

Role Description

Senior Security Assurance Analyst



Role Description Fields	Details
Cluster	Planning and Environment
Department/Agency	Department of Planning and Environment
Division/Branch/Unit	Corporate Services / Digital Information Office
Role number	
Classification/Grade/Band	Clerk Grade 9/10
Senior executive work level standards	Not Applicable
ANZSCO Code	262116
PCAT Code	1226292
Date of Approval	March 2023
Agency Website	www.dpie.nsw.gov.au

Agency overview

Our vision is to create thriving environments, communities and economies for the people of New South Wales. We focus on some of the biggest issues facing our state. We deliver sustainable water resource and environment management, secure our energy supply, oversee our planning system, maximise community benefit from government land and property, and create the conditions for a prosperous state. We strive to be a high-performing, world-class public service organisation that celebrates and reflects the full diversity of the community we serve and seeks to embed Aboriginal cultural awareness and knowledge throughout the department.

Primary purpose of the role

The Senior Security Assurance Analyst is responsible for leading information security assurance activities across the DPE by providing technical security expertise to ensure that existing and new ICT systems, services and products meet the security compliance requirements. The role is responsible for monitoring the effectiveness of implemented security controls and determining deviations from acceptable configurations, policy, or standards, and providing expertise in risk treatment management and compliance requirements for internal and external reviews of requirements.

Key accountabilities

- Lead the vulnerability management remediation project as an SME.
- Lead the monitoring of the effectiveness of implemented security controls to maintain compliance with internal and external security policies and standards.
- Lead the coordination, monitoring and evaluation including tracking, collating, and analysing data on security assurance activities (e.g. vulnerability management, penetration testing, third party assessments, audits and red teaming).
- Work closely with Digital Information Office teams to ensure that systems are properly protected, and security baselines are applied correctly.
- Gather cyber security metrics and provide regular reporting while improving the internal processes to promote consistent evaluations, automation, and reporting of metrics.

- Maintain various registers that support cyber security assurance and security reporting including security exception management.
- Coordinate and participate in information security audits, and conduct threat modelling and security reviews of applications, to minimise risk exposure and ensure DPE is in continuous compliance.
- Manage the penetration testing program, and report to management and track test findings and remediation.

Key challenges

- Providing technical expertise on the development and support of all assurance activities, processes, and tools used for validating and ensuring the protection of ICT systems.
- Building and promoting an active culture and high level of ICT security awareness within the organisation.
- Maintaining current knowledge of Information Security frameworks, standards and best practices, and audit, risk and compliance requirements, and maintaining links to legislative and statutory changes relating to ICT security.

Key relationships

Internal

Who	Why
Manager	<ul style="list-style-type: none"> • Escalate issues, keep informed, advise, receive guidance and instructions • Participate in meetings and discussions to share information and provide input and feedback • Identify sensitive issues, risk & opportunities and recommend potential solutions • Provide regular updates on key projects and priorities
Work team	<ul style="list-style-type: none"> • Support team members and work collaboratively to contribute to achieving business outcomes • Participate in discussions and decisions regarding resolution of issues and implementation of innovation and best practice • Represent work group perspective and share information • Review work and proposals of team members
Customers / Stakeholders	<ul style="list-style-type: none"> • Manage the flow of information, seek clarification and provide customer focused advice and responses to ensure prompt resolution of issues • Articulate the needs and requirements of the service and collaborate with to negotiate solutions, provide expert customer focused advice and regular updates • Address/respond to queries to provide advice where possible, or redirect to relevant party for review and resolution

External

Who	Why
Customers / stakeholders	<ul style="list-style-type: none">• Respond and resolve queries, providing information and/or resources or redirect to the appropriate person or business unit if required• Develop and maintain effective working relationships and open channels of communication to provide and obtain information, and ensure effective management and implementation of expectations and standards• Engage with, consult, seek clarification and provide customer focused advice and responses to ensure the prompt resolution of issues
Industry professionals / consultants	<ul style="list-style-type: none">• Seek/maintain specialist knowledge/advice and collaborate on the implementation of organisation strategies, to keep abreast of best practice• Collaborate with and seek/maintain specialist knowledge/advice• Participate in forums, groups to represent the agency and share information• Participate in discussions regarding innovation and best practice
Vendors / Service Providers	<ul style="list-style-type: none">• Develop and maintain effective working relationships• Monitor provision of service to ensure compliance with contracts and service arrangements

Role dimensions

Decision making

- This role has autonomy and makes decisions that are under their direct control as directed by their Manager. It refers decisions that require significant change to program outcomes or timeframes or are likely to escalate or require submission to a higher level of management to their manager.
- 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 manager.

Reporting line

Manager, Security Assurance

Direct reports

Nil

Budget/Expenditure

TBA

Key knowledge and experience

- Detailed understanding of vulnerability management prioritisation frameworks.
- Understanding of and exposure to typical assurance activities e.g. penetration testing, red teaming, audits, third party assessments.
- Knowledge of the NSW Government compliance requirements and other security frameworks and standards such as Australian Signal Directorate (ASD), the Australian Government Protective Security Policy Framework, and ISO/IEC 27001.

Essential requirements

- Tertiary qualifications in computer science, information and technology or related technical field and/or relevant experience.

Cyber Security

Cyber security forms an integral part of every employee's role description and responsibilities. Individuals such as those with privileged access, application developers, risk owners, and system and application owners have additional responsibilities in securing the Department's digital resources. As part of your role, you will be expected to undertake cyber security related activities to help contribute to the Department's overall security posture.

