Job description

Title: Cyber Risk and Assurance Manager

Post no: PREF106520

Department: Chief Executive

Division: Digital Data and Technology

Responsible to: Head of the Assurance and Business Services and DPO

Grade: M6

Purpose of post:

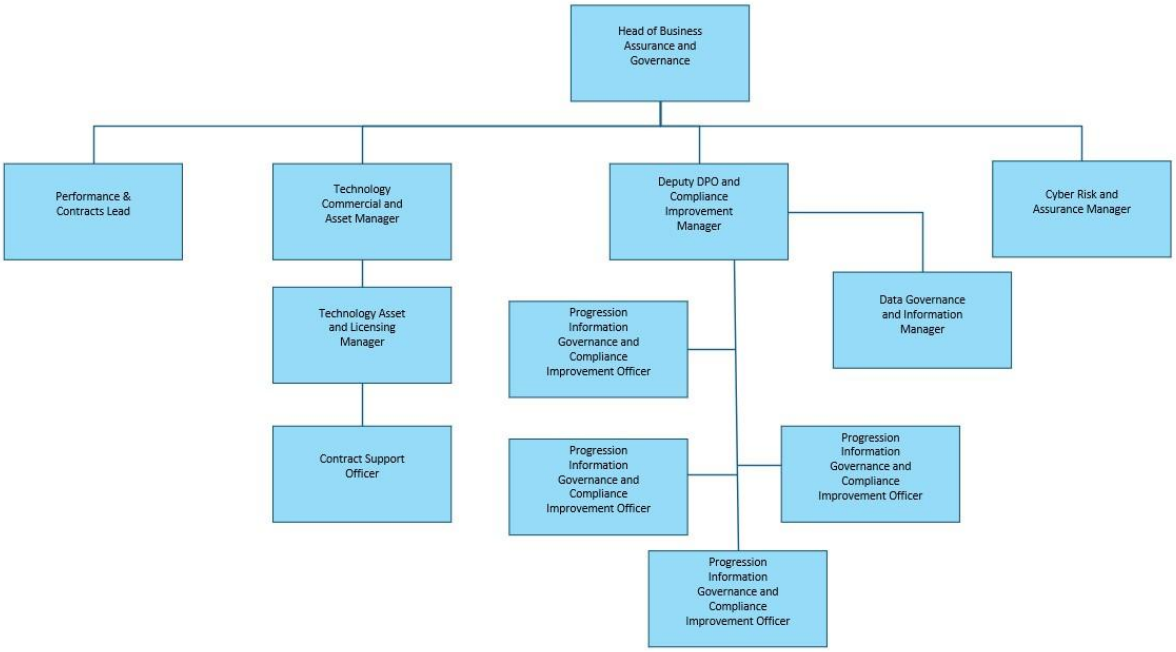
To lead, coordinate and continuously strengthen the Council's cyber risk and assurance arrangements, ensuring that risks, controls, sources of assurance and improvement actions are clearly identified, owned, evidenced and reported in a consistent, proportionate and auditable manner, with particular emphasis on cyber resilience, critical services and the Council's wider governance obligations.

This includes explicit ownership of the security RACI, so that accountabilities between DDaT governance, IT operations, suppliers, service teams and any SOC/SIEM capability are unambiguous, embedded and effective.

The postholder is accountable for ensuring the Council's security services are designed, deployed and operated in a way that meets agreed security requirements and quality standards, with strong performance management and assurance.

This role is not primarily a tool-operation post. Where monitoring, detection and triage are delivered by operational teams or an outsourced SOC provider, the postholder acts as the Council's relationship manager and intelligent client, ensuring governance, contractual oversight, escalation routes, assurance evidence, service performance and control effectiveness remain robust, measurable and demonstrable.

Organisation chart


Head of Business Assurance and Governance
Performance & Contracts Lead
Technology Commercial and Asset Manager
Deputy DPO and Compliance Improvement Manager
Cyber Risk and Assurance Manager
Technology Asset and Licensing Manager
Progression Information Governance and Compliance Improvement Officer
Data Governance and Information Manager
Contract Support Officer
Progression Information Governance and Compliance Improvement Officer
Progression Information Governance and Compliance Improvement Officer
Progression Information Governance and Compliance Improvement Officer

Principal responsibilities

1) Security Operating Model ownership (RACI, services, governance) – 20%

- Own and maintain the Council's Security Operating Model, including a published RACI covering governance, operations, suppliers, service owners and escalation pathways.
- Define and maintain the security service catalogue, including service boundaries, inputs/outputs, handoffs and performance expectations.

