

# ROLE DESCRIPTION

## Manager, Cyber Security Operations and Incident Response

Portfolio	Communities and Justice	
Department	Department of Communities and Justice	
Division/Branch/Unit	Corporate Services / Information and Digital Services / Cyber Risk Audit and Compliance	
Location	TBA	
Classification/Grade/Band	Clerk Grade 11/12	
Role Number	TBA	
ANZSCO Code	135199	
PCAT Code	3226392	
Date of Approval	7 July 2025	Ref: IDS172
Agency Website	www.dcj.nsw.gov.au	

### Agency overview

The Department of Communities and Justice (DCJ) is the lead agency in the Communities and Justice Portfolio. Communities and Justice aims to achieve a safe, just, and inclusive New South Wales (NSW) by operating an effective legal system; increasing access to social and affordable housing; protecting children and families; addressing domestic and family violence; promoting public safety; reducing reoffending; and supporting community harmony and social cohesion.

DCJ works to enable everyone's right to access justice and help for families through early intervention and inclusion, with benefits for the whole community by providing services that are effective and responsive to community needs.

### Primary purpose of the role

The Manager, Cyber Security Operations and Incident Response leads the internal monitoring, detection and incident response functions in DCJ and is responsible for safeguarding DCJ digital assets through collaboration with third party Managed Security Services Providers, as applicable, in regard to detection, response and mitigation of cyber threats. This role involves overseeing the monitoring of networks and systems for suspicious activities, coordinating incident response, and implementing robust security measures. The Manager, Cyber Security Operations and Incident Response also collaborates with other teams, including the Red Team and Cyber Threat Intelligence, to enhance the overall security posture through continuous improvement and strategic defence initiatives.

### Key accountabilities

- Implement systems that enable detection and responses to cyber security events and incidents within DCJ.
- Work with colleagues and, as applicable, managed services provider(s), to ensure security tools are configured and tuned to optimise security event detection and response (including analysis of security logs).
- Provide expert advice and leadership of technical analysis on cyber incidents and coordinate efforts to swiftly respond to cyberattacks and security breaches.

- Leverage partnerships with third party Managed Security Services Providers (as appropriate) to ensure that DCJ is well placed to identify, review and monitor cyber events and take appropriate action in accordance with the DCJ Cyber Incident Response Plan
- Prepare reports regarding security incidents, vulnerabilities, and other cyber security metrics to illustrate the overall security posture.
- Collaborate with other teams to ensure cohesive and collective understanding of cyber exposure points, cyber incidents and threat intelligence to inform cyber threat defence strategies and implementation of effective security controls and processes.
- Review, enhance and inform Cyber Security Awareness across DCJ and contribute to delivery of initiatives to uplift cyber security behaviour and culture.

## Key challenges

- Maintaining currency and applicability of subject matter knowledge and the links to legislative, legal and statutory changes relating to information security and management.
- Managing resource capacity to meet fluctuating demand in an ever-changing cyber threat environment.

## Key relationships

Who	Why
<b>Internal</b>	
Manager	<ul style="list-style-type: none"> <li>• Escalate issues, advise and receive instructions</li> <li>• Report on compliance metrics</li> </ul>
Work team	<ul style="list-style-type: none"> <li>• Inspire and motivate team, provide direction and manage performance</li> <li>• Guide, support, coach and mentor team members</li> <li>• Review the work and proposals of team members in the role's areas of specialisation and accountability</li> <li>• Encourage team to work collaboratively to contribute to achieving the team's business outcomes</li> <li>• Project Management Office – to assist in management of project related risk. Partner with assigned Project Managers for the delivery of cyber security projects.</li> <li>• Enterprise and Security Architects - ensure enterprise architecture and solution designs align with security policies and reflected in configuration of cyber security tools</li> </ul>
Clients/customers	<ul style="list-style-type: none"> <li>• Resolve and provide solutions to issues</li> <li>• Create awareness of policies and standards associated with security and how they are applied in the organisation</li> </ul>

