Job description

Title:	Security Architect
Post no:	PREF106522
Department:	Chief Executive
Division:	Digital Data and Technology
Responsible to:	Technical Services Lead
Grade:	M5

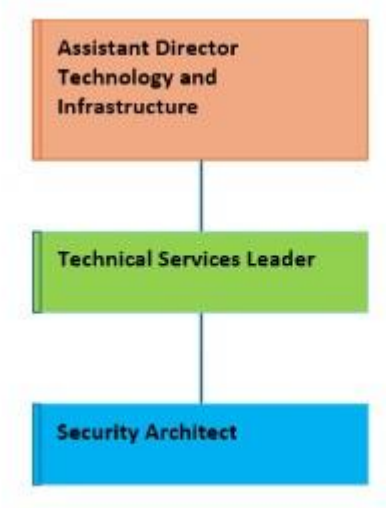
Purpose of post:

To provide security architecture design, assurance and expert guidance across the Council's technology estate, ensuring that security controls are designed into solutions from the outset and implemented in line with the agreed security operating model. Provide management of security related tools and systems.

The postholder will work closely with the Cyber Risk and Assurance Manager (Business Assurance) to ensure that architectural designs align with security policies, risk frameworks and assurance processes, while collaborating with networking, applications, infrastructure and wider technology teams to embed secure-by-design practices across all services.

This role is focused on security design, architecture, and management not ownership of organisational security policy, risk acceptance or governance.

Organisation chart:



Principal responsibilities: **%**

1. **Security Architecture Design**
   Lead the design of security architectures within technology solutions and platforms, ensuring appropriate controls are incorporated across network, infrastructure, application and cloud environments.
   20%
2. **Secure-by-Design Assurance**
   Provide security architecture assurance for projects and change, reviewing designs, identifying risks, and ensuring alignment with agreed security standards and architectural patterns. Collaborate with networking and technical services teams to design and assure security controls across connectivity, segmentation, identity, access, monitoring and resilience 20%
3. **Collaboration with the Security Operating Model**
   Work closely with the Cyber Risk and Assurance Manager (Business Assurance) to ensure security architecture designs are consistent with the council's operating model, policies, risk frameworks and assurance processes.
   10%
4. **Security Automation and Tools**
   Develop and deploy security tools such as SIEM, Purview, defender and data security platforms. Manage solutions and identify improvements. Configure, trouble shoot and maintain security infrastructure software and hardware.
   20%
5. **Security Risk Identification and Mitigation**
   Identify security risks and design mitigations, escalating design-level concerns through agreed processes without owning formal risk acceptance decisions.
   10%

6. **Standards, Patterns and Documentation**
   Develop and maintain security architecture patterns, reference designs and technical documentation to support consistent and secure solution design across the organisation. Including reporting and dashboards for various audiences.
   10%
7. **Technical Guidance and Capability Building**
   Provide expert security architecture advice and guidance across the wider Technology function, supporting improved security awareness and capability within delivery and operational teams.
   10%

Dimensions:

Supervisory management:
No direct line management. May provide specialist guidance to architects, engineers and delivery teams.

Financial resources:
No direct budget responsibility. Influences investment decisions through architectural recommendations.

Physical / Technical resources:
Accountability for security architecture artefacts, patterns and design documentation.

Context:

The Council operates a diverse and interconnected technology estate supporting corporate services, line-of-business systems and sensitive services.

Security architecture plays a critical role in ensuring that technology solutions are safe, resilient and trustworthy, while still enabling modern digital service delivery.

The Security Architect operates laterally across the Technology function, acting as a specialist design authority and trusted advisor.

The role supports delivery by providing clear, pragmatic security designs, aligned to the Security Operating Model and implemented collaboratively with technical teams.

This post supports agile working and operates in line with Council policies.

This role forms part of the Architecture pathway within the DDaT career progression scheme.

