BritishRedCross

Information Security GRC Manager

Job Level	5	**Korn Ferry Function**	KF 17
Directorate	Technology	**Function/Service**	Information Security
Direct Reports	6	**Indirect Reports**	None
Line Manager Title	Head of Cyber Security	**Budgetary Responsibility**	Programme related

The Leadership and Management of our people is critical to us as an organisation. The responsibilities and expectations of Leaders and Managers at this level can be found in Our Leadership Framework - RedRoom.

Our Leadership Framework defines the leadership standards we want to see at the British Red Cross. It shows what great leadership looks like. Our goal is to create a great workplace and deliver excellent services to our users. Our Leadership Framework - RedRoom, along with Our values and behaviours - RedRoom and Fundamental Principles, helps everyone understand how the leadership capabilities relate to their role and context.

Diversity is something we celebrate, and we want you to be able to bring your authentic self to the British Red Cross. We want you to feel that you are in an inclusive environment, and a great position to help us spread the power of kindness. You can read more about Equity, Diversity & Inclusion (EDI) at the British Red Cross - RedRoom here.

Role Description	
Purpose	The role leads a team responsible information security risk management framework for the British Red Cross, including the identification, assessment, and treatment of information and cyber security risks, as well as third-party and supply chain cyber security risk management. The role provides subject-matter expertise and strategic leadership for the organisation's Information Security Management System (ISMS) and ISO/IEC 27001 certification programme, ensuring effective implementation, maintenance, and continual improvement of the ISMS and compliance with ISO 27001 standards, policies, and controls. The role also ensures that the British Red Cross maintains ongoing compliance with key security standards, contractual, and regulatory requirements.
Key Responsibilities	**Information Security Governance & Strategy** • Develop and maintain information security governance framework for the British Red Cross, including policies, standards, and processes, ensuring they align with organisational objectives, legal, contractual, regulatory requirements, and best practices. • Regularly review and update security policies to reflect emerging threats, new technologies, and changes in the legal, regulatory, and operating environment. • Provide strategic input on security governance to ensure that information security remains a core part of business planning, projects and digital transformation initiatives.

Information Security Risk Management

- Oversee and continuously improve the information security risk management framework, ensuring robust processes for identifying, assessing, recording, and managing information security risks across the British Red Cross
- Own the management of information security risks, including developing appropriate risk mitigation and treatment plans when risk levels exceed acceptable thresholds, providing regular reporting and insight on key risks, risk trends, and control effectiveness to relevant internal governance boards, risk management forums, and senior leadership.
- Advise risk owners and decision-makers on security risk acceptance or remediation options, ensuring informed risk-based decisions.
- Manage the information security due diligence and assurance of suppliers, partners, and third parties, developing and enforcing a supply-chain security risk management processes ensuring that vendors and partners handling British Red Cross data or systems meet our security requirements.
- Collaborate with relevant teams and stakeholders to ensure security is integrated into third-party contracts and service agreements.

Compliance, Assurance & Certification

- Lead the ISO 27001 certification programme and ongoing compliance with the ISO/IEC 27001 standard.
- Act as the primary point of contact for external auditors and certification bodies, planning and coordinating certification (and surveillance) audits, ensuring that all necessary evidence, documentation, and corrective actions are managed effectively.
- Coordinate input from across the organisation to ensure that all mandatory assertions are evidenced and that the British Red Cross maintains compliance relevant security requirements.
- Monitor progress on any improvement plans and remediation of any findings arising security assessments and audits and liaise with relevant teams to close any gaps.

Stakeholder Engagement & Collaboration

- Work in partnership with other departments and functions to ensure a cohesive approach to information security across the organisation.
- Promote a strong security culture and understanding of governance processes.
- Support the development and delivery of training or communication initiatives related to policies, data handling, and risk responsibilities, to ensure staff and volunteers understand their roles in managing information security risks.
- Cultivate productive relationships with key external stakeholders such as certification bodies, regulators, and partner organisations to stay informed of emerging requirements and best practices, and to advocate for our interests.

	The responsibilities described are not a comprehensive list and additional tasks may be assigned from time to time that are in line with the level of the role.
Know-How [s] is used to denote the minimum shortlisting criteria.	**Essential** • Strong emotional intelligence, and a commitment to inclusive leadership, creating an environment where team members can grow and excel. • Excellent knowledge of information security compliance requirements relevant to the British Red Cross, including PCI DSS (Payment Card Industry Data Security Standard), Cyber Essentials, and the NHS Data Security and Protection Toolkit [s]. • Proven experience implementing or maintaining an ISO/IEC 27001 certified ISMS, including managing certification audits and continual improvement cycles [s]. • Demonstrable experience in information security risk management, including establishing risk assessment processes, running risk workshops, managing risk registers, and presenting risk statuses to senior management or governance boards. • In-depth knowledge of information security principles, standards, and best practices, such as ISO/IEC 27001, NIST Cybersecurity Framework, CIS Controls, and their application in an organisational context [s]. • Strong understanding of enterprise risk management methodologies and tools, particularly as they apply to information security risk identification, assessment (quantitative and qualitative), mitigation, and monitoring. • Able to explain complex security concepts or risk issues in plain language, influence decision-makers, and negotiate effectively across the organisation. • Developing and implementing security policies and controls that meet regulatory or standard requirements, such as PCI DSS and Cyber Essentials [s]. • Experience coordinating compliance audits or assessments for information security frameworks, such as ISO 27001 or Cyber Essentials, working effectively with external auditors/certifiers and internal stakeholders to achieve successful outcomes. **Desirable** • One or more relevant information security and risk management certifications or qualifications, such as CISSP, CISM, ISO 27001 Lead Auditor/Implementer, or equivalents. • Experience working in a public sector, healthcare, or similarly regulated environment, familiar with Government Digital Service (GDS) or National Cyber Security Centre (NCSC) guidance for security assurance. • Knowledge of technical cybersecurity domains, such as network security, cloud security, or incident response, to better contextualise and advise on risk mitigations and controls. • Prior experience in the humanitarian, non-profit, or voluntary sector, with an understanding of the unique challenges of these environments.

	• Familiarity with ITIL or service management frameworks in context of security processes.
Additional Requirements	None

Pre Engagement Checks Highlight bold as required		
DBS- England & Wales	None	
PVG- Scotland	None	
Access NI- Northern Ireland	None	
Driver Check	No	
International Roles Only		
International Police Check	No	
International Driving Licence for manual cars	No	

Role Reference		**Review Date**	

We guarantee an interview to disabled candidates (as defined in the 2010 Equality Act), who meet the minimum shortlisting criteria in the advertised person specification and apply under the disability confident scheme.