JOB DESCRIPTION & PERSON SPECIFICATION

JOB TITLE: **Communications Audit Team Manager**

DEPARTMENT: Good Practice

REPORTS TO: Communications Group Audit Manager

SALARY: Job level E

HOURS: 37 per week (full time)
Part time posts may be available

PURPOSE OF POST:

The post holder will provide in house audit expertise on technical and organizational security measures employed within the telecoms sector and will be able to liaise effectively on a technical level with external stakeholders.

Manage and conduct technical expert audits of information security management and controls within the telecoms sector. Support the ICO by providing technical expertise during the scoping, planning, delivery and reporting on technical electronic communications audits within the Telecoms sector.

The post holder will develop the ICOs understanding of telecoms security technologies particularly in respect of information security; in so doing contribute to the ongoing development of telecoms sector audit strategy.

The post holder will work with colleagues across the ICO to support effective delivery of audits and telecoms related work.

KEY RESPONSIBILITIES

- This technical role will focus on the effective delivery of electronic communications audits within the telecoms sector with a specific focus on the Data Retention Regulations 2014 and the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 Reg. 5(6)).
- Test auditee's network security procedures and their effectiveness, against specific criteria mandated by Home Office Data Retention Notices'.
- Test network security and report on their effectiveness, against Home Office baseline security architecture, Data Retention Directive Security Requirements and, the Retention of Communications Data Code of Practice (draft).
- Lead and coordinate regular audits to review measures taken by the provider of a public electronic communications service to safeguard the security of that service under the Privacy

and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

- Assess and test communications network security arrangements and their effectiveness, using ENISA guidance on the minimum security measures required to comply with Article 13a of EU Directive 2009/140/EC.
- Develop strong stakeholder relationships with both IT and IG technical staff and senior management functions to assist with the effective delivery of audits and development of audit methodology.
- Maintain a working knowledge and practical application of industry standards and guidance such as those required by ISO 27001, 27011, NICC ND1643, CESG (CAS-T), PCI DSS and ENISA.
- Where required lead and supervise small audit teams, in the delivery of, on and off site audit work.
- Oversee the work of other audit team members and ensure that such work is performed to the required standards.
- Manage audit related expenses and associated costs in line with ICO expense policy.
- Proactively adding value to the Telecoms audit team through developing and refining audit approach consistent with emerging technologies, sector standards and methodologies.
- Support the Group Manager - Telecoms Audit, in the production of Telecoms sector summary reports; providing ICO regulatory feedback to the Home Office.
- Support the production and maintenance of Telecoms Audit Team guidance, procedures and toolkits; in line with their experience and learnings from audit engagements.
- Add value to the wider operation of the ICO by participating in projects and providing specialist advice to assist with the creation of procedures and guidance.
- Contribute to the development of colleagues within the Good Practice team by preparing technical content or providing specialist support to Learning and Development for in-house training, as required.

PERSON SPECIFICATION

	Essential Criteria	**How Assessed**
Education and Qualification	Educated to degree level or equivalent OR Approximately 5 years work experience demonstrating graduate level ability Certification or already working towards certification in any of	Essential Application Desirable Application

	CISM, CISSP, CISA, 27001 Lead Auditor, Cobit 5 Certified Assessor, CESG Certified Professional, CLAS.	
Work Experience	Good experience of configuring, managing or auditing ISMS within ISO 27001, Cobit or similar frameworks as part of an IT, Information Governance, internal or external audit team.	Essential Application/Interview
Demonstrable experience in at least 1 of the following desirable areas	Practical experience of enterprise security design and architecture within fixed line or mobile telephony services.	Desirable Application
	Practical experience with vulnerability testing or evaluation of information security architecture, its effectiveness and compliance with legal, regulatory or industry standards.	Desirable Application
	Practical experience of configuring, managing or auditing user privileges including system log analysis.	Desirable Application
	Experience of working with HMG and the Security Policy Framework.	Desirable Application
Knowledge, skills and ability.	Strong verbal reasoning, and analytical skills and attention to detail.	Essential Online assessment/Interview
	Experience working with legal and regulatory requirements.	Desirable Application

	Good ability to apply minimum information security standards (as described above) practically and pragmatically.	Essential Application/Interview
	Demonstrate good understanding of current cyber threats and information security best practices.	Essential Application/Interview
	Practical understanding of the Data Protection Act and/or Privacy and Electronic Communications Regulations.	Desirable Application
	Strong influencing and negotiating skills and the confidence to make robust yet pragmatic recommendations to senior management.	Essential Application/Interview
	Ability to travel nationally and work away from home on audit engagements which will require 2/3 night overnight stays every 8/10 weeks.	Essential Application
	Strong written communication skills, including the ability to convey technical subject matter clearly and concisely.	Essential Application

Please note that post holders for this role will be required to receive security clearance to SC level. This requires the disclosure of spent and unspent convictions. Although convictions will be taken into account, any such information will not necessarily prevent you from obtaining a security clearance.