THE ROYAL BOROUGH OF KENSINGTON AND CHELSEA

JOB DESCRIPTION

Job title	**Head of Cyber Assurance**
Directorate	Resources
Service	Audit, Risk and Insurance
Team	Audit
Grade	Grade K

DBS Check Required	None
Justification for DBS	Choose an item.
Politically Restricted	No

Responsible to:	Director of Audit, Risk, Fraud and Insurance
Employees directly supervised *(if applicable)*:	Security Risk Analyst x 1 Cyber and Information Governance Training and Awareness Officer x 1

Organisational structure chart *(job titles only, no employee names)*

1. JOB PURPOSE:

1. To provide focused and strategic leadership in relation to cyber security across the council, providing insight, direction, guidance and assurance, keeping abreast of the threat landscape and required mitigations to address it.
2. To ensure that there is comprehensive assurance, guaranteeing that there are adequate and tested resilience and cyber risk management systems in place across the Council.
3. To ensure that cyber security is aligned to the Council risk appetite, to protect the Council's information, technology, operational systems, and digital services.
   To maintain a supportive safe and resilient service delivery for residents, partners, and staff.

2. DESCRIPTION OF DUTIES:

Key responsibilities

Cyber leadership

- Define and lead the implementation, of the Council's Cyber Security Strategy and related policies, ensuring compliance with Public Services Network (PSN), Cyber Assessment Framework and National Cyber Security Centre (NCSC) best practice for local government and in alignment with the Digital, Data and ICT Strategy and Council Plan.
- Act as the Council's most senior internal advisor on cyber threats, resilience, and incident response.
- Collaborate effectively with the Chief Information Officer (CIO), the Executive Team, Directors and partners to provide expert advice on cyber risk, resilience, and emerging threats.
- Oversee and assure the delivery of the Council's cyber maturity roadmap and associated programme of implementation, ensuring continuous improvement and alignment with ongoing updates to best practice.
- Represent the Council in regional and national cyber forums, including warning advice reporting point (WARP) meetings and in engagements with NCSC, Local Government Association (LGA), SOCITM, and local resilience partnerships.

Cyber risk, governance and compliance

- Own the Council's cyber risk management framework, ensuring risks are identified, assessed, mitigated, and reported effectively.
- Ensure compliance with all relevant law and with wider security elements of the PSN Code of Connection, PCI-DSS compliance related security requirements and any related requirements from central government or statutory partners.

Strategic assurance

- Provide assurance to Executive Leadership and to members in relation to the effectiveness of the cyber control and response framework, including delivery of controls within the ICT function.
- Work closely with the Head of Internal Audit, Fraud and Risk Management to scope, commission and report on internal audits and external specialist cyber audits in relation to key areas of risk. Ensure oversight of related action plans.
- Periodically audit / commission independent audits / test (depending on conflicts of interest) into how effective the Council's approaches are in relation to:
    - Assessing and mitigating cyber risk.
    - Disaster recovery and BCP readiness in the identification, classification and protection of services as expected under the CAF for local government.
    - Incident response and recovery preparedness.
    - Vulnerability and patch management.
    - Technical controls including endpoint, network and device security.
    - Control of 3rd party risk.
    - Application of identity and access control.
    - Security culture, training and human risk.
    - Continuous improvement and CAF alignment.

Security operations and incident response

- Manage the Council's Security Operations Centre (SOC) and Incident Response contracts ensuring continuity of coverage and assuring the embeddedness of processes and alerts within the wider Council teams as required (e.g. ICT).
- Provide assurance on the effectiveness of the Council's threat monitoring, detection, vulnerability management, and response, working closely with the CIO to ensure changes are made if / as required.
- Act as the Lead Advisor to the Council for major cyber incidents, coordinating technical, operational, and communications responses.
- Ensure that incident response and disaster recovery plans are appropriately tested and follow up actions are followed through, working closely with the Council's Resilience Lead to ensure alignment with business continuity plans. Ensure lessons learned are captured and taken forward and embedded into future service delivery Council wide.

Security Architecture and ICT service interface

- Work closely with the CIO and the ICT team to ensure and assure that ICT delivery is secure by design (delivery to be the responsibility of the ICT Service).
- Lead on cyber assurance for major programmes, procurement, and supplier onboarding.

