Job Description
Information Security Manager

Service:	Digital Services	**Team:**	Strategy & Assurance	
Location:	Preston			
Salary range:	£44,624 to £48,684	**Grade:**		11
Reports to:	Head of ICT Strategy & Assurance	**Staff responsible for:**		1-3

Job Purpose

To fulfil the role of expert on Information Security for LCC. To provide professional advice on all aspects of Information Security and Assurance to colleagues within LCC and to customers. To be responsible for the creation and operation of an Information Assurance framework, to meet evolving business needs and changing industry standards. To manage ICT staff and partners engaged in Information Security and Assurance activities.

Responsible for ensuring successful achievement of external certifications including but not be limited to ISO 27001, PSN and PCI-DSS.

Accountabilities/Responsibilities

- To be responsible for the maintenance of an Information Security framework of policies, procedures and controls across the whole Digital service. To align and modify these in line with emerging technologies and changing business requirements, and to seek to continually improve their effectiveness.
- To be responsible for the creation and operation of an Information Security risk and issue management framework, to ensure these are identified and recorded and agreed treatments are tracked to completion.
- To proactively identify any need for specialist, external expertise regarding best practice in Security and Information Assurance, and to procure appropriate services where necessary and then monitor their effectiveness and compliance.
- To provide specific expertise and advice on government standards and industry best practice relating to Information Security. Ensure that compliance with these standards is embedded into all aspects of ICT service delivery by providing direction and guidance to ICT colleagues.
- To work with senior customers to provide strategic input to the development and operation of a framework of policies, procedures and meetings to ensure that security and information assurance requirements are fulfilled across LCC and its customer groups.
- To be responsible for developing and operating a framework of internal and external security audits. To ensure such audits are scoped, commissioned and undertaken, that the outcomes are reviewed, and appropriate actions are performed.

- To communicate Information Security and Assurance matters internally and externally to key stakeholders, including LCC Senior Management, legal professionals, security regulators and internal/external auditors.
- To be responsible for staff management of the Digital Security Team, including staff development and discipline, ensuring that their work is carried out in line with standards.
- To guide and liaise with colleagues across Digital Services on matters related to Security by Design and Security Operations.
- To work closely with LCC Information Governance and Data Protection colleagues to ensure a joined up approach.
- To keep up to date with emerging Information Technology.
- Effectively establish and manage stake-holder relationships

In addition to the skills knowledge and experience described above, you may be required to undertake a lower graded role as appropriate.

Due to the changing nature of the business, this job description serves as a framework to outline the main areas of responsibility. It is not intended to be either prescriptive or exhaustive and will inevitably change. You may be required to undertake other activities of a similar nature that fall within the remit of your area of work, as directed by service management, and this may entail working from other locations.

Other

- **Equal Opportunities**
  We are committed to achieving equal opportunities in the way we deliver services to the community and in our employment arrangements. We expect all employees to understand and promote this policy in their work.

- **Health and safety**
  All employees have a responsibility for their own health and safety and that of others when carrying out their duties and must help us to apply our general statement of health and safety policy.

- **Customer Focused**
  We put our customers' needs and expectations at the heart of all that we do. We expect our employees to have a full understanding of those needs and expectations so that we can provide high quality, appropriate services at all times.

Our Values

We expect all our employees to demonstrate and promote our values:

- **Supportive**
  We are supportive of our customers and colleagues, recognising their contributions and making the best of their strengths to enable our communities to flourish.

- **Innovative**
  We deliver the best services we possibly can, always looking for creative ways to do things better, putting the customer at the heart of our thinking, and being ambitious and focused on how we can deliver the best services now and in the future.

- **Respectful**
  We treat colleagues, customers and partners with respect, listening to their views, empathising and valuing their diverse needs and perspectives, to be fair, open and honest in all that we do.

- **Collaborative**
  We listen to, engage with, learn from and work with colleagues, partners and customers to help achieve the best outcomes for everyone.

Person Specification
Information Security Manager

Requirements	Essential (E) or Desirable (D)	To be identified by: application form (AF), interview (I), test (T)
Qualifications:		
• Information Systems, Security or related degree or equivalent	D	AF/I
• Significant relevant vocational training	E	AF/I
• CISM / CISSP qualified	D	AF/I
• Certified with ISO 27001 lead implementer or lead auditor	D	AF/I
• ITIL V3 or 4 foundation	D	
Experience:		
• Experience implementing or working towards ISO 27001	D	AF/I
• Client facing with current experience delivering security consultancy specifically ISO27001, PCI, CLAS etc.	E	AF/I
• Current experience encompassing Information Security Management (policy, procedures, controls, awareness, ISO 27001, Risk Management, Information Security, Information Governance, Certification, GAP analysis, compliance and risk assessment backgrounds).	E	AF/I
• Local Government experience	D	AF/I
• Experience of NHS Data Security and Protection Toolkit, PSN, PCI-DSS and Compliance	D	AF/I
• Experience in managing staff	D	AF/I
• Experience of vulnerability management	D	AF/I
• Experience of Incident response processes	D	AF/I
Knowledge and skills:		
• Ability to analyse and interpret complex problems.	E	AF/I
• Comprehensive knowledge of Information Security Management Systems with the ability to scope, design and implement such systems.	E	AF/I
• Strong ICT infrastructure, application and cloud/SaaS technical skills.	D	AF/I
• Excellent written and verbal communication skills.	E	AF/I
• Ability to deal with highly complex and high-risk problems across the diverse range of IT security threats.	E	AF/I
• Ability to translate highly complex technical matters into user friendly language.	E	AF/I
• Ability to lead with innovative ideas, and proactively create and drive a 'business benefits' approach	E	AF/I

Other: Commitment to equality and diversity Commitment to health and safety Display the LCC values and behaviours at all times and actively promote them in others	 E E E	 AF/I AF/I AF/I