HOUSES OF PARLIAMENT
R&R DELIVERY AUTHORITY

Job Description

Post Title	Cyber Security Assurance Manager
Team	Data & Digital – Digital Services
Reports to	Head of Cybersecurity Operations
Contract type	Open ended

Purpose of the Role

This role will plan, and co-ordinate Accreditation, Assurance, and Risk Management activity related to our digital capability. They will suggest mitigation methods where our standards cannot be fully met and be able to explain how that impacts risk profile. They will work across Data & Digital to create and put in place cyber controls and monitor compliance.

They will be an active voice in architectural and solution designs to ensure controls and cyber requirements are considered from the outset. They will help evolve our current products, services and systems through threat intelligence, re-accreditation activity and open constructive challenge as they will have a broader but detailed view of our digital capability and ecosystem.

Key Accountabilities and Responsibilities

Assurance and Compliance

- Responsible for providing the Product Group Managers and any project delivery teams with conditions of accreditation for new services and systems and actions that must be completed to manage risk prior to entering service.
- Lead the planning and design at appropriate intervals for security risk assessments and re-accreditation activity to evaluate the effectiveness of security controls and identify areas for improvement, such as vulnerability scanning for networks, red, blue, purple team activities to test resilience etc; if the service or systems development roadmap has altered our risk position either positively or negatively advice on actions we can take.
- Contribute to the overarching digital assurance process with supporting risk assessment generation, tracking and escalation to the CDO and SIRO.
- Act as the lead compliance authority for internal security risk management and working with wider D&D colleagues be a conduit to inform and seek sign off from the Senior Information Risk Owner (SIRO).

Risk Management

- Act as the lead compliance authority for internal security risk management
- Responsible for confirming that any technical solutions that the DA wishes to use, interface with or exploit the capability of does not have any significant technical risks that cannot either be managed (mitigated/tolerated/transferred/avoided).
- Advise management of security risk within DA risk profile by developing and maintaining a framework of security controls for operational daily management and strategic alignment,

providing advice and guidance to D&D and where appropriate the wider DA on the selection of proportionate controls in designs and operating processes.

- Provide risk management input to the overall Programme Security Planning Process as required and support supply chain security risk management and compliance
- Identify, evaluate, monitor, and drive accountability for risk control mitigations, implementing risk strategies, processes, and protocols.
- Own the Security Risk Register, ensuring ongoing risk identification and mitigation takes place.

Security Culture, Awareness, & Learning

- Contribute to the management and resolution of security incidents and keep abreast with evolving threats/risks, industry trends and works to implement best practices; also use this to work collaboratively with the CSOC to identify opportunities and to influence and deliver colleague training content.
- Contribute to the threat intelligence framework by helping with the identification of emerging risk.
- Deliver and maintain 'Being Secure' mandatory training package with L&D Manager for permanent employees across the DA and permanent Supply Chain.
- Manage organisational risk through developing DA Security Culture, embedding good Cyber practice at all levels of the Programme.
- Assist with oversight of CSOC messaging and awareness campaigns.

Governance

- Facilitate an information security governance structure, including the formation of an information security steering committee. Ensure alignment with Parliamentary cyber security and Information Authority standards.
- Secretariat for the Programme Security Group.
- Develop and run a Security Risk & Compliance Working Group for the improvement and tracking of cyber security risk.
- Engage with legal, audit, assurance, and compliance teams to align security risk management practices with regulatory and parliamentary requirements. Includes reporting into the Information Governance Group when necessary.
- Support the development and implementation of policies and procedures around security risk and ensure compliance and alignment of internal controls with Parliamentary Cyber security standards, such as ISO27001, NCSC Cyber Assessment Framework and NIST.
- Align with the D&D Enterprise Architecture policies and collaborate in their development to include controls/standards and how we can balance risk.

Key Stakeholders and Relationships.

- The immediate day-to-day relations expected will include building a close relationship and liaising with stakeholders at all levels, providing expert and influential advice within the Data & Digital department, L&D Training Manager, Security Vetting Administrator. External to the immediate security team, you will interact with Head of Risk, Head of Internal Audit, and Legal Counsel. There will also be expected engagement with our external supply chain including our service providers and strategic partners as well as risk stakeholders in the Parliament Digital Services.

Qualifications, Skills and Experience.

Essential

- A proven security professional with a compliance and risk management background with extensive experience of Cyber Assurance, technology risk, information security risk, or IT audit.
- A strong understanding of fundamental information and cyber security concepts and technologies.
- Demonstrated ability to manage various streams of activity with minimal supervision. collaborating with other departments to effectively achieve desired outcomes.
- Experience collating, analysing and interpreting information in both written and presentation form with the ability to effectively present and communicate this in a way that will reach and influence a variety of audiences; making the technically complex simple to inform a variety of stakeholders and ensure that security and risk is at the forefront.
- Proven experience of establishing a security risk and compliance function and writing reports for governance committees and groups.
- Demonstrable expertise in adopting tools and techniques to protect infrastructure and information.
- Demonstrable understanding and experience of managing the security of the operational technology found in cyber-physical systems and knowledge of the cyber threat landscape.
- Familiarity with cloud security concepts and technology, in particular Azure.
- Experience with the application of shared responsibility security models.
- Experience of working with protective marking schemes and best practice security standards such as Gov 007, NCSC 10 steps, JSPs, NIST, SyAPs and NPSA guidelines.
- Show sensitivity and understanding in moving the organisation to a Cyber Aware orientated mindset and where needed resolving acute and complex conflicts.

Desirable

- Experience of contributing to the development of a Human Behaviours and Cyber Training.
- Familiarity with cloud security concepts and technology with providers other than Microsoft Azure.