

Role Description

Principal IT Security Architect



Customer
Service

Cluster	Customer Service
Agency	Department of Customer Service
Division/Branch/Unit	Digital.NSW/ NSW Telco Authority / Technology
Classification/Grade/Band	Clerk Grade 11/12
ANZSCO Code	262112
PCAT Code	1336368
Date of Approval	August 2020

Primary purpose of the role

Responsible for the design and implementation of technical controls derived from the NSW and Federal Government Cyber Security frameworks and policies and recommendations from other sources including Penetration Tests and Vulnerability Assessments

The role also supports identification of risks and monitors and reports on compliance with security policies and procedures.

Key accountabilities

- Collaborate with team members, business units and other stakeholders to develop, implement and maintain information security controls and standards in alignment with NSW and Federal Government frameworks and policies to ensure the security of information technology systems
- Provide expert input to the strategic direction of technology investments to assist in the development of the information security architecture and roadmap as well as maximise value for money investment
- Undertake investigations and report on security breaches and events, including guiding the refinement of practices and processes and reducing the likelihood and impact of security related incidents
- Manage stakeholder relationships through effective communication, negotiation and issues management to ensure stakeholders are engaged throughout projects and project deliverables are met
- Participate in regular security reviews and manage the coordination of remedial action to recommended solutions to resolve problems and mitigate risks
- Provide expert advice and information to stakeholders on emerging information security issues and present recommendations in line with established frameworks, budgets, timeframes, policy objectives and other project priorities
- Define information security solutions and tools to assist the business in meeting their business objectives

Key challenges

- Lifting current information security maturity levels to comply with applicable policies and frameworks where current levels may be low
- Facilitating an active culture of IT security awareness within the Organisation while continually building knowledge of enhance analysis and advice to key decision-makers
- Maintaining currency and applicability of subject matter knowledge and the relevant legislative, statutory and policy requirements in order to provide high quality, timely advice within a diverse, dynamic environment

Key relationships

Who	Why
Internal	
Manager	<ul style="list-style-type: none"> • 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
Work Team	<ul style="list-style-type: none"> • 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 • Work collaboratively to contribute to achieving business outcomes • Guide others in the development of service level agreements • Collaborate with others to appropriately communicate security related information to relevant stakeholders, customers and partners
External	
Customers / stakeholders	<ul style="list-style-type: none"> • 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 security 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	<ul style="list-style-type: none"> • Manage external security threat analysis and testing • Review threats and vulnerabilities • Review and recommend products and services
Industry professionals/consultants	<ul style="list-style-type: none"> • Participate in forums, groups to represent the agency and share information • Maintain specialist knowledge and keep up with best practice in operations management

Role dimensions

Decision making

This role has autonomy and makes decisions that are under their direct control. 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

Head of Networks and Cyber Security

Direct reports

Nil

Budget/Expenditure

As per Customer Service Delegations

Essential requirements

- Relevant certifications in IT and Cyber Security
- Satisfactory Criminal Record Check
- Must have, or be able to attain and maintain, 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
 <p>Personal Attributes</p>	Display Resilience and Courage Be open and honest, prepared to express your views, and willing to accept and commit to change	<ul style="list-style-type: none"> • Remain composed and calm and act constructively in highly pressured and unpredictable environments • Give frank, honest advice in response to strong contrary views • Accept criticism of own ideas and respond in a thoughtful and considered way • Welcome new challenges and persist in raising and working through novel and difficult issues • Develop effective strategies and show decisiveness in dealing with emotionally charged situations and difficult or controversial issues 	Advanced
	Act with Integrity Be ethical and professional, and uphold and promote the public sector values	<ul style="list-style-type: none"> • Model the highest standards of ethical and professional behaviour and reinforce their use • Represent the organisation in an honest, ethical and professional way and set an example for others to follow • Promote a culture of integrity and professionalism within the organisation and in dealings external to government • Monitor ethical practices, standards and systems and reinforce their use • Act promptly on reported breaches of legislation, policies and guidelines 	Advanced
 <p>Relationships</p>	Communicate Effectively Communicate clearly, actively listen to others, and respond with understanding and respect	<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

FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
	<p>Commit to Customer Service Provide customer-focused services in line with public sector and organisational objectives</p>	<ul style="list-style-type: none"> • Take responsibility for delivering high-quality customer-focused services • Design processes and policies based on the customer's point of view and needs • Understand and measure what is important to customers • Use data and information to monitor and improve customer service delivery • Find opportunities to cooperate with internal and external stakeholders to improve outcomes for customers • Maintain relationships with key customers in area of expertise • Connect and collaborate with relevant customers within the community 	Adept
	<p>Work Collaboratively 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

