



PAY & GRADING - JOB SPECIFICATION TEMPLATE

This Job Specification sheet covers specific areas of activities that are not included in the Generic Role Profile. It will include responsibilities, knowledge, skills, delivery and working arrangements relevant to this role. Please ensure that this is read and in conjunction with the given family role for the post.

Profile Owner: Service Director, IT & Digital

POLICE STAFF

ROLE SPECIFIC INFORMATION	
Job Title:	Head of Cyber Security and Information Assurance
Generic Role Profile:	IT
Salary Band:	Grade 11
Operational / Non Operational Role	Non-operational
Vetting Level:	Standard Vetting (MV) with SC
Reporting to:	Head of Architecture Management
Specific Role Purpose:	West Midlands Police have completed a large-scale digital transformation programme, and therefore technologies such as Cloud, Artificial Intelligence, Automation and Mobility are no longer visionary – they underpin policing today. The next stage in our technology ambition is focused around the concept of Synergy and delivering secure, resilient and exceptional services. This role will focus and shape our path in the Synergy strategy as it relates to cyber security and assurance—strengthening our ability to prevent, detect, respond and recover from cyber threats—thus driving real-world impact on policing technology and our mission to prevent crime, protect the public and help those in need. Aligned to IT&D Synergy 2030, this role will embed security as an enabler. Security must be seamless, invisible and silent in enablement—delivering frictionless, secure user journeys while assuring risk, compliance and resilience. You will continue to embed security from the start of projects utilising SbD (Secure by Design) principles. In this fast-paced and diverse role you will be responsible for West Midlands Police’s technical cyber security and information assurance capabilities. You’ll be instrumental in ensuring that the department can effectively understand, detect, investigate and respond to cyber security threats and vulnerabilities. This is a senior leadership opportunity. Leading a specialist team, you will own the operational cyber security and information assurance function, ensuring our capability to understand, detect, investigate and respond to threats and vulnerabilities across a large-scale organisation (~15,000 employees) and associated cloud/on-prem infrastructure. You will work closely with the Deputy for IT&Digital to design and drive implementation of the cyber security strategy and roadmap, deputising at senior

	governance forums (Digital Senior Leadership Team, Technical Design Authority, and programme boards). This is a one-of-a-kind opportunity, leading a small team - we want you to help take our policing technology cyber security and information assurance level to exceptional. This new role will own the “Defend as One” security arm of the Synergy 2030 technology strategy. You will be joining a dept that is consider a highly regarded “technology partner” to our organisation and post our digital transformation we need someone to think creatively around some of the existing and new security, information and cyber challenges that our organisation faces.
Key Responsibilities:	The Head of Cyber Security and Information Assurance is responsible for the following key areas; • Lead and be accountable for the Cyber Security and Assurance function—providing strategic direction and day-to-day coordination of security governance, risk management, incident response, threat detection, vulnerability management and information assurance activity. • Accountable as technical lead for major cyber security incidents and critical vulnerabilities impacting West Midlands Police. • Establish, own and continuously improve the security operations target operating model (processes, playbooks, tooling, coverage, KPIs). Leveraging suitable frameworks such as SABSA for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives. • Lead creation, publication and maintenance of Information Assurance and Cyber Security policies, procedures and standards—align to NCSC, Government Security Group and NIST CSF; operating proportionate policy exceptions. • Accountable for West Midlands Police SyAp (Security Assessment in Policing) across all controls and national submission. • Operate and chair the Cyber Security Assurance Board (CSAB) aligned to NIST CSF, report on vulnerabilities, patching compliance, configuration drift, security risk, ITHC status, security exceptions and Security Assessment in Policing (SyAP) progress. • Accountable for IT&D departmental risk management: maintain and govern the departmental risk register; ensure cyber/IA risks have owners, mitigation plans and review cycles; align to Force Risk process and escalate to SIRO/SLT as appropriate. • Refine and lead the Information Assurance team on the governance, standards and Information Security risk assessments created to support projects/programmes and standard operation. Effectively safeguarding our data in the digital world. Manage the Data Protection Impact Assessment (DPIA) process for applications in conjunction with the Force DPO (Data Protection Officer). • Set risk appetite and tolerances for cyber and information security (with Senior Leadership Team and Force SIRO) and embed risk-based decision making in design and change.

