Job Description – IT Security, Governance, Risk, and Compliance Manager (PB3)

Job summary

This exciting role within the wider IT Department/team is responsible for IT SGRC - Security, Governance, Risk and Compliance playing a leading role in ensuring all aspects of this critical function are delivered against strategic direction and align with our obligations as a government department and our duties to HMG and the public.

You will oversee our IT security strategy, ensuring it supports business objectives and meets legal, regulatory, and government standards. You will identify and manage security risks associated with our IT systems, promote a consistent approach to risk treatment, and embed a security-first culture. As our senior IT security advisor, you will be part of the IT Leadership Team and collaborate closely with internal teams, suppliers, consultants, and partners.

This is a hands-on team lead position where your efforts make a real difference across organisation. You will roll up your sleeves, leading by example, and applying your skills, knowledge, abilities, and experience in this crucial role.

Key responsibilities & accountabilities

Security strategy; governance; policy, process, guidance ownership

- shape and steer the direction of IT security governance, ensuring alignment with business strategy, HMG requirements, and evolving threat landscapes
- ensure the organisation meets the standards expected of a government department, embedding capabilities to identify, detect, protect, respond, and recover in line with defined frameworks, standards, and practices
- maintain and evolve IT security policies and procedures that reflect regulatory, and business requirements, and promote compliance across the organisation
- stay informed of emerging threats, industry trends, and changes in best practice and government guidance to ensure the role remains current and effective
- influence strategy and culture to promote information security, governance, risk, and compliance principles
- provide pragmatic, risk-based IT security advice to colleagues across the IT Security function, wider IT team, and stakeholders
- lead modern IT/cyber security thinking and deliverable initiatives
- work with our IT Business Partner and IT Security colleagues to create and deliver engaging security comms to deliver engaging and varied security comms and campaigns, through a variety of existing and new channels, guided by industry best practice and business requirements

Security risk and incident oversight and management

- understand the risk landscape affecting IT systems and information
- work alongside IT colleagues to influence the review and monitoring of systems, processes, and solutions to reduce risk across the IT estate
- function as an escalation point for IT security risks and incidents. Evaluate IT security risks and execute informed risk-based strategic decisions

- support working groups, and process that leverage and use your security, risk and compliance expertise into technology lifecycle planning, delivery, and management across the organisation; promoting awareness, escalation; understanding of risks, threats, and mitigations to help shape outcomes and resilience across the technology environment
- collaborate with Knowledge and Information Management colleagues on enabling and supporting data and information governance, security, policy, and process activities
- support HR led investigations as required of potential misconduct or policy breaches

Assurance and compliance oversight and management

- oversee and influence regular risk assessments, independent assurance activities, and security testing
- oversee and manage the internal IT Department Risk Register in collaboration with IT Leadership colleagues

Area and team leadership and management

- manage the IT Security, Governance, Risk and Compliance team, ensuring clear direction, support, and professional development
- create security processes and workflows that align with Incident Management and Disaster Recovery plans and ensure the resilience of critical systems and services
- drive the alignment of Business Continuity and Disaster Recovery policies with Forestry England's IT Disaster Recovery and Information Management frameworks, ensuring resilience of critical systems and services
- contributing toward developing wider aspects of the department to improve the service we provide; how we operate; the ongoing development of the department and team against strategy and plans

And any other tasks, reasonably requested by your line manager.

Skills, knowledge & experience

Essential professional and technical experience

- strong demonstrable experience of IT and cyber governance, compliance, risk, and security within enterprise IT environments
- awareness and experience of working within industry, Government and NCSC security governance frameworks, standards, policies, and legislation (e.g. GovAssure, Cyber Assurance Framework, Government Functional Standards, Cyber Essentials, GDPR
- communicating security and risk insights, trends, threat landscapes, regulatory change; as well as complex security matters clearly with authority, influencing outcomes, and producing concise, audience-appropriate policies, procedures, guidance
- embed and manage compliance with contractual and security obligations across third parties, supply chain, and procurement activities
- experience leading or contributing to the response and resolution of IT/cyber security incidents, including investigation, remediation, assurance, continuous improvement
- experience of being a central point for provision of IT/cyber security and risk guidance
- ability to produce clear, concise reports and presentations, explaining complex information to varied audiences
- awareness of vulnerability management tools; enterprise IT systems, services, infrastructure, networking, applications in cloud, on-prem, and hybrid environments. Security tooling such Mimecast and Microsoft Defender, Sentinel, IDAM services; ITSM tools such as Halo, Lansweeper

Desirable professional and technical experience

- experience leading and managing an IT/Cyber Security function and working groups

- experience of risk reporting and tooling to support compliance and assurance work
- ITIL and ITSM
- an inspiring, motivational, supportive, and hands-on leader and manager; able to deliver and promote a culture of wellbeing and resilience through healthy and effective practices, communication, and guidance
- commitment to personal development and continuous learning to remain current with evolving technologies, threats, and best practices

Qualifications

Essential

- two or more of the following professional certifications or equivalent: ISACA CISA, ISACA CISM, BCS CISMP

Desirable

- BCS MBCS professional membership
- ITIL Foundation and awareness of ITSM

Forestry England