Role Description

Associate Director, Digital Forensics and Incident Management

Role Description Fields	Details
Department/Agency	Department of Customer Service
Division/Branch/Unit	Service NSW – Cyber Security
Classification/Grade/Band	SNSW 11/12
ANZSCO Code	262118
OSCA Code	271136
PCAT Code	1326167
Role Family/Function/Type	Digital, ICT & Technology / Cyber Security / Incident Management
Date of Approval	August 2024
Agency website	www.service.nsw.gov.au

Agency Overview

Service NSW is making it easier for people and businesses across NSW to access government services. Since launching in July 2013, we have successfully transformed and streamlined NSW government service delivery with cutting edge digital solutions and an award-winning culture of passion and teamwork.
Our customer-centric solution offers simpler and faster access to government transactions through our digital channels, a 7-day-a-week phone service and an expanding network of service centres. We currently partner with over 70 agencies to offer over 1,300 NSW government transactions.

Primary purpose of the role

Providing complex cyber security, advice, awareness, resilience and/or training initiatives for Cyber Security to improve organisational or whole-of-government cyber security capability.

Key accountabilities

- Lead the identification, containment and eradication and recovery from cyber security incidents and implement incident response capabilities that include leveraging tools and third parties to contain and eradicate cyber threats.
- Reduce costs, strategically, and increasing efficacy of identification and containment activities through collaborating with Channel Enablement teams to provide SEIM/SOAR functionality.
- Provide visibility of cyber-attacks occurring against Service NSW targets and communicating to stakeholders within cyber leadership to continuously improve security.
- Prepare for potential cyber security events through preparation of cyber tabletop exercises, creation and maintenance of playbooks, collaboration with other teams to assess the efficacy of detective and preventative controls which can be used to continuously improve the service offering.
- Lead and manage a team of specialised forensics and incident responders and improve their performance by tracking relevant KPIs and metrics to uplift maturity of forensics and incident management.
- Provide access to cyber security tooling, monitoring, remediating and reviewing potential access control violations across the organisation to ensure security of information.

- Provide expert advice into defining, developing and communicating the practices and processes necessary for effective problem and demand management to enable ICT and the business to make evidence-based decisions to minimise the impact of service outages

Key challenges

- Establishing a systematic and proactive approach to managing cyber security incidents in a complex technical environment involving external agencies and stakeholders, and multiple internal stakeholders.
- Delivering outcomes in an environment of heavy reliance on input and approval from multiple stakeholders with varying timelines and needs
- Establishing and maintaining, proactively, an awareness of geopolitical trends and threats, emerging business priorities and gaps in controls that potentially impact service reliability given the pace of technological change

Key relationships

Internal

Who	Why
Manager	• Escalate issues, advise and receive instructions • Report on compliance metrics, security breaches and remedial actions • Make recommendations for changes and improvements to the management system, policy and practice
Direct reports	• Inspire, guide, support, motivate, coach, mentor and manage performance • Review work and proposals to ensure integrity and accountability of decision making • Provide own perspective and share information • Work collaboratively with, inspire and motivate
Work Team	• Guide, support, coach and mentor relevant staff to influence and motivate others, provide direction and track performance • Review the work and proposals of others in the role's areas of specialisation and accountability • Guide others in the development of service level agreements • Collaborate with others to appropriately communicate security related information to relevant stakeholders, customers and partners
Stakeholders/Customers	• Provide expert focused advice, assistance, support and solutions to issues • Develop and maintain effective working relationships and open channels of communication • Agree future requirements for new or modified services and products • Provide complex focused advice to ensure consistent approaches and appropriate standards are met

External

Who	Why
Stakeholders/Customers	• Develop and maintain effective working relationships to support management, staff, customers and stakeholders • Manage expectations, resolve issues and provide solutions to problems • Understand and accommodate a wide range of requirements in relation to incident management across the customer / stakeholder base and resolve issues or problems • Represent the organisation in key stakeholder interactions in the role's areas of specialisation and accountability
Suppliers/ Vendors	• Liaise regarding known errors and the promotion of problem management within outsourced service providers.
Customers/Stakeholders (Other Government Agencies)	• Ensure effective two-way communication on all matters relating to effective service delivery from an operational perspective • Develop and maintain effective working relationships and open channels of communication • Consult, provide and obtain information • Resolve and provide solutions to issues

Role dimensions

Decision making

This role has autonomy and makes decisions that are under their direct control as directed by their Executive. It refers to the Executive decisions that require significant change to program outcomes or timeframes or are likely to escalate. This role is fully accountable for the delivery of work assignments on time and to expectations in terms of quality, deliverables and outcomes. This role submits reports, business cases and other forms of written advice with minimal input from the Director.