	• Leadership and champion of “Secure by Design (SbD)” and embed cyber security and information assurance across teams, functions and major programmes. • Serve as the “Voice of Security, Cyber and Information” at Technical Design Authority and other technical governance forums; provide risk-based advice and challenge. • Brief senior stakeholders on threats, vulnerabilities, incidents, mitigations and residual risks; produce clear executive reporting and dashboards. • Accountable for developing and maintain incident response plans and playbooks (e.g. ransomware, data loss, DDoS) and lead exercising and lessons-learned. • Collaborate with National Technical Authorities—NCSC, Government Security Group (Cabinet Office), NPCC—and law enforcement to share intelligence and coordinate responses. • Oversee security monitoring and threat detection capabilities (SIEM, EDR/XDR, SOAR) across cloud (M365/Azure) and on-prem environments. • Be accountable and lead all Cyber Security and Information Assurance audits aligned to the CSAB and their remediations with Senior Leadership Team, for example Proxy/Firewall audits, cloud security and internal phishing exercising. • Establish and Lead Wargaming exercises internally (and with external suppliers) across a diverse range of technical teams in response to simulated cyber events. • Own vulnerability management lifecycle—asset coverage, scanning, prioritisation (risk-based), remediation and reporting. • Drive supply-chain and cloud security assurance, including identity and access management, zero trust principles and privileged access controls. • Ensure compliance with relevant policies and standards (e.g. NIST CSF, ISO/IEC 27001, NCSC guidance) and manage audit actions to closure. • Manage six figure budgets and resources for cyber operations and assurance; developing business cases for capability uplift as required. • Champion cyber security culture, awareness and training across the organisation; act as an evangelist for continual improvement. • Accountable for Cyber Security and Assurance KPIs and associated management reporting/ Dashboards into Senior Leadership Team. • Represent WMP on National Cyber/Security related boards and programmes (NIRMA, PIAB) with stakeholders at CSUPT/Director level. • As a Certified Information Systems Security Professional (CISSP) you will lead a team of Grade 10 (Manager) post (Information Security Manager), a team of SIRA’s (Information Security & Assurance Security Risk Advisor), a Senior IT Security Officer, and ITSO posts. • Ensure that WMP continues to meet it legal obligations and requirements around Information Security standards including Information Commissioners Office (ICO) alignment.
--	---

	• The post holder is responsible to the Senior Leadership Team but will be expected to work without direct supervision and will be required to make decisions using their own initiative and experience.
--	--

SPECIFIC COMPETENCIES REQUIRED FOR EFFECTIVE PERFORMANCE	
Knowledge & Experience	
<i>This section should detail the requirement of previous experiences and knowledge gained from academic qualifications if appropriate. e.g. significant experience of administrative duties, degree level educated.</i>	
Essential:	• Proven experience setting-up new and leading operational cyber security and information assurance functions (SOC/IR/Vulnerability Management) in a complex organisation. • Track record designing and delivering cyber security capabilities and operating models. • Experience building, developing and managing diverse, high-performing teams. • Strong operational and strategic planning capability; risk-based decision making. • Comprehensive technical understanding of cyber threats, vulnerabilities and mitigations. • Comprehensive experience in managing security for large-scale Enterprise technology solutions. • Excellent communication skills; clear and concise briefings for senior stakeholders on complex issues. • Ability to influence and coordinate activities across multiple teams and suppliers; strong stakeholder management. • Hands-on familiarity with SIEM/EDR/XDR/SOAR and cloud security controls (M365/Azure/AWS). • Experience with DLP (Data Loss Prevention) technologies and implementation/operation in large scale organisations. • Experience managing KPIs/SLAs and performance reporting for security operations and information assurance functions. • Experience leading technical responses to major security technical incidents and coordinating enterprise recovery. • Technical experience in relation to Network Security Operations and associated appliances (Firewall operations, PKI capabilities, encryption).