Supply chain assurance

- Lead timely and proportionate supply chain assurance in relation to information security and data protection risk (working closely with the DPO and all council teams) for third party suppliers, contractors and partners.
- Work closely with the Head of Strategic Procurement to ensure that procurement processes include cyber and information security requirements.

Managing human risk factors

- Lead the Council's cyber awareness programme for staff and members.
- Promote a culture of cyber vigilance and shared responsibility.
- Ensure training is role-specific, risk-based, and aligned with NCSC guidance.

Service leadership

- Build organisational capability, ensuring staff development and modern professional standards are defined, embedded and adhered to.
- Foster a culture of collaboration, innovation, customer focus and continuous improvement.
- Implement and lead a small Cyber Assurance team with a focus on driving change, compliance and assuring Council wide Cyber security delivery.
- Be accountable for effective budget management, ensuring the necessary controls are in place to proactively manage within budget and to ensure proactive and sufficiently pre-emptive contract pipeline management and associated supplier risk.
- Be accountable for cyber security risk oversight across the organisation and for ensuring mitigations are in place and effectively governed.

The duties and responsibilities outlined in this job profile are indicative of the role, however they are not exhaustive and may be subject to change. In addition, you will be required to undertake other reasonable duties as directed by your manager.

SELECTION CRITERIA/PERSON SPECIFICATION

Conditions to Note:
The person specification outlines the essential requirements the post holder or applicant must meet to fulfil the role and the duties outlined.

Candidates:
When completing your application form, please address your answers directly to each of the selection criteria below. This enables the panel to assess your ability to meet each criterion. It is essential that you give at least one example of your ability to meet each of the four Values and Behaviours: Putting Communities First, Respect, Integrity and Working Together.

Recruiting Managers:
The following values and behaviours are essential criteria in each post and must be addressed directly by candidates. The Guidance Notes on values and behaviours for managers give example questions to probe candidates in the interview and application stages of the recruitment process.

Resilience:
We encourage staff to assist the council during a significant emergency response which will focus on meeting the needs of residents. This may necessitate staff involvement, and in exceptional circumstances, could involve redeployment to support the emergency response.

Informed by our learning from the Grenfell tragedy, senior managers (Head of Service and higher) are expected to play an active coordination and leadership role in the Council's broader emergency response efforts during major or serious incidents. This includes arranging urgent resources from their own services and rallying staff teams to help residents during their time in need.

Values & Behaviours
The Royal Borough of Kensington and Chelsea have identified four key behaviours and values that should be demonstrated by all council employees. Successful candidates will show the ability to meet these behaviours.

A	**Equal Opportunities** Demonstrate an understanding of and commitment to Council policies in relation to Equal Opportunity, Customer Care and service delivery, and the ability to implement these policies in the workplace.
B	**Qualifications/Training/Certificates** • Degree in Computer Science/Cybersecurity or related field or comparable experience within security field Professional certificates related to the position such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or similar or comparable experience.

C	**Skills, knowledge and experience** ▪ Proven leadership of cyber security assurance within a large, complex organisation including oversight of technical controls, governance, risk management, compliance and assurance activities. ▪ Strong knowledge of National Cyber Security Centre (NCSC) best practice, the Cyber Assessment Framework for local government, cyber risk management, and incident response. ▪ Strong understanding and prior experience of managing technical and organisational cyber risks including risk identification, assessment, definition of mitigations and reporting. ▪ Strategic mindset and collaborative approach to delivery, evidenced in prior senior roles, including in the development of cyber security strategy and policy, as well as assurance frameworks. ▪ Experience managing cyber incidents, including incident response, coordination with internal and external stakeholders, and post-incident review. ▪ Experience managing suppliers, contracts and third-party cyber assurance, ensuring compliance with organisational and regulatory requirements. ▪ Experience influencing senior leaders, including elected members, directors, partners and suppliers, to support informed decision-making and investment in cyber resilience. ▪ Experience working within public-sector governance, risk, procurement and regulatory frameworks, including assurance requirements for local government. ▪ Experience working with complex technology estates, including legacy systems, cloud services, operational technology, and sensitive or regulated data environments. **Knowledge and Technical Skills** ▪ Strong knowledge of National Cyber Security Centre (NCSC) best practice, including secure-by-design principles, threat-led approaches and risk-based decision-making. ▪ Deep understanding of the Cyber Assessment Framework (CAF) and its application within local government and other regulated sectors. ▪ Knowledge of key cyber-security standards and frameworks, such as International Organisation for Standardisation (ISO) 27001, National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Zero Trust security models and of card security, including Payment Card Industry Data Security Standard (PCI-DSS). ▪ Strong technical understanding of cyber-security controls, including identity and access management, network security, vulnerability management, logging and monitoring, and secure configuration. ▪ Ability to assess the effectiveness of technical and organisational controls, identify gaps, and define assurance requirements. ▪ Understanding of local government systems, data flows, operational processes and service environments, including the risks associated with them.

