|  |  |
| --- | --- |
| **Classification/Grade/Band** | PSSE Band 1 |
| **ANZSCO Code** | NA |
| **PCAT Code** | NA |
| **Date of Approval** | XXXX |

Primary purpose of the role

The Manager Security Operations is responsible for leading the highly complex development, refinement, implementation and maintenance of security configuration management standards across multiple operating systems and disparate / geographically diverse ICT environments. Devising strategic and tactical interventions, the position engages in complex security operation activities that are critical to the ongoing security and durability of the ICT environment.

Key accountabilities

* Lead the development, refinement, implementation and maintenance of security configuration management standards, policies and guidelines across multiple operating systems in order to deliver crucial ongoing system safety.
* Manage operational compliance with NSW Government Cyber Security Policy, with a key focus on organisation’s crown jewels.
* Lead a team of security operations specialists focused on developing patching and vulnerability management strategy recommendations to quickly and efficiently secure the environment so that system performance and availability is maintained and customer usage is uninterrupted.
* Oversee the evaluation of software/solutions (prior to installation in the environment) in order to ensure reliability of any ICT interventions and potential security risks are managed and mitigated.
* Lead the development and application of effective security control measures to ensure the risk of penetration and security breaches are eliminated, overseeing penetration testing activities including development of a plan for implementation and assessment.
* Act as the escalation/resolution point for sensitive/critical security incidents/alerts, which may require a flexible and adaptable approach to working hours and working arrangements to ensure an effective response and resolution of the security issue.
* Lead the development, implementation and the testing of cyber security incident management processes, major incident management processes and response playbooks in order to improve incident response maturity.

Key challenges

* Identifying new security risks (potentially never seen within the TAFE NSW environment) and developing innovative resolutions to quickly respond, dissipate ICT threats and secure the environment.
* Remaining informed about potential threats within a rapidly evolving cyber security landscape.
* Ensuring sustainability of service provision, often dealing with complex challenges in situations where resolutions must be quickly developed and implemented

Key relationships

| Who | Why |
| --- | --- |
| **Internal** |  |
| Manager | * Receive leadership, advice and support. * Escalate issues, keep informed, advice and receive instructions * Contribute to the development of sustainable technology solutions. |
| Work Team | * Inspire, guide, support and motivate team. * Provide direction and manage performance. * Review work proposals of team members and provide technical specialty to contribute to achieving the team’s business outcomes. * Participate in meetings to obtain the work group perspective and share information. * Support the team and organisation with complex technical issues (e.g. group management and policy development / implementation). * issues, keep informed, advice and receive instructions |
| Agency managers and staff | * Resolve and provide solutions to issues. * Provide consistent and quality technical and/or hardware services advice for business improvement and compliance with TAFE NSW rules/standards. |
| **External** |  |
| Vendors/Service Providers and Consultants | * Manage relationship with strategic vendors and partners to ensure delivery continues to meet business outcomes. * Ensure strategic vendors and partners are compliant with TAFE cyber security policies and NSW Government Cyber Security Policy. |

# Role dimensions

## Decision making

* Makes decisions on complex and sensitive issues through the detailed analysis of alternative courses of action and their implications on achieving organisational objectives and strategies.
* Manage functional expenditure and resourcing within relevant policy and delegation frameworks.
* Matters requiring a higher level of approval are referred to the Reporting Line Manager.

## Reporting line

n/a

## Direct reports

n/a

## Budget/Expenditure

n/a

# Capabilities for the role

The [NSW public sector capability framework](https://www.psc.nsw.gov.au/workforce-management/capability-framework/the-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.

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 [www.psc.nsw.gov.au/capabilityframework/ICT](https://www.psc.nsw.gov.au/workforce-management/capability-framework/occupation-specific-capability-sets/ict-professionals)

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 icon | **Manage Self**  Show drive and motivation, an ability to self-reflect and a commitment to learning | * 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 |
| Relationships icon | **Communicate Effectively**  Communicate clearly, actively listen to others, and respond with understanding and respect | * Tailor communication to diverse audiences * Clearly explain complex concepts and arguments to individuals and groups * Create opportunities for others to be heard, listen attentively and encourage them to express their views * Share information across teams and units to enable informed decision making * Write fluently in plain English and in a range of styles and formats * Use contemporary communication channels to share information, engage and interact with diverse audiences | Adept |
| Results icon | **Deliver Results**  Achieve results through the efficient use of resources and a commitment to quality outcomes | * Seek and apply the expertise of key individuals to achieve organisational outcomes * Drive a culture of achievement and acknowledge input from others * Determine how outcomes will be measured and guide others on evaluation methods * Investigate and create opportunities to enhance the achievement of organisational objectives * Make sure others understand that on-time and on-budget results are required and how overall success is defined * Control business unit output to ensure government outcomes are achieved within budgets * Progress organisational priorities and ensure that resources are acquired and used effectively | Advanced |
|  | **Think and Solve Problems**  Think, analyse and consider the broader context to develop practical solutions | * 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 |
| Business Enablers icon | **Technology**  Understand and use available technologies to maximise efficiencies and effectiveness | * 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 |
| People Management icon | **Optimise Business Outcomes**  Manage people and resources effectively to achieve public value | * Initiate and develop longer-term goals and plans to guide the work of the team in line with organisational objectives * Allocate resources to ensure the achievement of business outcomes and contribute to wider workforce planning * When planning resources, implement processes that encourage the attraction and retention of people of diverse cultures, backgrounds and experiences * Ensure that team members base their decisions on a sound understanding of business and risk management principles, applied in a public sector context * Monitor performance against standards and take timely corrective actions * Keep others informed about progress and performance outcomes | Adept |