	• Experience authoring and maintaining security policies, procedures and standards; including operating policy exceptions. • Experience of leading, managing and identifying technical and security risks in a large-scale enterprise organisation. • Experience of creating and reviewing DPIAs in relation to technology, security and cyber capabilities. • Experience in the review and approval of Information Security Risk Assessments, including remediation plans and full accountability of those assessments and recommendations. • Experience in the drafting and review of ITHC (penetration testing), including scope drafting and annual renewals, including the full remediation of associated recommendations. • Experience of Enterprise “patch management” best practice and practical process in relation to Operating Systems across a large diverse technology landscape. • Experience in management of an organisations Cyber Response Plan, including the review, drafting, embedding, auditing and exercising of said plan. • Experience in down-selecting and formally drafting written tender requests for external suppliers, including security, cyber and information assurance requirement management (functional and non-functional). For example SOW (Statement of works) and associated processes. • Experience in leading (and Chairing) large governance boards around cyber security and information assurance with diverse stakeholders. • Proven leadership skills in an enterprise sized organisation. • Cyber and Security architecture technical design and engineering skills, via an IT cloud related certification from one of the public cloud providers (AWS, Microsoft, Oracle or Google) at Associate level. • Peer review and challenge ability for complex Solution Designs from a Cyber, Security and Information Assurance perspective. • Identifying and managing risks in relation to cyber, security and information assurance Solution Designs (low level). • Professional certifications: CISSP (minimum), plus one or more of CISM, CRISC, ISO 27001 Lead Auditor/Implementer, GIAC (e.g. GCIA, GCIH, GCED), CEH) and Experience of SABSA. • Experience applying Security Frameworks and associated advice from industry bodies (NCSC, NIST etc) in large enterprise organisations, especially in relation to the Cyber Security Framework (CSF) and associated controls.
--	--

	• University Degree in related topic at Masters or BSc level. • Understanding of new and emerging technologies (cloud-native, AI, IoT) and their security implications for public services. • Experience of detailed technical analysis to gather existing 'as-is' state of landscape across systems and platforms in relation to security. • Experience in formulating roadmaps to showcase future security direction and alignment to strategic direction. • Experience in line management of individuals, including performance appraisals, workload and wellbeing. • Ability to present formally to a range of senior stakeholders, for example technical experts and senior leadership teams and suppliers. • Comprehensive specialist technical knowledge, certification and experience of Cyber Security and Assurance as it relates to a large-scale organisation. • Strong stakeholder management skills and ability to communicate and negotiate with many stakeholder groups, in particular senior leaders and executives. Including demonstrable ability to build consensus across diverse stakeholder groups. • Demonstrable experience in reviewing and challenging technical designs and architecture in relation to Security viewpoints, standards and principals. • Demonstrable experience of directly communicating with senior managers from a professional perspective using written and oral methods; • Participate in, and chair, meetings both locally and at national level (representing an authority in cyber security on behalf of the organisation); • Promote equality, diversity and Human Rights in working practices; • Ability to work with national Chief Information Security Officers (CISO) to define organisational level outcomes around cyber security and assurance. • Experience of formal audit processes and approach in relation to cyber, security and information assurance (via internal audits or via external 3rd party suppliers). • Maintain standards for security of information, alongside Secure by Design principles of good security architecture.
Desirable:	• Experience with police sector assurance regimes (e.g. SyAP) and national governance structures. • Understanding of ITIL practices in the context of security operations.