Capabilities for the role

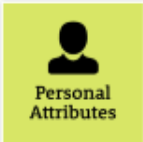
The [NSW public sector capability framework](#) describes the capabilities (knowledge, skills and abilities) needed to perform a role. There are four main groups of capabilities: personal attributes, relationships, results and business enablers, with a fifth people management group of capabilities for 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.



Capability group/sets	Capability name	Behavioural indicators	Level
	Manage Self Show drive and motivation, an ability to self-reflect and a commitment to learning	<ul style="list-style-type: none">• Keep up to date with relevant contemporary knowledge and practices• Look for and take advantage of opportunities to learn new skills and develop strengths• Show commitment to achieving challenging goals• Examine and reflect on own performance• Seek and respond positively to constructive feedback and guidance• Demonstrate and maintain a high level of personal motivation	Adept

Capability group/sets	Capability name	Behavioural indicators	Level
 <p>Relationships</p>	<p>Communicate Effectively</p> <p>Communicate clearly, actively listen to others, and respond with understanding and respect</p>	<ul style="list-style-type: none"> • Present with credibility, engage diverse audiences and test levels of understanding • Translate technical and complex information clearly and concisely for diverse audiences • Create opportunities for others to contribute to discussion and debate • Contribute to and promote information sharing across the organisation • Manage complex communications that involve understanding and responding to multiple and divergent viewpoints • Explore creative ways to engage diverse audiences and communicate information • Adjust style and approach to optimise outcomes • Write fluently and persuasively in plain English and in a range of styles and formats 	Advanced
 <p>Relationships</p>	<p>Work Collaboratively</p> <p>Collaborate with others and value their contribution</p>	<ul style="list-style-type: none"> • Encourage a culture that recognises the value of collaboration • Build cooperation and overcome barriers to information sharing and communication across teams and units • Share lessons learned across teams and units • Identify opportunities to leverage the strengths of others to solve issues and develop better processes and approaches to work • Actively use collaboration tools, including digital technologies, to engage diverse audiences in solving problems and improving services 	Adept
 <p>Results</p>	<p>Plan and Prioritise</p> <p>Plan to achieve priority outcomes and respond flexibly to changing circumstances</p>	<ul style="list-style-type: none"> • Understand the links between the business unit, organisation and the whole-of-government agenda • Ensure business plan goals are clear and appropriate and include contingency provisions • Monitor the progress of initiatives and make necessary adjustments • Anticipate and assess the impact of changes, including government policy and economic conditions, on business plans and initiatives and respond appropriately • Consider the implications of a wide range of complex issues and shift business priorities when necessary • Undertake planning to help the organisation transition through change initiatives, and evaluate progress and outcomes to inform future planning 	Advanced

Capability group/sets	Capability name	Behavioural indicators	Level
	Technology Understand and use available technologies to maximise efficiencies and effectiveness	<ul style="list-style-type: none"> Identify opportunities to use a broad range of technologies to collaborate Monitor compliance with cyber security and the use of technology policies Identify ways to maximise the value of available technology to achieve business strategies and outcomes Monitor compliance with the organisation's records, information and knowledge management requirements 	Adept

Occupational Specific Focus Capabilities



Capability group/sets	Capability name	Description	Level
	Strategy and architecture / Security and privacy / Information assurance (INAS)	<ul style="list-style-type: none"> Interprets information assurance and security policies and applies these to manage risks. Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines. Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain. Contributes to the development of policies, standards and guidelines. 	Level 5
	Vulnerability assessment (VUAS)	<ul style="list-style-type: none"> 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. 	Level 5









Capability group/sets	Capability name	Description	Level
	Strategy and architecture / Security and privacy / Information security (SCTY)	<ul style="list-style-type: none"> Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Contributes to development of information security policy, standards and guidelines. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems. Investigates major breaches of security and recommends appropriate control improvements. Develops new architectures that mitigate the risks posed by new technologies and business practices 	Level 5
	Strategy and architecture / Governance, risk and compliance / Audit (AUDT)	<ul style="list-style-type: none"> Plans, organises and conducts audits of complex domains areas, cross-functional areas, and across the supply chain. Confirms the scope and objectives of specific audit activity with management. Aligns with the scope of the audit program and organisational policies. Determines appropriate methods of investigation to achieve the audit objectives. Presents audit findings to management describing the effectiveness and efficiency of control mechanisms. Provides general and specific audit advice. Collaborates with professionals in related specialisms to develop and integrate findings. 	Level 5

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
	Display Resilience and Courage	Be open and honest, prepared to express your views, and willing to accept and commit to change	Intermediate
	Act with Integrity	Be ethical and professional, and uphold and promote the public sector values	Adept

Capability group/sets	Capability name	Description	Level
	Value Diversity and Inclusion	Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives	Intermediate
	Commit to Customer Service	Provide customer-focused services in line with public sector and organisational objectives	Adept
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Adept
	Deliver Results	Achieve results through the efficient use of resources and a commitment to quality outcomes	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	Intermediate
	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

Complementary Specific Focus Capabilities

Complementary / profession specific capabilities			
Capability group/sets	Capability name	Description	Level
	Penetration testing (PENT)	<ul style="list-style-type: none"> Selects appropriate testing approach using in-depth technical analysis of risks and typical vulnerabilities. Produces test scripts, materials and test packs and tests new and existing networks, systems or applications. Provides advice on penetration testing to support others. Records and analyses actions and results and modifies tests if necessary. Provides reports on progress, anomalies, risks and issues associated with the overall project. 	Level 4