2) Security service performance management and reporting – 10%

- Implement and maintain processes, procedures, tools and practices for monitoring and managing security service performance, producing management information and ensuring action is taken when performance dips.
- Establish meaningful measures that demonstrate control operation and service outcomes (not just policy existence).

3) Incident governance, escalation and lessons learned – 15%

- Define and run the Council's security incident governance model: classification, escalation, decision points, communications routes and postincident review expectations.
- Ensure incident learning is translated into improved controls, updated RACI, and measurable actions tracked to completion.
- Work with service areas, IT operations and relevant suppliers to plan, coordinate and test IT business continuity and recovery arrangements for critical services, ensuring lessons learned are captured, actions are tracked, and resilience improvements are implemented.

4) Vulnerability, patch and remediation governance (assurance layer) – 10%

- Establish governance for vulnerability remediation and security technical debt: standards, prioritisation approach, risk acceptance routes, and reporting to senior stakeholders.
- Ensure remedial actions are owned and progressed by delivery teams/suppliers, with appropriate escalation where risk persists

5) Identity and access security governance (IAM/PAM oversight) – 10%

- Own the governance arrangements for identity, access and privilege assurance: access review cadence, exception handling, audit evidence expectations and escalation routes.

- Ensure access-related security controls are consistently applied and evidenced across relevant systems and platforms.

6) Third-party / supplier security assurance (commercial interface) – 15%

- Define and run the supplier security assurance model for DDaT: minimum security requirements, evidence expectations, review cycles, and escalation for non-compliance.
- Work closely with commercial and contract leads to ensure security requirements are embedded into supplier management, including service reviews and improvement plans.

7) Compliance and accreditation management (PSN, ISO, Cyber Essentials etc.) – 10%

- Manage the approach to maintaining relevant security accreditations and compliance requirements (e.g., PSN and ISO-aligned practices), ensuring evidence, corrective actions and audit readiness.
- Ensure security policies/standards are current, approved, and adopted, with clear ownership and review cycles.
- Ensure the Council's security assurance approach is informed by recognised frameworks, standards and sector good practice (for example CAF or equivalent), using these to support maturity assessment, improvement planning, audit readiness and executive reporting.

8) Stakeholder engagement and organisational enablement – 10%

- Engage and influence stakeholders across the Council to ensure security requirements are understood, adopted and met, including supporting decision-making through clear risk and options.
- Provide a work environment, guidance and enablement that supports delivery teams in meeting security expectations.
- Provide visible leadership in building a culture of knowledge transfer, capability development and continuous improvement across DDaT and service and stakeholders, including championing security awareness, mentoring and practical learning, and ensuring lessons learned, good practice and operational knowledge are actively shared and embedded.

Dimensions

Supervisory management: 1 direct report (where applicable), plus matrix working across DDaT for security responsibilities.

Financial resources: Supports the Head of Service with security service planning and budget oversight (amount TBC).

Physical resources: Accountable for the governance and integrity of the Council's security service model, security policy set, and associated assurance artefacts.

Other: Responsible for ensuring security services meet agreed quality and performance expectations.

Context

The Information Security function protects the Council from internal and external threats and works closely with operations and digital teams to ensure controls are implemented and sustained.

This role exists to ensure security is not fragmented across teams or suppliers, by running a coherent, measurable, and auditable operating model with explicit accountability

Security Operating Model
The postholder runs the security operating model for the Council, including:

- **RACI ownership for:** governance, SOC/SIEM (where applicable), IT operations, suppliers, service areas, and incident escalation.
- **Governance forums:** cadence, agendas, decision logs, action tracking and reporting packs.
- **Service performance:** defined service levels, measures, review cycles and improvement actions.
- **Evidence and assurance:** ensuring compliance and audit evidence is complete, traceable and current.

Additional information

Physical effort and/or working environment
Physical Effort

Normal office environment

Working environment:

Remote/office working conditions. The service will operate a rota covering the agreed service operating hours. Currently 7am to 7pm Monday to Friday.

Skills Framework for the Information Age (SFIA) Alignment:

This role is aligned to a primary SFIA skillsets of Technology Service Management (ITMG) and Performance Management (PEMT)

This role carries a level of professional responsibility aligned to SFIA Level 6: Initiate/Influence for Autonomy and Influence, and Level 7: Set Strategy/Inspire/Mobilise for Complexity and Knowledge

Attribute Skills	Level	SFIA Description
Autonomy	6	Guides high level decisions and strategies within the organisation's overall policies and objectives. Has defined authority and accountability for actions and decisions within a significant area of work, including technical, financial and quality aspects. Delegates responsibility for operational objectives.
Influence	6	Influences the formation of strategy and the execution of business plans. Has a significant management level of contact with internal colleagues and external contacts. Has organisational leadership and influence over the appointment and management of resources related to the implementation of strategic initiatives.
Complexity	7	Performs extensive strategic leadership in delivering business value through vision, governance and executive management.
Knowledge	7	Applies strategic and broad-based knowledge to shape organisational strategy, anticipate future industry trends, and prepare the organisation to adapt and lead.