Who	Why
Internal partners	<ul style="list-style-type: none"> <li>Undertake assessments of compliance with risk and ICT governance practices</li> <li>Corporate Risk Management – to identify and integrate the ICT risk framework with the corporate risk framework</li> <li>Collaborate with Business Divisions (including Open Government and Information Privacy) regarding cyber security incidents and data breaches</li> </ul>
<b>External</b>	
Third Party Providers	<ul style="list-style-type: none"> <li>Engage and collaborate with third party cyber security providers in the joint delivery of Security Operations Centre (SOC) activities</li> </ul>
Auditors / Suppliers	<ul style="list-style-type: none"> <li>Undertake security reviews</li> <li>External security threat assessments</li> </ul>
Government Agencies	<ul style="list-style-type: none"> <li>Work with other agencies to share information and guidance</li> </ul>

## Role dimensions

### Decision making

The role has a high level of independence and is expected to make day-to-day decisions relating to work priorities and workload management.

### Reporting line

See divisional structure and supplementary material.

### Direct reports

Up to 7 direct reports.

### Budget/Expenditure

Nil

## Key knowledge and experience

- Extensive experience in the cyber security field with experience in Incident Response, Detection and Prevention cyber security systems/tools, and analysing cyber security incident artifacts.
- Demonstrated expert knowledge with cyber security, detection and prevention systems/tools, forensic analysis of cyber incidents.

## Essential requirements

Tertiary qualifications in a related discipline and/or equivalent knowledge, skills and experience with demonstrated commitment to ongoing professional development.

Appointments are subject to reference checks. Some roles may also require the following checks/clearances:

- National Criminal History Record Check in accordance with the Disability Inclusion Act 2014
- Working with Children Check clearance in accordance with the Child Protection (Working with Children) Act 2012

## 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	<b>Act with Integrity</b> Be ethical and professional, and uphold and promote the public sector values	<ul style="list-style-type: none"><li>• Model the highest standards of ethical and professional behaviour and reinforce their use</li><li>• Represent the organisation in an honest, ethical and professional way and set an example for others to follow</li><li>• Promote a culture of integrity and professionalism within the organisation and in dealings external to government</li><li>• Monitor ethical practices, standards and systems and reinforce their use</li><li>• Act promptly on reported breaches of legislation, policies and guidelines</li></ul>	Advanced

## FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
	<b>Communicate Effectively</b> Communicate clearly, actively listen to others, and respond with understanding and respect	<ul style="list-style-type: none"> <li>• Present with credibility, engage diverse audiences and test levels of understanding</li> <li>• Translate technical and complex information clearly and concisely for diverse audiences</li> <li>• Create opportunities for others to contribute to discussion and debate</li> <li>• Contribute to and promote information sharing across the organisation</li> <li>• Manage complex communications that involve understanding and responding to multiple and divergent viewpoints</li> <li>• Explore creative ways to engage diverse audiences and communicate information</li> <li>• Adjust style and approach to optimise outcomes</li> <li>• Write fluently and persuasively in plain English and in a range of styles and formats</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

## FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
 Business Enablers	<b>Technology</b> Understand and use available technologies to maximise efficiencies and effectiveness	<ul style="list-style-type: none"> <li>• Champion the use of innovative technologies in the workplace</li> <li>• Actively manage risk to ensure compliance with cyber security and acceptable use of technology policies</li> <li>• Keep up to date with emerging technologies and technology trends to understand how their application can support business outcomes</li> <li>• Seek advice from appropriate subject-matter experts on using technologies to achieve business strategies and outcomes</li> <li>• Actively manage risk of breaches to appropriate records, information and knowledge management systems, protocols and policies</li> </ul>	Advanced
	<b>Manage and Develop People</b> Engage and motivate staff, and develop capability and potential in others	<ul style="list-style-type: none"> <li>• Collaborate to set clear performance standards and deadlines in line with established performance development frameworks</li> <li>• Look for ways to develop team capability and recognise and develop individual potential</li> <li>• Be constructive and build on strengths by giving timely and actionable feedback</li> <li>• Identify and act on opportunities to provide coaching and mentoring</li> <li>• Recognise performance issues that need to be addressed and work towards resolving issues</li> <li>• Effectively support and manage team members who are working flexibly and in various locations</li> <li>• Create a safe environment where team members' diverse backgrounds and cultures are considered and respected</li> <li>• Consider feedback on own management style and reflect on potential areas to improve</li> </ul>	Intermediate

