

JOB DESCRIPTION

Job title	Security Risk Analyst
Directorate	Resources
Service	Audit, Risk, Fraud and Insurance
Team	Cyber Assurance
Grade	Grade G

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

Responsible to:	Head of Cyber Assurance
Employees directly supervised (if applicable):	None
Organisational structure chart (job titles only, no employee names)	



1. JOB PURPOSE:

1. To strength the Council's cyber security posture by identifying, assessing, and managing cyber and information risks across all services.
2. Reporting to the Head of Cyber Assurance, the role ensures that risks are understood, prioritised, and addressed through appropriate controls.
3. To work closely with ICT, Information Governance, service managers, and external partners assuring that risk controls and actions are successfully embedded and tested on a regular basis.
4. To ensure effective prevention, detection and response mechanisms are in place to mitigate the risks of a cyber attack.

5. DESCRIPTION OF DUTIES:

Key responsibilities

Risk identification and assessment

- Identify, analyse, and document cyber and information risks across the Council's systems, services, suppliers, and processes to enable prioritisation, management, and mitigation of risk.
- Conduct structured risk assessments.
- Evaluate threats, vulnerabilities, likelihood, and impact to produce clear, evidence-based risk ratings.
- Work directly with service areas to build their understanding of cyber and information risks, including those arising from digital transformation, cloud adoption, and third-party systems.

Risk Management and controls

- Work with ICT, Information Governance, and service teams to define appropriate risk treatments, controls, and mitigation plans.
- Track and monitor risk actions, ensuring progress is made and escalating delays or concerns to the Head of Cyber Assurance.
- Review the effectiveness of technical and organisational controls, identifying gaps and recommending improvements.
- Support the development and maintenance of the Council's cyber risk register and associated governance documentation ensuring that services update the register on a regular basis and assessing the mitigations input from services to determine their effectiveness, and to advise on additional controls where needed.

Supplier vetting

- Take responsibility for vetting suppliers who will handle the Council's Information, ensuring Information Security Risk questionnaires are completed for all relevant contracts, and associated actions are followed through. Ensure that any ensuing risks are added to, and tracked within, the cyber risk

register.

- Continually review the Council's ICT asset list to ensure that there are no gaps in security questionnaire completion.
- Act as the Application Owner for the Security Supplier risk management system.
- Maintain regular reporting on supplier risk position.

Governance and reporting

- Prepare clear, concise risk reports for the Head of Cyber Assurance, senior leadership, Information Risk Board and committees as required.
- Document compliance requirements relating to cyber and information security standards, including PSN and oversee and assure the Council's progress towards these, taking inputs from the relevant teams, escalating non-completion to the Head of Cyber Assurance.
- Make recommendations for policy development, ensuring cyber and information risk considerations are embedded in council processes.

Stakeholder engagement

- Champion good practice in engagement with stakeholders cyber and information risk implications of new projects, procurements, and system changes clear.
- Challenge and support managers to embed strong cyber and information security practices within their teams, resulting in improved compliance with policies and reduced risk exposure.
- Promote a risk-aware culture across the organisation, helping non-technical colleagues understand threats and responsibilities.
- Work with suppliers and partners to assess third-party cyber risks and ensure contractual controls are in place.
- Demonstrable commitment to equality, diversity and inclusion in all aspects of engagement and delivery.

Incident support

- Collaborate with the Head of Cyber Assurance and ICT teams in analysing risks arising from security incidents, near misses, or vulnerabilities to gain clear understanding of root caused and risk impacts.
- Carry out lessons-learned reviews and ensure resulting risks are captured and managed appropriately.

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 ICT/Computer Science or related field OR comparable experience within Digital, Data and Technology • Professional certifications e.g. CompTIA • Evidence of continuous professional development in digital, data and technology, including cyber security best practice.

C	Skills, knowledge and experience Person Specification Essential • Experience in cyber security, information risk management, or information governance within a complex organisation. • Strong understanding of cyber threats, vulnerabilities, and common attack vectors. • Familiarity with risk assessment methodologies and frameworks (e.g., National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF), International Organisation for Standardisation (ISO) standard 27001, National Institute of Standards and Technology (NIST). • Knowledge of modern technology environments (cloud services, digital platforms, third-party suppliers). • Ability to translate technical risks into clear, business-focused language including documentation and reporting skills. • Strong analytical and problem-solving skills with attention to detail and accuracy. • Excellent communication and stakeholder engagement skills, able to work effectively with ICT teams, service managers, and senior leaders. • Experience maintaining risk registers and producing risk reports. • Ability to work proactively, managing competing priorities and driving follow-through on risk actions. • Knowledge of UK public sector regulatory requirements including Public Services Network Code of Connection (PSN CoCo), the Data Protection Act 2018, and the UK General Data Protection Regulations (UK GDPR). • Understanding of zero trust, best practice security delivery. • Understanding of business continuity, incident response, and resilience planning.
---	---

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.