Physical effort:

Normal office environment

Working environment:

Normal office conditions

Skills Framework for the Information Age (SFIA) Alignment:

This role is aligned to a primary SFIA skillset of Solution Architecture (ARCH)

This role carries a level of professional responsibility aligned to SFIA Level 5: Ensure/Advise for Autonomy and Influence, and SFIA Level 6: Initiate/Influence for Complexity and Knowledge

Attribute Skills	Level	SFIA Description
Autonomy	5	Works under broad direction. Work is self-initiated, consistent with agreed operational and budgetary requirements for meeting allocated technical and/or group objectives. Defines tasks and delegates work to teams and individuals within area of responsibility.
Influence	5	Influences critical decisions in their domain. Has operational level contact impacting execution and implementation with internal colleagues and external contacts. Has significant influence over the allocation and management of resources required to deliver projects.
Complexity	6	Performs highly complex work activities covering technical, financial and quality aspects.
Knowledge	6	Applies broad business knowledge to enable strategic leadership and decision-making across various domains.

The business skills and behaviours required to be successful in this role are aligned to SFIA Level 5: Ensure/Advise for Decision making, Planning and Collaboration and SFIA Level 6: Initiate/Influence for Problem solving and Communication

Business Skills	Level	SFIA Description
Decision making	5	• Uses judgement to make informed decisions on actions to achieve organisational outcomes such as meeting targets, deadlines, and budget. • Raises issues when objectives are at risk.
Planning	5	• Analyses, designs, plans, establishes milestones, and executes and evaluates work to time, cost and quality targets.
Collaboration	5	• Facilitates collaboration between stakeholders who have diverse objectives. • Ensures collaborative ways of working throughout all stages of work to meet user/customer needs. • Builds effective relationships across the organisation and with customers, suppliers and partners.
Problem solving	6	• Anticipates and leads in addressing problems and opportunities that may impact organisational objectives, establishing a strategic approach and allocating resources.
Communication	6	• Communicates with credibility at all levels across the organisation to broad audiences with divergent objectives. • Explains complex information and ideas clearly, influencing the strategic direction. • Promotes information sharing across the organisation.

Person specification

This acts as selection criteria and gives an outline of the types of person and the characteristics required to do the job.

Essential (E): - without which candidate would be rejected.
Desirable (D): - useful for choosing between two good candidates.

Please make sure, when completing your application form, you give <u>clear examples</u> of how you meet the <u>essential and desirable</u> criteria.				
Attributes	**Essential**	**How Measured**	**Desirable**	**How Measured**
Experience	Significant experience working in security architecture, technical architecture, or a senior security engineering/design role. Demonstrable experience designing security controls within networks, infrastructure, applications or cloud platforms. Experience providing security design assurance for projects or technical change. Experience working collaboratively across multiple technical teams. Proven ability to communicate security risks and design decisions to both technical and non-technical audiences.	1,2 1,2 1,2 1,2 1,2	Previous experience of working within a public sector organisation	1

Skills/Abilities	Strong ability to analyse technical designs and identify security risks and mitigations. Ability to influence design decisions without formal authority. Clear and structured communication skills, particularly when explaining security concepts. Pragmatic approach to balancing security, usability and delivery needs. Collaborative and advisory working style.	1,2 © 1,2 1,2 1,2 © 1,2		
Equality Issues	Demonstrable knowledge and understanding of equality issues and legislation - able to integrate equality policies into service delivery, appraisals and employment practices.	1,2		

Specialist Knowledge	Strong knowledge of security architecture principles and secure-by-design practices. Practical understanding of network, infrastructure and application security controls. Understanding of identity and access management. Microsoft Technical stack Awareness of data protection and information security obligations relevant to public sector environments. Professional knowledge and experience in a relevant skill (ARCH, SEDN, IFDN, or NTDS) from the SFIA framework, equivalent to Level 5	1,2 1,2 © 1,2 1,2 © 1,2 © 1		
Education and Training	Undergraduate degree, NVQ/SVQ Level 4, or BTEC HNC in a STEM subject, or equivalent experience. Relevant Practitioner level professional qualification (e.g. TOGAF	1,4 1,4	Evidence of continuous professional development	1,4
Other Requirements	Occasional requirement to work outside of core office hours. Ability to attend various sites including data centres.			

(1 = Application form 2 = Interview 3 = Test 4 = Proof of Qualification 5 = Practical exercise)

We will consider any reasonable adjustments under the terms of the Equality Act (2010), to enable an applicant with a disability (as defined under the Act) to meet the requirements of the post.

The Jobholder will ensure that **Luton Council's** policies are reflected in all aspects of his/her work, in particular those relating to.

1. Equal opportunities

2. Health and Safety
3. Data Protection Act (2018) and General Data Protection Regulation (2018)

(i)