

# Role Profile and Person Specification

## ROLE PROFILE

<b>Role Title:</b>	Senior Information Security Analyst	<b>Leadership level:</b>	<i>To be determined at later phase</i>
<b>Post reference:</b>	20881 /20882	<b>Job family:</b>	<i>To be determined at later phase</i>
<b>Grade:</b>	I	<b>Location:</b>	Bedlington Police Station/Remote
<b>Allowances:</b>	Not Applicable	<b>Politically restricted post:</b>	No
<b>Area command / Department:</b>	Information Management Unit	<b>Vetting level:</b>	MV and SC Level Clearance
<b>Reporting to:</b>	Information Security and Assurance Manager	<b>Date accepted as a role profile:</b>	
<b>Posts responsible for:</b>	Allocated staff and volunteers		

### Part A – Job Description

#### Overall purpose of the role:

To provide professional guidance and specialist advice with regard to all information security, assurance and risk matters and ensure implementation of all necessary policies, procedures and processes to achieve compliance with national codes of connection for Police information systems. Management of Information Management functions specific to role, which may include the following: Record Review, Data Quality, Information Assessment, Accreditation and Cyber Support.

#### Key responsibilities of the role:

<b>1</b>	To support the Northumbria Police Information Security and Assurance programme to enable accreditation, assurance and compliance with wider mandatory information security requirements and national reporting standards.
<b>2</b>	To develop, review and implement policies and best practice for the ongoing management and maintenance of information security and assurance management – incorporating risk management, record review, accreditation and information system audit.
<b>3</b>	To implement processes and techniques to regularly assess information assets for compliance with security policies, national policing and best practice information assurance standards, legal and regulatory requirements.
<b>4</b>	To ensure information security and assurance audits and compliance assessments are undertaken to ensure the physical and data security protection of all information systems and information assets and compliance with information security regulations, standards, policies, and information risk management.

# Role Profile and Person Specification

5	To identify information security and assurance requirements where there are new or changed processes, information assets or activities; working with departments and business areas and Project Leads to ensure that appropriate assurance is undertaken and documents such as Information Risk Assessment Reports (IRAR) are created.
6	Co-ordinate investigative and reporting action of all actual and suspected information security incidents, ensuring that action is taken to prevent reoccurrence and incident trends are monitored to inform organisational learning.
7	To design, deliver and evaluate information security training, education, and awareness in relation to information security, information assurance and information risks.
8	To actively engage all key stakeholders, including partner agencies and third party suppliers, sharing, storing or processing information owned by Northumbria Police in the application of information security best practice and HMG standards, ensuring compliance with legalisation, statutory requirements, national and best practice standards Home Office legislation and statutory guidance.
9	To maintain awareness and up to date knowledge of all current relevant information security management legislation, methods and practices ensuring that an environment of continuous improvement, innovation and emerging best practice are evaluated.
10	Represent professionally and promote the reputation of Northumbria Police at meetings and groups both internally and externally, including the development of appropriate and constructive partnerships with relevant organisations.
11	Manage and supervise allocated staff, undertaking recruitment, appraisals, development and discipline of staff ensuring that all staff have the knowledge, skills and experience to achieve required standards and performance. Manage welfare and development and ensuring high levels of motivation.

## Part B – Scope of contacts

### Internal / External relationships:

**Internal:** Heads of Department/Area Commanders, Police Officers and Police Staff of all ranks/levels and those officers in specialist operational roles such as Safeguarding, Covert Policing and NERSOU, alongside Contractors and Volunteers. Includes extensive regular contact with Police Staff in Digital Policing, Procurement, People Development and Professional Standards.

**External:** Senior Officers and Staff (Information Management/Security Peers in the main) at other Police Forces, Home Office, National Management Centre (NMC) for Cyber, Office of the Police and

# Role Profile and Person Specification

Crime Commissioner, National Police Chiefs Council (NPCC), College of Policing, Regulatory Bodies such as the Information Commissioners Office (ICO), National Police Information Risk Management Team (NPIRMT), Supplier Companies.

## Part C – Competencies and Values

### Northumbria competencies and values framework (NCVF)

*Level – tbc*

## Part D – Continuous Professional Development (CPD) role 6 months *To be determined*

### First 6 months

1

2

3

4

### 12 months and beyond

5

6

7

8

## Part E - PERSON SPECIFICATION

Criteria	Essential	Desirable	How to be assessed
Qualifications, knowledge and experience	Technology and ICT background  Knowledge of Information Security and Risk accreditation processes,	Possess the Certificate in Information Security Management Principles (CISMP) certification.	Application/interview/CPD

# Role Profile and Person Specification

	<p>including risk assessment and reporting.</p> <p>Experience in supporting internal investigations (relating to Information Security Threats and Data Breaches) or relevant experience in data protection.</p> <p>Proven ability to interpret legislation and advise on changes to working practices.</p> <p>Experience of working with a range of national and local Information Systems</p>	<p>Possess Certificate Cyber Professional (CCP) for Security and Information Risk Adviser (SIRA) and Information Assurance Auditor (IAA) certification.</p> <p>Knowledge of Management of Police Information (MoPI) and associated records management retention guidelines.</p> <p>Understanding of the Data Protection Act (2018), both General Data Protection Regulations (GDPR) and the Law Enforcement Directive.</p> <p>Accredited ISO27001 Internal Auditor certification or understanding and experience as an Auditor.</p>	
Planning and organising	<p>Proven ability to manage own workload with competing demands and deadlines.</p> <p>Understanding the assessment, recording and monitoring of risk from an organisational and person specific perspective and to manage matters in accordance.</p>	<p>Ability to prioritise the workloads self and others and to implement measures to monitor productivity.</p>	Application/interview/ CPD
Problem solving and initiative	<p>Understands the wider implications of risks related to decision making and process and actively escalates where appropriate.</p> <p>Seeks to find solutions to problems with competing interdependencies.</p>		Application/interview/ CPD

# Role Profile and Person Specification

Management and teamwork	<p>Professional attitude to work and able to communicate in a confident manner with people of all levels within and outside of the Force.</p> <p>Experience of managing a small team, maintaining high levels of performance and service delivery.</p> <p>Able to work both as part of a team and independently.</p> <p>Possess the ability to organise, develop and motivate staff and develop processes to meet anticipated service demands.</p>	<p>Understanding of staff recruitment, appraisal, grievance, and training processes.</p> <p>Ability to deliver training provision to a range of audiences, including both coaching and mentoring.</p>	Application/interview/CPD
Communicating and influencing	<p>Able to communicate at all levels within the organisation and participate in meetings and briefings at a senior level.</p> <p>Ability to communicate with national bodies on matters such as compliance, security and accreditation.</p> <p>Effective, pragmatic negotiating and influencing skills</p>	<p>Ability to communicate with external suppliers regarding risk and assurance processes.</p>	Application/interview/CPD
Other skills and behaviours	<p>Must have a flexible approach with the ability to develop new ideas to improve security efficiency</p> <p>Keen interest in all matters relating to Information Management and specifically Information Security and Risk Management, the</p>	<p>Ability to interpret complex technical information security, assurance, and risk documentation</p> <p>Proven experience of writing reports and board papers for a range of audiences.</p>	Application/interview/CPD

# Role Profile and Person Specification

	associated legislation and accreditation.		
--	---	--	--