| **Occupation specific focus capability set** | | | |
| --- | --- | --- | --- |
| Capability Set / Skill | Category and Sub-Category | Level Descriptions | Level and Code |
| Security administration  Skills Framework for the Information Age logo | Delivery and operation  Service operation | * Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. * Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented. * Ensures that security records are accurate and complete and that request for support are dealt with according to set standards and procedures. * Contributes to the creation and maintenance of policy, standards, procedures and documentation for security. | SCAD  Level 5 |
| Penetration testing  Skills Framework for the Information Age logo | Delivery and operation  Service operation | * Coordinates and manages planning of penetration tests, within a defined area of business activity. * Delivers objective insights into the existence of vulnerabilities, the effectiveness of defences and mitigating controls - both those already in place and those planned for future implementation. * Takes responsibility for integrity of testing activities and coordinates the execution of these activities. * Provides authoritative advice and guidance on the planning and execution of vulnerability tests. * Defines and communicates the test strategy. * Manages all test processes, and contributes to corporate security testing standards. | PENT  Level 5 |
| Incident management  Skills Framework for the Information Age logo | Delivery and operation  Service operation | * Ensures that incidents are handled according to agreed procedures. Investigates escalated incidents to responsible service owners and seeks resolution. * Facilitates recovery, following resolution of incidents. * Ensures that resolved incidents are properly documented and closed. * Analyses causes of incidents, and informs service owners in order to minimise probability of recurrence, and contribute to service improvement. * Analyses metrics and reports on performance of incident management process. | USUP  Level 5 |
| Information security  Skills Framework for the Information Age logo | Strategy and architecture  Information strategy | * Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. * 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. * Contributes to development of information security policy, standards and guidelines. | SCTY  Level 5 |
| Business risk management  Skills Framework for the Information Age logo | Strategy and architecture  Business strategy and planning | * Carries out risk assessment within a defined functional or technical area of business. * Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. * Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. * Co-ordinates the development of countermeasures and contingency plans. | BURM  Level 5 |
| Digital forensics  Skills Framework for the Information Age logo | Skills and quality  Quality and conformance | * Conducts investigations to correctly gather, analyse and present the totality of findings including digital evidence to both business and legal audiences. * Collates conclusions and recommendations and presents forensics findings to stakeholders. * Contributes to the development of policies, standards and guidelines. | DGFS  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.

| **COMPLEMENTARY CAPABILITIES** | | | |
| --- | --- | --- | --- |
| Capability group/sets | Capability name | Description | Level |
| Personal Attributes icon | Display Resilience and Courage | Be open and honest, prepared to express your views, and willing to accept and commit to change | Adept |
| Act with Integrity | Be ethical and professional, and uphold and promote the public sector values | Intermediate |
| Value Diversity and Inclusion | Demonstrate inclusive behaviour and show respect for diverse backgrounds, experiences and perspectives | Intermediate |
| Relationships icon | 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 |
| Results icon | 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 | Intermediate |
| Business Enablers icon | Finance | Understand and apply financial processes to achieve value for money and minimise financial risk | Adept |
| Procurement and Contract Management | Understand and apply procurement processes to ensure effective purchasing and contract performance | Adept |
| Project Management | Understand and apply effective planning, coordination and control methods | Adept |
| People Management icon | Manage and Develop People | Engage and motivate staff, and develop capability and potential in others | Adept |
| 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 | Adept |

| Occupation specific complimentary capabilities | | | |
| --- | --- | --- | --- |
| **Capability Set / Skill** | **Category and Sub-category** | **Description** | **Level and Code** | |
| Problem management  Skills Framework for the Information Age logo | Delivery and operation  Service operation | The resolution (both reactive and proactive) of problems throughout the information system lifecycle, including classification, prioritisation and initiation of action, documentation of root causes and implementation of remedies to prevent future incidents. | Level 5  PBMG | |