Security & Information Risk Advisor

Registers of Scotland
ros.gov.uk

Services	Security & Information Risk Advisor
Department	Risk and Information Governance
Grade	SEO
Directorate	Policy and Corporate Services
Role Reports to	Head of Information Security, Risk & Assurance
Hours of work	35 hours per week. We are a flexible employer and will consider a variety of working patterns; compressed hours, term time working or part time working on a case-by-case basis, depending on the role and departmental requirements.
Contract Type	Permanent
Location	This will be a hybrid role with office attendance as required at either Meadowbank House (Edinburgh) or St Vincent Plaza (Glasgow). It is expected that you would attend the office regularly during your initial training and learning period.
Role Purpose	An experienced **Security and Information Risk Advisor (SIRA)** is required to play a pivotal role in strengthening and maturing our organisation's cyber security posture. You will provide expert guidance on the identification, analysis, and treatment of information security risks, and support the continued development, operation, and improvement of our Information Security Management System (ISMS). This is a key position within Information Security Risk and Assurance, in this role, you will offer technical information security expertise across both established and emerging services, ensuring compliance with Registers of Scotland (RoS) policies, standards, and relevant legislation and frameworks. Working collaboratively with technical and non-technical teams, you will help embed effective security controls, improve security outcomes, and foster awareness of threats and best practice. You will also contribute to the continual enhancement of our policies, standards, processes, and controls, as well as support organisational reporting and assurance activities across on premise and cloud environments.

JOB DESCRIPTION	
Main Responsibilities	As part of the Information Security Risk and Assurance team you will: • Formulate strong relationships between the Information Security and Risk function and business teams, both technical and non-technical • Promote Information Security and Risk Services offered. • Conduct technical assurance activities of systems, services, and products. • Assist stakeholders in understanding and fulfilling their information security roles and responsibilities. • Provide advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. • Obtain and act on vulnerability information and conducts security risk assessments and business impact analysis on complex information systems. • Contribute to development of information security policy, standards and guidelines.

	• Interpret information assurance and security policies and apply these in order to manage risks. • Provide advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines. • Use control testing information to support information assurance assessments. • Collection and dissemination of relevant information and risk management information. • Deliver sessions and workshops for the scoping, identification, and analysis of security risks to the confidentiality, integrity, and availability of information assets, and propose appropriate controls and actions for risk remediation. • Observe instances of Non-Conformance, providing details of findings and the motivation for the issue. • Undertake internal audit/assurance activities to observe and evaluate ISMS processes and Security Controls and provide internal stakeholders with reports that outline findings and areas for improvement of compliance. • Deliver Supply Chain risk assessment and assurance activities for identified suppliers and 3rd parties that have access to RoS information.
PERSON SPECIFICATION	
Essential Criteria	**Technical** The SIRA will hold the following certifications/qualifications or equivalent: • Certified Information Systems Security Professional (CISSP) • Certified ISO 27001 Lead Implementer/Auditor of Management Systems (including Information Security and Business Continuity) **Experience** A strong understanding and background in technical information security and risk and can engage with management and technical/non-technical SMEs for the successful implementation and operation of the ISMS and its associated deliverables. Possessing knowledge in (and not limited to): • Technical information security and risk. • Identification, assessment and management of risk. • Security assurance and the measurement of controls. • Creation of ISMS and IT Security documentation (Policies, Standards, Processes, Procedures and Patterns). • Internal and Third-Party Audits. • Risk and threat modelling. • Compliance and Assurance Activities. • Business process analysis and mapping (to determine alignment against agreed industry practice and recognised control frameworks). **Behaviours** **Making effective decisions** • Use evidence and knowledge to support accurate, expert decisions and advice. Carefully consider alternative options, implications and risks of decisions. • Approach problems and issues with regard to information security and risk, use techniques to analyse the information within scope and formulate resolve to maintain objective/achieve outcome.

	Managing a quality service • Deliver service objectives with professional excellence, expertise and efficiency, taking account of diverse customer needs. • Understand the objective of Information Security, Risk Management and mentor engaged teams and colleagues. Can articulate the distinction and relationships between Information Security Risk, Cyber Security, Security Controls, and Assurance. **Communicating and influencing** • Communicate purpose and direction with clarity, integrity and enthusiasm. Respect the needs, responses and opinions of others. • Able to facilitate engagement between non-technical, technical, and non-information security colleagues. Able to mediate between stakeholders and promote the realisation of common goals. **Changing and improving** • Seek out opportunities to create effective change and suggest innovative ideas for improvement. Review ways of working, including seeking and providing feedback. • Able to support the Head of Information Security, Risk and Assurance with improvements to the Information Security Management System and ensuring that it meets the requirements of international standards (ISO/IEC27001:2022) as well as the Cyber Assessment Framework.
Desirable skills & experience	• Supporting organisations through security certification activities (ex. ISO27001 and Cyber Assessment Framework) • Building security capability, training and awareness or exercising programmes • Designing information security incident management procedures • Understanding of the NCSC Cyber Assessment Framework