FOCUS CAPABILITIES

Capability group/sets	Capability name	Behavioural indicators	Level
	<p>Think and Solve Problems</p> <p>Think, analyse and consider the broader context to develop practical solutions</p>	<ul style="list-style-type: none"> • Undertake objective, critical analysis to draw accurate conclusions that recognise and manage contextual issues • Work through issues, weigh up alternatives and identify the most effective solutions in collaboration with others • Take account of the wider business context when considering options to resolve issues • Explore a range of possibilities and creative alternatives to contribute to system, process and business improvements • Implement systems and processes that are underpinned by high-quality research and analysis • Look for opportunities to design innovative solutions to meet user needs and service demands • Evaluate the performance and effectiveness of services, policies and programs against clear criteria 	Advanced
	<p>Technology</p> <p>Understand and use available technologies to maximise efficiencies and effectiveness</p>	<ul style="list-style-type: none"> • Champion the use of innovative technologies in the workplace • Actively manage risk to ensure compliance with cyber security and acceptable use of technology policies • Keep up to date with emerging technologies and technology trends to understand how their application can support business outcomes • Seek advice from appropriate subject-matter experts on using technologies to achieve business strategies and outcomes • Actively manage risk of breaches to appropriate records, information and knowledge management systems, protocols and policies 	Advanced
<h3>Occupation specific capability set</h3>			
	<p>Strategy & Architecture – Information Strategy</p> <p>Information Security</p> <p>The selection, design, justification, implementation and operation of controls and management strategies to maintain the security, confidentiality, integrity, availability, accountability and</p>	<ul style="list-style-type: none"> • Develops and communicates corporate information security policy, standards and guidelines. • Contributes to the development of organisational strategies that address information control requirements • Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks • Leads the provision of authoritative advice and guidance on the requirements for security controls 	Level 7 - SCTY





<p>relevant compliance of information systems with legislation, regulation and relevant standards.</p>	<p>in collaboration with experts in other functions such as legal, technical support</p> <ul style="list-style-type: none"> • Ensures architectural principles are applied during design to reduce risk and drives adoption and adherence to policy, standards and guidelines 	
<p>Development and Implementation-Systems Development Network Design The production of network designs and design policies, strategies, architectures and documentation, covering voice, data, text, e-mail, facsimile and image, to support strategy and business requirements for connectivity, capacity, interfacing, security, resilience, recovery, access and remote access. This may incorporate all aspects of the communications infrastructure, internal and external, mobile, public and private, Internet, Intranet and call centres</p>	<ul style="list-style-type: none"> • Produces outline system designs and specifications, and overall architectures, topologies, configuration databases and design documentation of networks and networking technology within the organisation • Specifies user/system interfaces, including validation and error correction procedures, processing rules, access, security and audit controls • Assesses associated risks, and specifies recovery routines and contingency procedures • Translates logical designs into physical designs. 	<p>Level 5 -NTDS</p>

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	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
	Influence and Negotiate	Gain consensus and commitment from others, and resolve issues and conflicts	Adept
 Results	Deliver Results	Achieve results through the efficient use of resources and a commitment to quality outcomes	Intermediate
	Plan and Prioritise	Plan to achieve priority outcomes and respond flexibly to changing circumstances	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 planning, coordination and control methods	Intermediate
 People Management	Manage and Develop People	Engage and motivate staff, and develop capability and potential in others	Intermediate
	Inspire Direction and Purpose	Communicate goals, priorities and vision, and recognise achievements	Intermediate
	Manage Reform and Change	Support, promote and champion change, and assist others to engage with change	Intermediate

Occupation specific capability set



Strategy & Architecture – Technical strategy and planning Network Planning	The creation and maintenance of overall network plans, encompassing the communication of data, voice, text and image, in the support of an organisation's business strategy. This includes participation in the creation of service level agreements and the planning of all aspects of infrastructure necessary to ensure provision of network services to meet such agreements. Physical implementation may include copper wire, fibre-optic, wireless, or any other technology	Level 5 - NTPL
Strategy and architecture - Technical strategy and planning Emerging Technology Monitoring	The identification of new and emerging technologies, products, services, methods and techniques. The assessment of their relevance and the potential impacts (both threats and opportunities) upon business enablers, cost, performance or sustainability. The communication of emerging technologies and their imp	Level 4 - EMRG
Strategy and architecture - Business strategy and planning IT Management	The management of the IT infrastructure and resources required to plan for, develop, deliver and support IT services and products to meet the needs of a business. The preparation for new or changed services, management of the change process and the maintenance of regulatory, legal and professional standards. The management of performance of systems and services in terms of their contribution to business performance and their financial costs and sustainability. The management of bought-in services. The development of continual service improvement plans to ensure the IT infrastructure adequately supports business	Level 5 – ITMG
Relationships and engagement- Stakeholder management Relationship Management	The systematic identification, analysis, management, monitoring and improvement of stakeholder relationships in order to target and improve mutually beneficial outcomes. Gains commitment to action through consultation and consideration of impacts. Design the relationship management approach to be taken; including roles and responsibilities, governance, policies, processes, and tools, and support mechanisms. Creatively combines formal and informal communication channels in order to achieve the desired result	Level 5 - RLMT