The business skills and behaviours required to be successful in this role are aligned to SFIA Level 6: Initiate/Influence for Decision making, Planning, Collaboration, and Leadership and SFIA Level 7: Set Strategy/Inspire/Mobilise for Problem Solving and Communication

Business Skills	Level	SFIA Description
Decision making	6	• Uses judgement to make decisions that initiate the achievement of agreed strategic objectives including financial performance. • Escalates when broader strategic direction is impacted.

Planning	6	• Initiates and influences strategic objectives and assigns responsibilities.

Collaboration	6	• Leads collaboration with a diverse range of stakeholders across competing objectives within the organisation. • Builds strong, influential connections with key internal and external contacts at senior management/technical leader level.
Problem solving	7	• Manages inter-relationships between impacted parties and strategic imperatives, recognising the broader business context and drawing accurate conclusions when resolving problems.
Communication	7	• Communicates to audiences at all levels within own organisation and engages with industry. • Presents compelling arguments and ideas authoritatively and convincingly to achieve business objectives.
Leadership	6	• Provides leadership at an organisational level. • Contributes to the development and implementation of policy and strategy. • Understands and communicates industry developments, and the role and impact of technology. • Manages and mitigates organisational risk. • Balances the requirements of proposals with the broader needs of 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 clear examples of how you meet the essential and desirable criteria.

Please make sure, when completing your application form, you give clear examples of how you meet the essential and desirable criteria.				
Attributes	**Essential**	**How Measured**	**Desirable**	**How Measured**
Experience	Senior experience designing or running a security operating model (people/process/governance/tooling) in a complex organisation.	1, 2	Experience in public sector or similarly regulated environments	1, 2
	Experience defining and maintaining RACI and governance routes across technical teams and suppliers.	1, 2		
	Experience managing security service performance (metrics, reporting, service improvement actions).	1, 2		
	Experience governing incident management (escalation frameworks, post-incident review, action tracking).	1, 2		
	Experience with third-party/supplier security assurance and contract/service review environments.	1, 2		
	Experience supporting audits/accreditations and maintaining compliance	1, 2		

	evidence (e.g., ISO/PSN style requirements). Experience working across security, operations, and digital delivery teams to embed controls into BAU.	1, 2		

Skills/ Abilities	Ability to define and run a multi-team operating model, including RACI, escalation paths and governance.	1,2		
	Strong risk judgement: ability to communicate risk, options, mitigations and residual exposure clearly.	1,2 ©		
	Ability to influence and align stakeholders to security requirements without relying solely on hierarchy.	1,2		
	Ability to create and maintain clear, auditable documentation and assurance evidence.	1,2 ©		
	Strong analytical skills to interpret metrics, trends and control effectiveness.	1,2		
	Ability to manage supplier performance, reviews and improvement actions in partnership with commercial teams.	1,2		
	Ability to manage competing priorities and drive actions to completion across teams.	1,2		
	Strong written and verbal communication (briefing senior stakeholders, producing clear packs, decisions and logs).	1,2 ©		

Equality Issues	Demonstrable knowledge and understanding of equality issues and legislation;	1,2		
Specialist Knowledge	Security governance and operating model design, translating threat landscape into control priorities and assurance requirements (controls, accountability, evidence). Governance across the security lifecycle: incident response, vulnerability remediation prioritisation, IAM/PAM access assurance, supplier security assurance, and how SIEM/SOC operations support escalation and evidence.	1,2 © 1,2 ©	Experience supporting internal audits and external inspections	1,2
Education and Training	A recognised qualification such as CISSP CISM CCSP or CRISC (or equivalent) or ISO 27001	1,2 ©	ITIL (v3/v4) knowledge/qualification Public sector security compliance experience	1,2 1,2
Other Requirements	Able to attend meetings in and outside the borough when required and be able to work flexibly Able to work remotely and cover service operating hours	1,2 1,2		

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 job-holder will ensure that Luton Council's /Luton Cultural Services Trust/ Active Luton (delete where appropriate) policies are reflected in all aspects of his/her work, in particular those relating to:

- Equal opportunities
- Health and Safety
- Data Protection Act (2018) and General Data Protection Regulation (2018)
- GCSx Acceptable Usage Policy (where applicable)