Forestry England

Job description – IT Security Assurance Manager (PB4)

Job summary

The Forestry England IT Team provide systems, services and capabilities to over 2000 staff, across a broad range of business functions. The team consists of highly-skilled IT professionals with our IT Security, Governance, Risk and Compliance, function part of the IT Team.

This role provides an excellent opportunity to join the Forestry England IT Security Governance, Risk and Compliance team. You will be responsible for taking forward and developing our IT Security assurance and audit activities, governance, risk-awareness, security, and compliance obligations in a dynamic environment. The IT Security Assurance Manager will be:

- Overseeing audit assessment, assurance and remedial/improvement actions.
- Leading liaison activities to drive awareness and collaborative improvement workstreams.
- Leading efforts to attain and work to industry frameworks, standards and best practice.

You will help us drive forward security standards and capabilities, understanding and identifying the risks associated with systems, services and suppliers to align standards to HMG security requirements, legislative obligations, and best practices effectively.

Key work areas: responsibilities & accountabilities

- **Assessment, audit, assurance and remedial improvement**
  You will have responsibility for overseeing and responding to internal audits and assurance testing programmes, and for managing and driving our programme of external audit and assurance testing. Forming strong relationships, you will use the results of assessments, audits, assurance exercises and testing, to lead and drive continuous improvement; overseeing planned improvement actions until vulnerabilities are treated. You will also provide information and guidance to contract managers, system owners and managers to drive change and improvement across our procurements, contracts, and supply chains; working to improve their security posture and meet HMG standards.

- **Cross-departmental liaison**
  You will be responsible for and lead IT Security Team efforts to proactively improve protective security standards for all departments and the Forestry Commission as a whole. You will position yourself as a consultant focussing on new product/service evaluation, procurements, and improvement to existing third-party products/services. You will promote and embed IT security governance, principles and best practice; and provide tailored advice on risk and information management, guidance to System Owners and Managers, and colleagues as required.

- **Delivering Beneficial System Change**
  You will stay abreast of evolving threats, industry trends, and government guidance to elevate our system-security standards while serving as an escalation point for vulnerabilities and risks, offering clear risk treatment planning and management. You will also advise and support physical security initiatives in collaboration with the Estates Department, prioritising high-value and exposed assets. You will also contribute to Disaster Recovery, Incident Management, and Business Continuity efforts, and participate in collaborative IT Security initiatives.

- **Standards and accreditation**
  The ITSAM will contribute to efforts to drive forward accreditation applications to demonstrate our approach, and competencies, and protective standards for the benefit of all departments and the Forestry Commission as a whole. You will act as lead and subject matter expert to progress attainment of accreditations from start to completion.

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

Location-Specific Information (optional)

Person Specification: Skills, knowledge & experience

Essential Professional and Technical experience

- Strong experience in all aspects of IT/Cybersecurity and technology audit, assessment, assurance, and compliance.
- Strong demonstrable experience and knowledge within an enterprise IT environment and strong familiarity with enterprise IT security or service-provision requirements.
- The ability to write fluently, accurately and concisely with clarity and authority.
- Proven abilities documenting and presenting concise reports, explaining complex information to varied audiences.
- Excellent relationship-building and collaboration skills.
- Strong negotiation and problem-solving skills at all levels.
- Well-developed Microsoft 365 skills, (Teams, SharePoint, Outlook, Excel, Word).

Desirable Professional and Technical experience

- An understanding of the requirements and principles of GDPR and the Data Protection Act.
- Familiarity with HM Government security and assurance frameworks and standards such as GovAssure, Government Functional Standards, SecureByDesign.
- Experience of managing technology testing activities, e.g. pen-testing.

- Awareness of Artificial Intelligence, it's use in government settings, and the associated risks. Awareness of AI Assurance is highly desirable.
- BCS professional membership or membership of other role related authoritative Professional Accreditation body.
- A track-record of the ability to influence and guide senior IT leadership team on strategy direction and delivery.
- Awareness of ITIL.
- Ownership of personal development.

Qualifications

Essential

- A formal qualification or accreditation in the field of IT Security or Audit, such as CISM or CISA, or proven equivalent experience in an audit, governance, communications, IT Security role, or very similar.

Desirable

- Any formal qualification or accreditation in an Information Technology technical field.