Role Profile

Part A - Grade & Structure Information

Job Family Code	**13RT**	**Role Title**	**Chief Information Security Officer (CISO)**
Grade	PS13	**Reports to (role title)**	**Chief Digital and Information Officer (CDIO)**
		Directorate	**Resources**
JE Band	614-734	**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	The CISO leads cyber security strategy and delivery across a complex hybrid estate spanning cloud, on-premises and supplier-managed services, ensuring that confidentiality, integrity and availability risks are understood, governed and reduced in a way that supports critical public services. This is a hands-on leadership role expected to drive rapid maturity uplift as well as set longer-term direction, including establishing clear governance, risk management and assurance. Key outputs include: •A clear, agreed cyber strategy and roadmap for IT&D, aligned to risk appetite and service priorities. •Strengthened cyber governance, including defined roles, responsibilities and decisions. •Improved incident response readiness, exercising, and coordinated response with suppliers and information governance functions. •Measurable improvements in vulnerability management, logging/monitoring coverage, and supplier assurance. •Clear reporting to senior stakeholders on risk, control effectiveness, and progress against agreed priorities. Leadership, strategy and culture •Set the cyber security vision, principles and priorities across IT&D, balancing risk reduction with service continuity and delivery. •Embed security into organisational culture through targeted engagement, pragmatic guidance, and role-based expectations for key groups (admins, system owners, service owners and leaders). •Build and lead a cyber security function, including matrix management across ICT and suppliers where required. Governance, risk and assurance •Establish and maintain a consistent cyber governance approach across the , including forums, reporting, escalation routes and decision-making. •Own the cyber risk management approach, ensuring risks are identified, assessed, prioritised, assigned and tracked, with clear reporting to senior stakeholders and audit. •Implement a proportionate control assurance and performance approach, using evidence from tools and processes to validate that controls operate as intended. Security operations and incident management •Lead and oversee response to cyber threats and incidents, ensuring robust incident management, recovery coordination, and lessons learned are embedded. •Ensure documented incident response plans, playbooks, severity criteria, and escalation paths exist, including for supplier incidents and cross-council impacts. •Establish a formal cyber exercise programme (tabletop and technical), involving ICT, information governance and key suppliers. Technology, architecture and control uplift •Oversee effective use of security technologies and controls, ensuring configuration, coverage and alerting are fit for purpose. •Drive improvements in vulnerability management, patching governance and exception handling, ensuring risk-based prioritisation and measurable remediation progress. •Improve visibility across the estate, including logging/monitoring coverage and critical service dependencies, prioritising areas of greatest risk. Supplier and third-party security •Define and enforce cyber assurance expectations in procurement and contract renewal, including minimum security requirements, incident notification, and evidence-based assurance for critical suppliers. •Ensure supplier relationships support timely risk mitigation, vulnerability disclosure, logging requirements and coordinated incident response. Policy, standards and compliance •Develop, implement and maintain cyber security policies, standards and procedures that reflect the shared-service operating model and are supported by measurable assurance. •Provide expert guidance on compliance and regulatory obligations (for example UK GDPR and ICO expectations), working closely with information governance colleagues. Representative accountabilities Analysis, reporting and documentation •Provide clear, evidence-based reporting on threat landscape, incident trends, control performance, and cyber risk posture, tailored to senior audiences. Planning and organising
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 CISO works closely with IT operations, service owners, information governance, and suppliers to oversee cyber security governance and maturity. 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	Yes (cyber security function, including analysts and/or virtual team members via matrix management)
Budget responsibility if applicable	Yes, c £1.5m investment into improving Cyber Security at the SCC.
Representative Accountabilities Typical accountabilities in roles at this level in this job family	Planning & Organising • Plan, organise and control the work of the service area to deliver organisation's objectives. • Lead the formulation of strategic longer term plans for the area to fit broader functional and council strategy. • Translate strategic objectives into operational plans and initiatives and manage their effective delivery. • Lead major projects and reviews and represent the business area in internal and/or external initiatives to enhance reputation and service delivery. Policy & Compliance • Ensure legal, regulatory and policy compliance of technically complex or high profile schemes/ initiatives. • Lead the development of strategic policy in own area of specialism and monitor and control its implementation. People and Partnerships • Lead and manage a group of staff across a function/service, or as a significant part of a wide function to ensure programmes of work are effectively delivered. • Work collaboratively with a range of agencies and partners to develop innovative solutions, and promote and coordinate initiatives to achieve business plan objectives and targets. Resources • Plan, control and monitor allocation and use of allocated budget/resources/funding effectively to ensure maximum value is delivered. Analysis, Reporting & Documentation • Apply specialist expertise and use judgment to make decisions where solutions are not obvious. • Identify issues and trends that may have an impact in their area of responsibility to enable and ensure that appropriate action is 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 or equivalent professional qualification plus a relevant technical qualification or equivalent experience in the specialist area. • Membership of an appropriate professional body may be required. • Substantial experience working at a senior level in a relevant role. • Authoritative knowledge of the legislation, regulations and technical requirements relevant to the role. • Proven ability to manage budgets and resources. • Proven ability to deliver technically complex programmes of work to deliver agreed outcomes and objectives. • Comprehensive knowledge of computerised business systems. • Excellent verbal and written communication and interpersonal skills with high level negotiation and influencing skills. • High levels of political awareness and acumen. • Proven ability to work collaboratively with internal and external partners/professionals. • Advanced problem solving and analytical skills with the capacity to devise and implement innovative solutions for strategic change. • Proven ability to assess risks and benefits in a complex environment and respond appropriately. • Clear evidence of political sensitivity and awareness. • Excellent leadership skills with substantial experience in 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	•Significant senior cyber security leadership experience, ideally in a complex, multi-stakeholder environment. •Strong capability operating at both strategic and hands-on levels, with evidence of delivering measurable improvements in security posture. •Deep understanding of cyber risk management, governance and assurance, including establishing practical controls and evidence-based reporting. •Proven incident leadership experience, including planning, exercising, and coordinating response and recovery with internal teams and suppliers. •Excellent communication and stakeholder management skills, with the ability to influence senior leaders, technical teams and third parties. •Familiarity with common cyber maturity frameworks and approaches (for example NIST CSF and/or NCSC-aligned approaches). Professional qualifications •CISSP, CISM (or equivalent) is strongly preferred.
Role Summary	Roles at this level involve significant coordination of services of a technical or specialist nature and will typically engage with a range of agencies, internal and external partners. They will manage a professionally qualified team to deliver major technical projects and/regulatory services. They have a key role in regulatory assessment, decision and enforcement and require a high degree of technical/specialist knowledge and expertise which is used to exercise a significant degree of judgement and decision making in their area within broad parameters and policy guidance. Roles at this level are accountable for the professionalism of technical or regulatory services under their remit.
Reference Number	BM-2026-064