Skills <i>This section should detail the competency requirement which could be developed through non formal training. e.g. effective time management, influencing and negotiating, effective communication including written and verbal.</i> <i>Refer to skills database for core operational skills</i>	
Essential:	Must have skills in relation to; • Connecting with people, listening and learning around our User Communities and being able to empathise with User viewpoints. • Strong interpersonal and influencing skills with the ability to communicate effectively at very senior levels (Senior Leadership Team and Executive level) both locally within force and nationally. • First class technical analytical skills, both in understanding as-is landscape and to-be state in relation to systems and platforms and how they are impacting user experience. • Experience of working on end to end technical solutions that encompass various systems and software – with a viewpoint on security, cyber and information assurance and providing proposals on those technical solution options for further consideration. • Specialist technical skills from a support or design background with experience of working within a technical domain (Infrastructure, Applications, Cloud Services, Integrations, Identity, Authentication or End User Devices) • Proven ability to shape business requirements and align solutions based on those requirements. • Excellent presentation and organisational skills, having an ability to work under pressure and be capable of balancing competing demands and priorities. • Ability to negotiate and influence with suppliers regarding technical solutions.
Desirable:	- An understanding of the ITIL processes as they apply to a large scale organisation.

IT gets more complex and pervasive there is an ever-growing need clearly to define, recruit and grow the skilled resources that you need. SFIA provides a language that is the foundation for consistent, unambiguous and clear definitions of IT based skills. The below skillset is based on the latest SFIA (Skills Framework for the Information Age).

SFIA Category	Level	High-Level Description	Role Relevant Interpretation
Security	6–7	Establishes organisational security strategy, governance and controls.	Sets enterprise cyber strategy; ensures controls are proportionate to risk; leads security posture.
Security	6	Provides authoritative assurance over information risk and controls.	Owns assurance framework; validates control effectiveness; leads audit & assurance programmes.
Strategy & Architecture	6–7	Defines risk appetite, governance and enterprise risk processes.	Oversees cyber risk governance; ensures alignment with legal/regulatory requirements.
Strategy & Architecture	6–7	Establishes policies, standards, and organisational governance.	Owns cyber security policies; ensures compliance with UK Gov Security Function guidance.
Security	5–6	Plans and oversees security testing activities.	Directs penetration testing, vulnerability management and assurance testing.
Assurance	6	Leads audit strategy and ensures compliance.	Oversees cyber audit programmes; ensures controls meet risk management plans.
Strategy & Architecture	6	Aligns risk with organisational mission and business context.	Advises senior leadership on cyber risk impact to public services.
Strategy & Architecture	6	Sets architectural direction and standards.	Ensures security architecture aligns with organisational strategy and threat landscape.
Change	6	Leads organisational change initiatives.	Embeds security culture; drives cross-government security-mindedness.
Relationships	6–7	Manages complex stakeholder relationships at senior levels.	Acts as primary cyber security contact for internal/external stakeholders.
People	6–7	Sets direction, inspires teams, builds capability.	Builds diverse cyber workforce; champions accreditation and professional development.
Strategy & Architecture	6	Provides authoritative advice and guidance.	Advises execs on cyber risk, threat trends, and strategic decisions.
Security	6	Oversees major incident response and recovery.	Ensures organisation has robust IR capability aligned to UK Gov standards.

Assurance	6	Ensures adherence to legal, regulatory and policy requirements.	Oversees compliance with data protection, privacy, and government security policies.
-----------	---	---	--

Hours of Work and Flexibility:	Standard Office Hours in relation to WMP staff. Typically; 37.5 hrs per week. Flexible patterns of start/end time (8~4/9~5)
Agile Work Style: (if applicable)	The role is an Agile worker role, based at Lloyd House Headquarters and issued the relevant technology in order to facilitate agile working at multiple locations in alignment with West Midlands Police policy agile working policy.

Restriction Level:	
--------------------	--