This role also utilises an occupation specific capability set which contains information from the Skills Framework for the Information Age (SFIA). The capability set is available at <http://www.psc.nsw.gov.au/workforce-management/capability-framework/access-the-capability-framework/occupation-specific/occupation-specific>

#### Focus Occupation Specific Capabilities

	Capability name	Capability Set	Level
	Capability description		
	<b>Cybersecurity Operations and Resilience, Cybersecurity Resilience, Digital Forensics</b> Recovering and investigating material found in digital devices	<ul style="list-style-type: none"> <li>Leads investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences.</li> <li>Collates conclusions and recommendations and presents forensic findings to stakeholders.</li> <li>Plans and manages digital forensics activities within the organisation. Provides expert advice on digital forensics.</li> <li>Contributes to the development of digital forensics policies, standards and guidelines. Evaluates and selects digital forensics tools and techniques.</li> </ul>	<b>Level 5 - DGFS</b>
	<b>Cybersecurity Operations and Resilience, Cybersecurity Resilience, Security Operations</b> Manages and administers security measures, using tools and intelligence to protect assets, ensuring compliance and operational integrity	<ul style="list-style-type: none"> <li>Oversees security operations procedures, ensuring adherence and effectiveness, including cloud security practices and automated threat responses.</li> <li>Reviews actual or potential security breaches and vulnerabilities and ensures they are promptly and thoroughly investigated. Recommends actions and appropriate control improvements.</li> <li>Ensures the integrity and completeness of security records, ensuring timely support and adherence to established procedures.</li> <li>Contributes to the creation and maintenance of security policies, standards and procedures integrating new compliance requirements and technology advances.</li> </ul>	<b>Level 5- SCAD</b>
	<b>Strategy &amp; Architecture, Business Strategy &amp; Planning, Business Risk Management</b>	<ul style="list-style-type: none"> <li>Plans and implements complex and substantial risk management activities</li> </ul>	<b>Level 5-BURM</b>

## Focus Occupation Specific Capabilities

Planning and implementing processes for managing risk across the enterprise, aligned with organisational strategy and governance frameworks.

- within a specific function, technical area, project or programme.
- Establishes consistent risk management processes and reporting mechanisms aligned with governance frameworks.
- Engages specialists and domain experts as necessary.
- Advises on the organisation's approach to risk management.





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 is 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	Intermediate
 Relationships	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
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Adept



## COMPLEMENTARY CAPABILITIES

Capability Group/Sets	Capability Name	Description	Level
 Results	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	Adept
	Think and Solve Problems	Think, analyse and consider the broader context to develop practical solutions	Adept
	Demonstrate Accountability	Be proactive and responsible for own actions, and adhere to legislation, policy and guidelines	Adept
 Business Enablers	Finance	Understand and apply financial processes to achieve value for money and minimise financial risk	Intermediate
	Procurement and Contract Management	Understand and apply procurement processes to ensure effective purchasing and contract performance	Intermediate
	Project Management	Understand and apply effective project planning, coordination and control methods	Intermediate
 People Management	Inspire Direction and Purpose	Communicate goals, priorities and vision, and recognise achievements	Intermediate
	Optimise Business Outcomes	Manage people and resources effectively to achieve public value	Intermediate
	Manage Reform and Change	Support, promote and champion change, and assist others to engage with change	Adept