Reporting line

Director

Direct reports

This role may have direct reports

Budget/Expenditure

As per the Customer Service Delegations

Key knowledge and experience

- 8+years of cyber security/ICT Security experience
- Bachelor degree in Computer Science or equivalent certification: CISSP, GIAC, CEH, CISA
- Experience in analysing cyber events and resolving cyber incidents
- Experience in cyber tools including vulnerability management, advanced anti-malware and cloud tools e.g.; WAF and API Gateways.
- Excellent listening skills and communication skills include oral, written, and formal presentations
- The monitoring of endpoints, vulnerability information revealed by scanners, security intelligence feeds, intrusion prevention (IPS), and detection (IDS) systems
- Operating systems
- Cloud services e.g.: AWS
- Experience in working with external vendors who provide security services
- Must have or be able to obtain a baseline security clearance

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, show initiative and respond quickly when situations change • Give frank and honest feedback and advice • Acknowledge when someone challenges your ideas, seek to understand why and respond appropriately • Raise and work through challenging issues and seek alternatives • Respond professionally when under pressure and in challenging situations	Adept
 Relationships	**Communicate Effectively** Communicate clearly, pay attention to others and respond with understanding and respect	• Present with credibility, engage diverse audiences and test whether they understand you • Translate technical and complex information clearly and concisely for different audiences • Create opportunities for others to contribute to discussion and debate • Set an example by promoting information sharing across your organisation • Manage complex communications that involve understanding and responding to multiple and divergent viewpoints • Explore creative ways to share information and communicate with diverse audiences • Leverage insights from people with lived experience to shape communication and engagement strategies • Write clearly, concisely and persuasively in a range of styles and formats	Advanced

Capability group/sets	Capability name	Behavioural indicators	Level
	**Commit to Customer Service** Provide customer-focused services in line with public sector and organisational objectives	• Promote an inclusive, customer-focused culture in your organisation and consider new ways of working to improve customer experience • Ensure that your organisation's systems, processes, policies and programs collect customer feedback and insights, and use these to inform your response to customer needs • Initiate and develop partnerships with customers to define and evaluate service performance outcomes • Promote and manage partnerships within your organisation and across the public, private and community sectors • Communicate with senior stakeholders about key issues and provide expert and influential advice • Consider customers' experience when designing business processes and improving services • Encourage new ideas and creative ways to involve customers in designing business processes and improving services	Advanced
	**Think and Solve Problems** Think, analyse and consider the broader context to develop practical solutions	• Undertake objective, critical analysis to reach accurate conclusions that recognise and manage contextual issues • Work through issues, weigh up alternatives and identify the most effective solutions in collaboration with others • Consider the wider business context when thinking about options to resolve issues • Explore a range of possibilities and creative alternatives to improve systems, processes and business practices • Put systems and processes in place that are supported by high-quality research and analysis • Look for opportunities to design innovative solutions to meet customers' needs and service demands • Evaluate the performance and effectiveness of services, policies and programs against clear criteria	Advanced

Capability group/sets	Capability name	Behavioural indicators	Level
	**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
	**Manage and Develop People** Engage with and motivate staff, and develop their capability and potential	• Define and clearly communicate roles, responsibilities and performance standards to achieve team outcomes • Adjust performance development processes to meet the diverse abilities and needs of individuals and teams • Develop work plans that consider capability, strengths and opportunities for development • Be aware of the effects of bias when managing team members • Seek feedback about your management capabilities and develop strategies to improve on them • Address and resolve team and individual performance issues, including unsatisfactory performance, promptly and effectively • Monitor and report on team performance in line with established performance development frameworks • Develop positive relationships to ensure cultural safety and trust between team members	Adept

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.	• Responsible for the operation of the incident management process. • Manages incident communications, ensuring al parties are aware of incidents and their role in the process. • Leads the review of major incidents and informs service owners of outcomes. Ensures incident resolution within service targets. Analyses metrics and reports on the performance of the incident management process. • Develops, maintains and tests incident management policy and procedures. Ensures compliance with regulatory requirements.	USUP - Level 5
SFIA	**Problem management** Managing the lifecycle of all problems that have occurred or could occur in delivering a service.	• Ensures appropriate action is taken to anticipate, investigate and resolve problems in systems and services. • Ensures problems are fully documented within the relevant reporting systems. • Enables development of problem solutions. Coordinates the implementation of agreed remedies and preventative measures. • Analyses patterns and trends and improves problem management processes.	PBMG - Level 5
SFIA	**Digital forensics** Recovering and investigating material found in digital devices.	• Plans and leads the organisation's approach to digital forensics. • Sets policies, standards and guidelines for how the organisation conducts digital forensic investigations. • Leads and manages high risk, large or wide-ranging digital forensics investigations engaging additional specialists if required. • Authorises the release of formal forensic reports. Engages with external stakeholders on forensic matters.	DGFS - Level 6

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	Adept
	Manage Self	Be persistent, self-reflect and commit to learning	Adept
	Value Diversity and Inclusion	Be inclusive and respect diverse backgrounds, experiences and perspectives	Intermediate
	Work Collaboratively	Collaborate with others and value their contribution	Adept
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Adept
	Deliver Results	Achieve results by using resources efficiently and committing to quality outcomes	Adept
	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Adept
	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	Intermediate
	Procurement and Contract Management	Understand and use procurement processes to ensure effective purchasing and contract performance	Intermediate
	Project Management	Understand and use effective ways to plan, coordinate and control projects	Adept
	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

Capability group/sets	Capability name	Description	Level
People management	Manage Reform and Change	Support and champion change, and help others to engage with change	Adept