	▪ Knowledge of cyber-security legislation and regulatory requirements, including data protection, public-sector compliance obligations and supply-chain security. **Leadership and Interpersonal Skills** ▪ Strategic mindset, with the ability to set direction, prioritise effectively and balance operational needs with long-term resilience. ▪ Collaborative approach to delivery, working across ICT, services, partners and suppliers to embed a culture of cyber assurance. ▪ Strong influencing and relationship-building skills, with the ability to engage confidently with senior officers, elected members, technical specialists and external partners. ▪ Excellent communication skills, with the ability to translate complex cyber-security issues into clear, accessible language for non-technical audiences. ▪ Ability to lead, motivate and develop teams, fostering a culture of continuous improvement, accountability and professional growth. ▪ Calm, credible leadership during incidents, providing assurance and direction under pressure. ▪ Demonstrable commitment to equality, diversity and inclusion, ensuring cyber-security approaches support accessible, inclusive and fair services. ▪ High levels of integrity, professionalism and personal accountability, particularly when handling sensitive information and risk decisions. ▪ Forward-looking and proactive, anticipating emerging threats and shaping organisational readiness. Committed to public-service values, transparency and responsible stewardship of public resources.

OUR VALUES AND BEHAVIOURS

Our values and behaviours underpin everything we do.
They guide our interactions with residents, businesses, visitors, partners and each other.
They are also a measure of how well we've done.

	Our Values & Behaviours
D	**PUTTING COMMUNITIES FIRST** • We put local people at the heart of decision making in everything we do. • We seek to include and involve: all voices matter. • We provide quality services that are responsive, effective and efficient. The following examples are indicators of effective behaviour: • I actively involve and include the communities that I serve in my work. • I shall reflect the views of the communities in my daily work. • I shall improve the service I provide through seeking feedback from others.

	Our residents will feel that: • I have been included • I can see how my views have been taken into account • I can see improvements and developments based on my input
E	**RESPECT** • We listen to everyone and value the personal experiences of people in our communities and of each other. • We adopt a fair and involving approach regardless of any way in which an individual is different to us. The following examples are indicators of effective behaviour: • I adapt my approach to take account of all differences and cultures in the community and with colleagues. • I ensure I am equitable and fair by including those who are quiet or may not be able to represent themselves. • I communicate in a way that is respectful, encourages involvement and meets people's needs. Our residents will feel that: • I feel my culture and background are respected. • I have confidence that action is being taken. • I feel I am being treated fairly.
F	**INTEGRITY** • We act with openness, honesty, compassion, responsibility and humility. • We let people know what we are doing and communicate why and how decisions have been made. The following examples are indicators of effective behaviour: • I demonstrate empathy in my interactions with others. • I am honest and transparent about the decisions I take. • I follow through on the actions I say I will take and take ownership for communicating the outcome. Our residents will feel that:

	• I am told when something is not possible, and the reasons why are explained to me. • I feel my perspective is listened to and understood. • I feel my views are valued
G	**WORKING TOGETHER** We work together and in partnership with everyone that has an impact on the lives of our residents. • We want to understand, learn from each other and continually adapt. The following examples are indicators of effective behaviour: • I work with others to provide an effective service for residents, local communities and other departments within the Council. • I seek ways to work with other departments to deliver a seamless service and find opportunities to improve. • I seek out opportunities to learn from my colleagues and build on good practice. Our residents will feel that: • I can get my issue resolved without being passed around departments. • I find it easy to access the services that I need. • I feel the Council is open to new ideas.