



# Role Description

## Manager - Cyber Security Threat and Vulnerability

Cluster	Stronger Communities
Agency	NSW Police Force
Command/Business Unit	Technology Command
Location	Various
Classification/Grade/Band	CSO6
ANZSCO Code	135199
PCAT Code	3326192
NSWPF Role Number	RD 1007
Date of Approval	02/04/2024
Agency Website	<a href="http://www.police.nsw.gov.au">www.police.nsw.gov.au</a>

### Agency overview

The NSW Police Force (NSWPF) vision is for *A Safer New South Wales*, which is achieved by police working with the community to prevent, disrupt and respond to crime.

It is one of the largest police forces in the western world, with more than 20,000 NSW Police Force employees, including more than 17,000 sworn officers providing a range of law and order services 24 hours a day, seven days a week to the socially, geographically and culturally diverse community of NSW.

The organisation has four function lines, based across a number of locations. Metropolitan Field Operations and Regional NSW Field Operations provide frontline services directly to the community. Investigations & Counter Terrorism provides investigative, technical and counter terrorism expertise. Corporate Services, provides business support services such as technology and communication, education and training and corporate human resources functions.

The NSW Police Force is a proud employer of a diverse range of people. This includes, but is not limited to, people who identify as Aboriginal or Torres Strait Islander, LGBTIQ, people with disability, people who come from a variety of cultural, religious or ethnic backgrounds, and workers of all ages. The NSWPF is committed to reflecting the diverse community we serve and creating an inclusive and respectful workplace for all employees, where difference is embraced, contributions are valued, and everyone has a sense of connection and belonging. This enables the growth and development of a talented and diverse workforce across the state, in a wide range of roles, at all levels.

The NSWPF *Statement of Values* and *Code of Conduct & Ethics* outlines appropriate behaviour for all NSW Police Force staff. All employees of NSWPF are expected to ensure ethics are incorporated into all aspects of their work making ethical behaviour, practices and decision making a part of daily routine. This further extends to ensuring confidentiality and information security is maintained at all times.

Work, Health and Safety legislation requires all employees to have specific responsibilities. This role is responsible for identifying, assessing, prioritising and controlling health and safety risks, and ensuring that safe systems of work are developed, documented and followed by staff and contractors through appropriate training, supervision and monitoring.

## Primary purpose of the role

The role provides guidance and leadership to the Cyber Security Threat and Vulnerability team. This team is tasked with identifying, monitoring, and evaluating threats from cyber actors, as well as assessing our risk exposure resulting from vulnerabilities within our ecosystem. The role collaborates closely with technology teams to minimise risk exposure and mitigate impacts on police operations.

## Key accountabilities

- Develop and execute cyber threat intelligence and vulnerability management capabilities within the Security Operations Team, to ensure consistency with NSWPF cybersecurity policies and procedures
- Develop and coordinate containment plans for newly identified vulnerabilities to proactively mitigate risks and safeguard the organisational interests of NSWPF
- Manage the cyber threat intelligence generation process and products ensuring comprehensive and timely insights into potential threats
- Oversight of vulnerability management processes, identifying asset owners of vulnerable devices, developing risk-based remediation plans for vulnerabilities and setting priorities for responsible teams
- Lead and manage the Cyber Threat Intelligence (CTI) input into Vulnerability Analysis, Threat Hunting and Forensic Analysis promoting a proactive and strategic approach
- Manage and lead the identification of vulnerabilities to conduct analysis and assessment, including the collaboration with the risk function and security awareness of vulnerabilities, attack techniques, tool/exploit development, intelligence analysis and adversarial tactics across the Cyber Enterprise
- Lead the remediation activities with the required resolver groups for vulnerabilities that are assessed as a risk to NSWPF, overseeing prompt and effective resolution
- Research and analyse threat and vulnerability intelligence to provide actionable data to enable mitigations and countermeasures against potential threats.

## Key challenges

- Build trust and strong cross-functional relationships within the organisation to achieve common goals and outcomes
- Organisational agility and the ability to read the subtle nuances of a situation and react/plan accordingly
- Develop and establish cyber threat and vulnerability management as part of the organisations key tools to minimise cyber threat.

Who	Why
<b>Internal*</b>	
Chief Information Security Officer	<ul style="list-style-type: none"> <li>• Provide expert strategic and technical advice to the CISO to influence decisions regarding Technology initiatives and innovation</li> </ul>
Work Team	<ul style="list-style-type: none"> <li>• Represent work group perspective and share information</li> <li>• Lead discussions and decisions regarding implementation of innovation and best practice</li> </ul>
Client / Customers	<ul style="list-style-type: none"> <li>• Provide strategic advice for business improvement</li> <li>• Provide information regarding agency sector wide rules and standards</li> <li>• Ensure compliance with agency and sector rules and standards</li> </ul>
<b>External</b>	

Who	Why
Vendors/Service Providers and Consultants	<ul style="list-style-type: none"> <li>Communicate needs and resolve issues</li> <li>Engage with vendors, service providers &amp; consultants</li> </ul>

## Role dimensions

### Decision making

The role exercises significant autonomy in setting priorities, independently managing workload, and providing advice within government policies. Responsible for implementing workload, ensuring quality control, and making judgments based on evidence or expert advice, and consulting management on sensitive or high-risk matters.

