

Job Family	
Role Title:	Information & Cyber Security Manager
Banding	2b
Summary:	Responsible for the operational management of the Society's information and cyber security capability, ensuring effective security controls, monitoring, assurance activities, risk management and regulatory compliance. Acts as the Society's subject matter expert for information and cyber security whilst supporting the secure delivery and operation of business and technology services.
Purpose:	To protect the confidentiality, integrity and availability of the Society's information assets through effective cyber security governance, risk management, assurance and operational controls. The role is responsible for the day-to-day management of the Society's cyber security capability, overseeing security monitoring, vulnerability management, incident response, supplier assurance, colleague awareness and compliance activities whilst supporting secure business and technology change.

What I Do:	How I Work:	What I Can Do:
Security Governance & Risk Management - Act as the Society's subject matter expert for information and cyber security, providing advice, guidance and assurance to colleagues, management teams, projects and third-party suppliers. - Develop, maintain and periodically review information security policies, standards, procedures and supporting controls to ensure ongoing regulatory and industry compliance. - Conduct security risk assessments across systems, infrastructure, suppliers and business processes, identifying opportunities to improve the Society's security posture. - Identify, assess and communicate current and emerging cyber threats, vulnerabilities and risks to relevant stakeholders. - Provide cyber security assurance and risk oversight for technology and business change initiatives.	- Build strong relationships with colleagues, suppliers, auditors and business stakeholders to ensure cyber security is effectively embedded within everyday operations. - Take a pragmatic and risk-based approach when balancing security requirements, regulatory obligations and business needs. - Communicate complex technical risks and security matters in a clear and understandable manner for both technical and non-technical audiences. - Foster a culture of security awareness, accountability and continuous improvement across the Society. - Work collaboratively with technology and business teams to ensure security considerations are incorporated into operational processes and change initiatives.	- Strong knowledge of information and cyber security frameworks and standards including ISO27001, NIST, Cyber Essentials Plus and relevant regulatory requirements. - Strong understanding of network security, identity and access management, privileged access controls, cloud security principles and modern security platforms including Microsoft Defender, Microsoft Sentinel, Microsoft Purview and Secure Access Service Edge (SASE) solutions. - Experience of vulnerability management, penetration testing, security assurance and risk assessment activities. - Understanding of security monitoring, threat detection, incident response and cyber resilience practices.

- Produce security reporting, metrics, KRIs, KPIs and management information to support governance, oversight and risk-based decision making. Security Operations and Monitoring - Oversee security monitoring activities and supplier-delivered security services, ensuring security events and threats are identified and investigated appropriately. - Manage vulnerability management activities, ensuring vulnerabilities are identified, risk assessed, prioritised and remediated within agreed timescales. - Coordinate firewall reviews, network security assessments and vulnerability scanning activities. - Manage Data Loss Prevention (DLP) reporting and alert reviews, supporting the protection of sensitive and regulated information. - Lead privileged access governance activities, including periodic access reviews and assurance exercises. - Support the implementation of security improvements, control enhancements and remediation activities across the Society. Incident Response and Resilience - Develop, maintain and test cyber incident response plans, ensuring readiness to respond to security incidents. - Coordinate cyber security incident response activities, supporting investigation,	- Take ownership of issues through to resolution, ensuring security risks are appropriately managed and mitigated. - Remain informed of emerging threats, vulnerabilities, technologies and regulatory developments that may impact the Society. - Promote consistency, professionalism and high standards in the application of security controls, policies and procedures.	- Knowledge of data protection principles, information governance and data security controls. - Experience managing third-party suppliers and outsourced security service providers. - Experience supporting audit, compliance and assurance activities within regulated environments. - Ability to interpret technical threats and risks and translate them into meaningful business impacts and recommendations. - Strong analytical, investigative and problem-solving skills. - Excellent stakeholder management, communication and influencing skills. - Ability to manage competing priorities while maintaining focus on operational delivery and risk reduction.
--	--	--

containment, recovery, lessons learned and reporting. ▪ Design and coordinate cyber simulations, tabletop exercises and resilience testing activities. ▪ Support operational resilience, disaster recovery and cyber recovery testing and continuous improvement activities. Supplier Assurance and Security Compliance ▪ Assess and manage information security risks associated with third-party suppliers and service providers, ensuring contractual security obligations are met. ▪ Coordinate internal and external security audits, regulatory reviews and assurance activities. ▪ Maintain and coordinate the annual penetration testing programme, ensuring remediation activities are tracked through to completion. Security Awareness and Culture ▪ Deliver and coordinate security awareness programmes, phishing simulations, training initiatives and colleague engagement activities. ▪ Support and promote data security initiatives including data classification, ownership, retention, minimisation and protection controls.		
General duties:		

- Carry out all duties as detailed and in accordance with documented policies and procedures
- Maintain risk awareness within the role, ensuring relevant controls are implemented and are operating effectively, reporting of all risk events identified and escalating risk issues which have the potential to breach the Society's appetite for risk / control environment.
- Prepare and collate management information in accordance with laid down procedures and standards
- Contribute to the wider Society goals through active contribution and supporting colleagues
- Promote the interests of and ensure adherence to the policies of the Society.
- Carry out all duties taking into account the FCA's Conduct Risk requirements and principles of Treating Customers Fairly and the need to comply with relevant Conduct Rules.
- Carry out all duties in compliance with the FCA's Conduct Rules as applicable to the role (as detailed in the Code of Conduct Sourcebook (COCON)).
- Ensure that regulatory requirements in respect of Anti Money Laundering (AML) and Terrorist Financing are complied with, including:
- Carry out prescribed customer due diligence measures (CDD) for all customers (including appropriate enhanced due diligence (EDD) measures, where applicable) before establishing a business relationship and at appropriate times during the business relationship in accordance with documented procedures.
- Understand the law and personal obligations and responsibilities under it and the potential legal and regulatory penalties for any breach / non-compliance.
- Complete training as required in order to attain and maintain knowledge and continuing competence in AML systems, controls and procedures.
- Report knowledge or suspicion of any money laundering or terrorist financing activity promptly in accordance with procedures.
- Undertake other duties as may be required in the post and department detailed above or any other post in any department or branch of the Society.