methodologies, with a particular focus on securityDemonstrating an ability to engage colleagues and make IT Security fun and relevant (Desirable)Experience of managing Security IR (Desirable)