### Reporting line

- Chief Information Security Officer – SE Band 1

### Direct reports

- Senior Security Administrator – CSO4
- Security Administrator – CSO3

### Budget/Expenditure

- Nil

## Key knowledge and experience

- Demonstrated experience in information security strategy and policy management including managing and designing procedures in running or supporting security operations activities to detect, analyse and respond to events, incidents, and alerts
- Demonstrated experience in Cyber Security Management including Cyber Threat Intelligence and Vulnerability Management and leading security programs within a complex organisation
- Up-to-date knowledge of information security risk management and cybersecurity technologies, methodologies, and trends in both business and IT.

## Essential requirements

- Obtain and maintain the requisite security clearances for this position
- Qualification in computer science, information security/Cyber Security, or a related field.

## Capabilities for the role



The [NSW public sector capability framework](#) describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for roles with managerial responsibilities. These groups, combined with capabilities drawn from occupation-specific capability sets where relevant, work together to provide an understanding of the capabilities needed for the role.

The capabilities are separated into **focus capabilities** and **complementary capabilities**.

## Focus capabilities

*Focus capabilities* are the capabilities considered the most important for effective performance of the role. These capabilities will be assessed at recruitment.


The focus capabilities for this role are shown below with a brief explanation of what each capability covers and the indicators describing the types of behaviours expected at each level.

FOCUS CAPABILITIES			
Capability group/sets	Capability name	Behavioural indicators	Level
<div> Personal Attributes</div>	<b>Act with Integrity</b> Be ethical and professional, and uphold and promote the public sector values	<ul style="list-style-type: none"><li>• Represent the organisation in an honest, ethical and professional way and encourage others to do so</li><li>• Act professionally and support a culture of integrity</li><li>• Identify and explain ethical issues and set an example for others to follow</li><li>• Ensure that others are aware of and understand the legislation and policy framework within which they operate</li><li>• Act to prevent and report misconduct and illegal and inappropriate behaviour</li></ul>	Adept
<div> Relationships</div>	<b>Influence and Negotiate</b> Gain consensus and commitment from others, and resolve issues and conflicts	<ul style="list-style-type: none"><li>• Negotiate from an informed and credible position</li><li>• Lead and facilitate productive discussions with staff and stakeholders</li><li>• Encourage others to talk, share and debate ideas to achieve a consensus</li><li>• Recognise diverse perspectives and the need for compromise in negotiating mutually agreed outcomes</li><li>• Influence others with a fair and considered approach and sound arguments</li><li>• Show sensitivity and understanding in resolving conflicts and differences</li><li>• Manage challenging relationships with internal and external stakeholders</li><li>• Anticipate and minimise conflict</li></ul>	Adept


## FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
 Results	<b>Think and Solve Problems</b> Think, analyse and consider the broader context to develop practical solutions	<ul style="list-style-type: none"> <li>Undertake objective, critical analysis to draw accurate conclusions that recognise and manage contextual issues</li> <li>Work through issues, weigh up alternatives and identify the most effective solutions in collaboration with others</li> <li>Take account of the wider business context when considering options to resolve issues</li> <li>Explore a range of possibilities and creative alternatives to contribute to system, process and business improvements</li> <li>Implement systems and processes that are underpinned by high-quality research and analysis</li> <li>Look for opportunities to design innovative solutions to meet user needs and service demands</li> <li>Evaluate the performance and effectiveness of services, policies and programs against clear criteria</li> </ul>	Advanced
	<b>Demonstrate Accountability</b> Be proactive and responsible for own actions, and adhere to legislation, policy and guidelines	<ul style="list-style-type: none"> <li>Design and develop systems to establish and measure accountabilities</li> <li>Ensure accountabilities are exercised in line with government and business goals</li> <li>Exercise due diligence to ensure work health and safety risks are addressed</li> <li>Oversee quality assurance practices</li> <li>Model the highest standards of financial probity, demonstrating respect for public monies and other resources</li> <li>Monitor and maintain business-unit knowledge of and compliance with legislative and regulatory frameworks</li> <li>Incorporate sound risk management principles and strategies into business planning</li> </ul>	Advanced
 Business Enablers	<b>Procurement and Contract Management</b> Understand and apply procurement processes to ensure effective purchasing and contract performance	<ul style="list-style-type: none"> <li>Understand and comply with legal, policy and organisational guidelines and procedures relating to purchasing</li> <li>Conduct delegated purchasing activities in line with procedures</li> <li>Work with providers, suppliers and contractors to ensure that outcomes are delivered in line with time and quality requirements</li> </ul>	Intermediate

## FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
	<b>Manage and Develop People</b> Engage and motivate staff, and develop capability and potential in others	<ul style="list-style-type: none"> <li>Define and clearly communicate roles, responsibilities and performance standards to achieve team outcomes</li> <li>Adjust performance development processes to meet the diverse abilities and needs of individuals and teams</li> <li>Develop work plans that consider capability, strengths and opportunities for development</li> <li>Be aware of the influences of bias when managing team members</li> <li>Seek feedback on own management capabilities and develop strategies to address any gaps</li> <li>Address and resolve team and individual performance issues, including unsatisfactory performance, in a timely and effective way</li> <li>Monitor and report on team performance in line with established performance development frameworks</li> </ul>	Adept

## Occupation / profession specific capabilities

Capability Set	Category, Sub-category and Skill	Level and Code
	Strategy and Architecture, Governance, Risk and Compliance, Risk Management	Level 5 - BURM
	Strategy and Architecture, Security and Privacy, Threat Intelligence	Level 6 - THIN
	Delivery and Operation, Security Services, Vulnerability Assessment	Level 5 - VUAS
	Strategy and Architecture, Security and Privacy, Information Security	Level 6 - SCTY
	Delivery and Operation, Security Services, Security Operations	Level 5 - SCAD
	Strategy and Architecture, Security and Privacy, Vulnerability Research	Level 5 - VURE








NSW Government employees can access the ICT set through the [Skills Framework for the Information Age](#) Foundation website by registering as a corporate user via their NSW Government email address.

## Complementary capabilities

*Complementary capabilities* are also identified from the Capability Framework and relevant occupation-specific capability sets. They are important to identifying performance required for the role and development opportunities.

Note: capabilities listed as 'not essential' for this role are not relevant for recruitment purposes however may be relevant for future career development.

COMPLEMENTARY CAPABILITIES			
Capability group/sets	Capability name	Description	Level
 Personal Attributes	Display Resilience and Courage	Be open and honest, prepared to express your views, and willing to accept and commit to change	Adept
	Manage Self	Show drive and motivation, an ability to self-reflect and a commitment to learning	Adept
	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Adept
 Relationships	Communicate Effectively	Communicate clearly, actively listen to others, and respond with understanding and respect	Advanced
	Commit to Customer Service	Provide customer-focused services in line with public sector and organisational objectives	Adept
	Work Collaboratively	Collaborate with others and value their contribution	Adept
 Results	Deliver Results	Achieve results through the efficient use of resources and a commitment to quality outcomes	Adept
	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Advanced
 Business Enablers	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Intermediate
	Technology	Understand and use available technologies to maximise efficiencies and effectiveness	Adept
	Project Management	Understand and apply effective planning, coordination and control methods	Intermediate
 People Management	Inspire Direction and Purpose	Communicate goals, priorities and vision, and recognise achievements	Adept
	Optimise Business Outcomes	Manage people and resources effectively to achieve public value	Adept
	Manage Reform and Change	Support, promote and champion change, and assist others to engage with change	Adept



Occupation specific capability set (Skills Framework for the Information Age – SFIA)		
Category, Sub-category	Skill and Level Description	Level and Code
<b>Strategy and architecture,</b> Governance, Risk, and Compliance	<b>Risk Management</b> Plans and implements complex and substantial risk management activities within a specific function, technical area, project, or programme.  Implements consistent and reliable risk management processes and reporting to key stakeholders.  Engages specialists and domain experts, as necessary.  Advises on the organisation's approach to risk management.	<b>Level 5 - BURM</b>
<b>Delivery and Operation,</b> Security Services	<b>Vulnerability Assessment</b> Plans and manages vulnerability assessment activities within the organisation.  Evaluates and selects, reviews vulnerability assessment tools and techniques.  Provides expert advice and guidance to support the adoption of agreed approaches.  Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.	<b>Level 5 - VUAS</b>
<b>Strategy and Architecture,</b> Security and Privacy	<b>Threat Intelligence</b> Sets direction, plans and leads the organisation's approach to threat intelligence, including the use of suppliers.  Identifies requirements for threat intelligence based on the assets to be protected and the types of intelligence that can help protect those assets.  Engages with, and influences, relevant stakeholders to communicate results of research and the required response.  Ensures quality and accuracy of threat intelligence information.  Reviews threat intelligence capabilities.	<b>Level 6 - THIN</b>



NSW Government employees can access the ICT set through the [Skills Framework for the Information Age](#) Foundation website by registering as a corporate user via their NSW Government email address.

Version Control

Version	Summary of Changes	Date
V1.0	New Role Description created for new role	02.04.2024

Roles attached

Position Number	Region	Position Number	Region	Position Number	Region	Position Number	Region
	TC						