Role Description
Cyber Security Analyst

Role Description Fields	Details
Department/Agency	Department of Customer Service
Division/Branch/Unit	Digital NSW/ Cyber Security NSW.
Classification/Grade/Band	Clerk Grade 7/8
ANZSCO Code	262116
OSCA Code	271133
PCAT Code	2336392
Role Family/Function/Type	Digital, ICT & Technology / Cyber Security / Security Analyst
Date of Approval	August 2025 (updated June 2026)
Agency Website	www.customerservice.nsw.gov.au

Primary purpose of the role

Responsible for the provision of expertise and analysis to deliver intelligence and reporting on cyber security and threats in NSW. The role supports all-of-government (AoG) responses to cyber security issues, and the management of risks to the NSW Government, and contributes to strengthening the NSW Governments cyber security posture through the provision of advice on IT security, information security threats, and drives practices for risk management across the sector.

Key accountabilities

- Monitor, identify assess and alert agencies to cyber security issues and threats including breaches and potential intrusion incidents
- Deliver initiatives, develop reports, perform analysis and provide advice and recommendations to uplift cyber security resilience across the sector, through strengthening cyber security risk management, investment prioritisation, and governance
- Produce timely and actionable intelligence and reporting on emerging cyber trends, threats and issues affecting NSW assets
- Work collaboratively with internal and external stakeholders and vendors to monitor, detect, report and share cyber vulnerabilities, incidents, threats and trends
- Provide advice to maintain the compliance with AoG cyber security policies and standards
- Contribute technical expertise and knowledge to reporting on current and emerging cyber security risks and trends
- Provide recommendations to improve cyber security across NSW government
- Identify stakeholder requirements, prioritise workload and manage team portfolios to meet agreed outcomes and timeframes

Key challenges

- Maintaining up-to-date knowledge and understanding of current and the future NSW cyber security environment, threats and vulnerabilities to information, assets and services
- Developing and maintaining positive stakeholder relationships to ensure oversight and value to leading departments and agencies from a AoG cyber security perspective
- Ensuring work is completed to agreed timeframes while managing competing priorities and outputs

Key relationships

Internal

Who	Why
Manager	• Participate in discussions, meetings and decisions regarding policy • Escalate issues, keep informed, advise and receive guidance and instructions • Report on projects, issues, products and systems
Work team	• Work collaboratively to contribute to achieving organisation's business goals • Participate in meetings and discussions to obtain the work group perspective and share information. • Review work and proposals of team members
Clients/Customers	• Manage the flow of information, seek clarification and provide advice and responses to ensure prompt resolution of issues • Guide and inform NSW Government and local government users regarding relevant security practices and processes • Address/respond to queries and provide solutions where possible, or redirect query to relevant area • Develop and maintain effective working relationships and open channels of communication

External

Who	Why
Stakeholders/Industry Professionals	• Develop and maintain effective working relationships and open channels of communication • Consult, provide and obtain information • Address/respond to queries and provide solutions where possible, or redirect query to relevant party for review and resolution • Participate in discussions regarding innovation and best practice
Vendors/Service Providers	• Assist in the management of contracts and monitor provision of service to ensure compliance with contracts and service arrangements • Contact to provide and gather information and resolve routine issues.

Role dimensions

Decision making

This role has autonomy and makes decisions that are under their direct control as directed by their manager. It refers to a manager's decisions that require significant change to program outcomes or timeframes or are likely to escalate or require submission to a higher level of management. This role is accountable for the delivery of work assignments on time and to expectations in terms of quality, deliverables and outcomes.

