Role Profile

Part A - Grade & Structure Information

Job Family Code	**11RT**	**Role Title**	**Senior Security Analyst**
Grade	PS11	**Reports to (role title)**	**Chief Information Security Officer**
		Directorate	**Resources**
JE Band	439-518	**Service**	**IT & Digital**
		Team	**CISO**
		Date Role Profile was created	**26th January 2026**

Part B - Job Family Description

The below profile describes the general nature of work performed at this level as set out in the job family. It is not intended to be a detailed list of all duties and responsibilities which may be required. The role will be further defined by annual objectives, which will be developed with the role holder. The Council reserves the right to review and amend the job families on a regular basis.

Role Purpose including key outputs

Provide a proactive, consistent cyber security operations and assurance capability for IT&D and the council. The postholder will lead day-to-day security monitoring, incident response support, vulnerability management, and security assurance activities, helping to uplift control maturity and reduce risk across on-prem, cloud and supplier-managed services.

Key outputs include:
•High-quality triage and investigation of security alerts, with clear documentation and evidence capture.
•Effective incident response support (playbooks, coordination, post-incident reviews, corrective actions).
•A risk-based vulnerability management and remediation process with measurable improvement.
•Improved visibility and monitoring coverage (including priority supplier systems where feasible).
•Clear reporting to the CISO and senior stakeholders on trends, risk hot-spots, and control health.
•Policy and process development

Key responsibilities

Security monitoring, triage and investigation
•Monitor SIEM/EDR/NDR and other security tooling; triage alerts, enrich with context, and prioritise based on business impact and likelihood.
•Conduct investigations across identity, endpoint, email, cloud and network, working with IT & D colleagues and suppliers to contain and eradicate threats.
•Maintain case notes, timelines, and evidence suitable for audit and lessons learned.
Incident response and readiness
•Support operational incident response, including coordination, communications inputs, and stakeholder updates (internal and external as appropriate).
•Develop and maintain practical incident playbooks (for example phishing/BEC, compromised accounts, malware outbreaks, ransomware precursors).
•Contribute to incident exercises and ensure learning is translated into actions that are tracked to closure.
Vulnerability and exposure management
•Operate a vulnerability management lifecycle: validation, risk rating, assignment, remediation tracking, exception handling and reporting.
•Work with service owners to reduce exposure windows, improve patch cadence, and manage legacy or unsupported technology risks.
Threat intelligence and detection improvement
•Consume relevant alerts and advisories (including NCSC and key vendors) and translate these into actionable defensive measures.
•Tune detection content to reduce noise and improve fidelity; propose monitoring improvements based on emerging threats and observed incidents.
Security assurance and supplier engagement
•Support proportionate assurance of supplier controls, including evidence collection, incident notification routes, and monitoring/logging integration requests.
•Contribute to security reviews for new or changed services (including cloud/SaaS), ensuring security requirements are understood and tracked.
Reporting and governance support
•Produce regular operational reporting for the CISO, including incident metrics, vulnerability position, trend analysis, and control performance.
•Support audits and assessments by gathering evidence and demonstrating operation of controls.
•Develop policies and procedures in support of improving the security posture for Surrey CC

Work Context

IT&D is the IT and digital service supporting Surrey County Council. The cyber security function operates across a complex hybrid estate spanning cloud, on-premises, and supplier-managed services, supporting both corporate and frontline systems. The Security Analyst works closely with IT operations, service owners, information governance, and suppliers to monitor for threats, investigate security events, support incident response, and drive vulnerability remediation. The role requires sound judgement, clear documentation, and the ability to balance risk reduction with service continuity in a public services environment.

Line management responsibility if applicable

None

Budget responsibility if applicable

None

Representative Accountabilities Typical accountabilities in roles at this level in this job family	Planning & Organising • Direct, manage and monitor the operation of an efficient and effective service ensuring the work of the team supports service objectives and that necessary resources are secured. • Lead major projects and reviews within a defined area of work to optimise and enhance service delivery. Policy & Compliance • Ensure legal, regulatory and policy compliance of relevant schemes/ initiatives. • Contribute to and where appropriate lead the development of practical strategies, works programmes and service improvement in own area of specialism and monitor and control their implementation to manage and mitigate risks. People and partnerships • Directly or matrix manage a diverse group of staff to ensure the successful delivery of a service. • Monitor and support the performance management and development of team members using a coaching approach, to support individual development and ensure that individual contributions are maximised. • Work with managers, service representatives and partners to identify and apply cost effective means of delivering improvements to business processes and strategies. Resources • Review the operations of the teams to identify improvements in systems, processes, procedures and working methods, and propose changes to secure greater efficiency and compliance. • Monitor, analyse and manage delegated budgets, funding and resources in accordance with council policies and procedures. Analysis, Reporting & Documentation • Analyse, interpret and evaluate relevant data applying judgment and technical expertise to identify risk, support the resolution of issues and support decision making. • Through management and supervision ensure that appropriate record keeping is kept and risks and issues are identified and actions taken. Duties for all Values: To uphold the values and behaviours of the organisation. Equality & Diversity: To work inclusively, with a diverse range of stakeholders and promote equality of opportunity. Health, Safety & Welfare: To maintain high standards of Health, Safety and Welfare at work and take reasonable care for the health and safety of themselves and others.
Education, Knowledge, Skills & Abilities, Experience and Personal Characteristics	• Degree/ HNC or equivalent, or substantial relevant experience in a relevant subject. • May be required legislatively to maintain a professional qualification or competency. • Substantial practical or professional experience and understanding of a specialist area or supporting service teams and/or providing support to the public. • Excellent understanding of subject matter, principles and practices relevant to technical area. • Proven ability to apply project management principles and techniques to a wide range of complex projects or programmes. • Extensive knowledge of principles, practices, and procedures relating to business planning and financial management • Ability to collate, monitor and interpret a range of data. • Proven ability to establish and maintain highly effective working relationships with a range of stakeholders. • Comprehensive knowledge of computerised business systems • Proven written and oral communication with the ability to influence and work in collaboration with others. • Excellent management skills with proven experience motivating, coaching, mentoring and developing staff.
Details of the specific qualifications and/or experience if required for the role in line with the above description	Degree level or equivalent in a relevant subject and/or relevant professional qualification. Proven ability to interpret and analyse information and formulate and present reports and recommendations. High level of skill in the use of IT/digital media and software applications Willingness and ability to travel around the county and work outside normal office hours. Evidence of continuing professional development in cyber security. Desirable: CISSP, SC-200, CySA+, Security+, GCIH/GMON or similar; ITIL Foundation

Role Summary	Roles at this level typically have significant management responsibility either for a large team or coordinating sub functions within a service, and/or will provide professional, specialist or high level technical advice, direction and input across a wide range of activities. They require a conceptual understanding of a technical, professional or specialised field, and job holders require the knowledge and experience to handle and resolve complex issues, anticipate problems and recommend solutions. There will be a requirement to plan and organise own and/or team activity over a significant time scale and coordinate work with associated functions. They will typically be required to influence/motivate others both inside and outside immediate reporting lines, including external stakeholders, and have a primary role in setting service levels. They ensure that their services achieve the agreed financial and service standards, and will have professional autonomy and discretion within operational policies and practice guidance.
Reference Number	BM-2026-065