Reporting line

Manager, Cyber Technical Centre

Direct reports

The role may have direct reports

Budget/Expenditure

As per the Customer Service Delegations

Key knowledge and experience

Nil

Essential requirements

- The successful applicant must have, or be able to attain and maintain, baseline security clearance and willingness to undergo a police check as a condition of employment

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
 Personal attributes	**Display Resilience and Courage** Be open and honest, prepared to express your views, and willing to accept and commit to change	• Be flexible and adaptable and respond quickly when situations change • Offer your opinion and raise challenging issues • Acknowledge when someone challenges your ideas and respond respectfully • Work through challenges • Remain calm and focused in challenging situations	Intermediate

Capability group/sets	Capability name	Behavioural indicators	Level
	**Commit to Customer Service** Provide customer-focused services in line with public sector and organisational objectives	• Focus on providing a positive customer experience • Support a customer-focused culture in your organisation • Demonstrate a thorough knowledge of the available services and share relevant information with customers • Identify and respond quickly to customer needs • Consider different customer needs and experiences when developing solutions to meet needs • Resolve complex customer issues • Cooperate across work areas to improve outcomes for customers	Intermediate
	**Think and Solve Problems** Think, analyse and consider the broader context to develop practical solutions	• Make recommendations based on evidence by researching and critically analysing information and identifying interrelationships • Anticipate, identify and deal with issues and potential problems that may impact organisational goals and the customer experience • Think creatively to come up with new ideas to resolve issues and improve customer experience • Seek input and ideas from people with different backgrounds and experiences • Participate in and contribute to team or business unit initiatives to resolve common issues or barriers to effectiveness • Identify and share business process improvements to enhance effectiveness • Analyse data and information to identify insights and communicate findings in a clear and meaningful way	Adept
	**Technology** Understand and use available technologies to maximise efficiencies and effectiveness	• Identify opportunities to collaborate using a range of technologies • Monitor compliance with policies for cyber security and acceptable technology use • Identify and evaluate how technology supports business strategies and objectives, raising concerns where outputs may be inappropriate • Monitor compliance with your organisation's records, information and knowledge management requirements • Check that outputs from systems and digital tools support objectives and meet expected standards	Adept

Capability group/sets	Capability name	Behavioural indicators	Level
	**Project Management** Understand and use effective ways to plan, coordinate and control projects	• Research and analyse data at a basic level to inform and support the achievement of project deliverables • Contribute to developing project documents and resource estimates • Contribute to reviews of progress, outcomes and future improvements • Identify when projects differ from their plans and tell your supervisor	Intermediate

Occupation specific capability set

Capability group/sets	Capability name	Behavioural indicators	Level
SFIA	**Incident Management** Coordinating responses to a diverse range of incidents to minimise negative impacts and quickly restore services	• Monitors and manages incident queues to ensure incidents are handled according to procedures and service levels • Contributes to developing, testing and improving incident management procedures. Uses analytics tools to track trends • Ensures resolved incidents are properly documented and closed. • Supports team members in the correct use of the incident process	Level 4 - USUP

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.

Capability group/sets	Capability name	Description	Level
	Act with Integrity	Be ethical and professional, and uphold and promote the public sector values	Intermediate
	Manage Self	Be persistent, self-reflect and commit to learning	Intermediate
	Value Diversity and Inclusion	Be inclusive and respect diverse backgrounds, experiences and perspectives	Foundational
	Communicate Effectively	Communicate clearly, pay attention to others and respond with understanding and respect	Intermediate

Capability group/sets	Capability name	Description	Level
	Work Collaboratively	Collaborate with others and value their contribution	Intermediate
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Intermediate
	Deliver Results	Achieve results by using resources efficiently and committing to quality outcomes	Intermediate
	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Intermediate
	Demonstrate Accountability	Be proactive and responsible for your actions, and follow legislation, policy and guidelines	Intermediate
	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Foundational
	Procurement and Contract Management	Understand and use procurement processes to ensure effective purchasing and contract performance	Foundational

Occupation specific capability set

Capability group/sets	Capability name	Description	Level
SFIA	Application Support	Delivering management, technical and administrative services to support and maintain live applications	Level 4 - ASUP
SFIA	Infrastructure Operations	Provisioning, deploying, configuring, operating and optimising technology infrastructure across physical, virtual and cloud-based environments	Level 4 - ITOP
SFIA	Systems Installation and Removal	Installing and testing, or decommissioning and removing, systems or system components	Level 4 - HSIN