GOVERNMENT OF WESTERN AUSTRALIA

Department of **the Premier and Cabinet**
Office of Digital Government

Cyber Security Operations

A guideline to support implementation of Western Australian Cyber Security Policy clause 1.3 (Cyber Security Operations)

2024

Produced and published by
Office of Digital Government
Department of the Premier and Cabinet
Published **August 2024**

Principal address:
Dumas House
2 Havelock Street
West Perth WA 6005

Postal address:
Locked Bag 3001
West Perth WA 6872

Telephone: (08) 6552 5000
Fax: (08) 6552 5001
Email: Cyber.Policy@dpc.wa.gov.au

Acknowledgement of Country

The Government of Western Australia acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders past, present and emerging.

Approval

Name / Title	Date
Peter Bouhlas Chief Information Security Officer	24 July 2024

Contact Officers

Name	Email	Phone
Danijela Kambaskovic-Schwartz	Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au	+61 8 6552 6020
Sandra Franz	Sandra.Franz@dpc.wa.gov.au	+61 8 6551 3971

Contents

1. The relevant WA Cyber Security Policy clause

1.3 Cyber Security Operations

Each entity must ensure sufficient technical cyber security capability (HR) is available to implement this Policy and ensure the continuity of its implementation.

2. Responsibility for implementation

Responsibility for implementing this clause lies with the Cyber Security Executive, in collaboration with the Head of Human Resources and Head of Procurement, as appropriate.

3. Overview – establishing and improving cyber security operations

The WA Government Cyber Security Policy (the Policy) requires that Western Australian Government entities have sufficient cyber security capacity and capability for the Policy to be implemented.

This guideline is intended to assist the Cyber Security Executive and managers in making appropriate staffing decisions to ensure successful implementation of the Policy.

Security Operations staff report to the ICT Managers or directly to Cyber Security Executive and have responsibilities related to:

- ICT Asset inventory
- Information Security Risk assessment
- Implementation of Information Security controls
- Vulnerability monitoring and remediation
- Incident management and response
- Asset backup and recovery

An entity's operational cyber security capability must be continually assessed, and staffing gaps addressed to maintain a robust cyber security posture.

3.1 Gap Analysis

An initial gap analysis is essential to determine the adequacy of your entity's current operational capability to your entity's current or future needs. This will inform your decision making to determine the most efficient and cost-effective method to build your entity's cyber security operations.

3.2 Regular reviews

Once in place, the entity should undertake regular reviews of the structure of operational teams and their capability to manage operational requirements.

3.3 Improving workforce capability

Entities should take steps to upskill their workforce and improve their operational capability as their needs develop.

4. Guidance

4.1 Gap Analysis

Initial gap analysis

Step 1: Assess your entity's needs:

- the complexity and criticality of the entity's systems
- the confidentiality / classification of the entity's information
- the entity's need for data integrity and availability
- the entity's tolerance for system and service disruption
- the entity's data sharing needs
- the number of staff using the ICT services
- the skill level and knowledge of the existing staff.

Step 2: Rate your entity's ability to implement the requirements of the Cyber Security Policy.

Step 3: Identify any gaps by comparing the current capability against the capability required for Policy implementation. This will help to understand which ICT staff might initially be impacted by the Policy and the pace at which you'll need to enhance their skills or expand the team.

Step 4: Anticipate future workforce changes.

Step 5: Determine a Policy implementation timeline and understand and record the scope, scale and costs of the implementation process (a Roadmap).

Determine needs based on the size of the organisation

Operational security analyst roles should start at 2 FTE, scaling up by an additional 1 FTE for every 1000 staff members. These roles are responsible for managing:

- Endpoint Devices (Endpoint Detection and Response, e.g., Microsoft Defender)
- Servers and Applications (Web Application Firewall, External Attack Surface Management, Platforms & Infrastructure)
- Network Traffic Analytics (i.e., flow baselining and alerting on deviations)
- Training and Awareness (increasing staff understanding of secure use of technology)

Consider the cost of an in-house Cyber Security Analyst

A typical starting cost to hire a cyber security analyst is around AUD$40 000, which equates to 200 hours per year at AUD$200 per hour). This includes:

- Monitoring 50-200 staff with 2-3 incidents requiring investigation daily
- Spending 10 hours per month (or 120 hours per year) on triaging incidents
- Allocating 20 hours per quarter (or 80 hours per year) to detection engineering

Determine the best approach based on cost

Utilising the provided sizing information and the basic cost assessment, determine the most suitable method for establishing operational cyber security capability:

1. Recruitment (either permanent or fixed-term)
2. Short-term contract staff
3. Appointment of a managed service provider (below)

Office of Digital Government-recommended approach to establishing cyber security operational capability

Office of Digital Government has developed a recommendation of optimal options (combinations) of in-house staff and Managed Service Providers (MSPs) depending on entity size. Please note that traditional IT service roles (or MSPs performing traditional ITSM and user support helpdesk roles) are not included in this recommendation and are additional. S

Entity size	External contractors	Internal (in-house) staff
Under 500 staff	**Option 1**	
	• 1 Managed Service Provider (Outcome - as-a-Service) responsible for operating infrastructure, applications, cyber security, threat detection, incident response and **connection to WA SOC, AND**	• Cyber Security Executive • 1-2 FTE dedicated to IT/Cyber Security Governance, Risk and Compliance (GRC) roles responsible for cyber security governance and management of services to ensure information security risks are controlled.
	Option 2	
	• 1 Managed Service provider Software-as-a-Service or public cloud and internet services, **AND**	• Cyber Security Executive • 1-2 FTE dedicated to IT/Cyber Security Governance, Risk and Compliance (GRC) roles (responsible for cyber security governance and management of services to ensure information security risks are controlled), **AND** • 2-3 FTE dedicated to management of network, infrastructure and applications, cyber security, threat detection, incident response and **connection to WA SOC.**
500-2000 staff	**Option 1a**	
	• 1 Managed Service Provider (Outcome as a Service) responsible for operating infrastructure, applications, cyber security, threat detection, incident response and **connection to WA SOC, AND**	• Cyber Security Executive • 1-2 FTE dedicated to IT/Cyber Security Governance, Risk and Compliance (GRC) roles (responsible for cyber security governance and management of services to ensure information security risks are controlled.)
	Option 1b	
	More than 1 Managed Service Provider	• Cyber Security Executive

Entity size	External contractors	Internal (in-house) staff
	• For example, 1 or more Managed Service Providers responsible for cloud computing, operating infrastructure and applications; and • 1 Managed Service Provider providing dedicated Managed Detection and Response (MDR) service responsible for cyber security, threat detection, incident response and **connection to WA SOC; AND**	• 1-2 FTE dedicated to IT/Cyber Security Governance, Risk and Compliance (GRC) roles (responsible for cyber security governance and management of services to ensure information security risks are controlled).
	Option 2	
	• 1 Managed Service provider ○ Responsible for Software-as-a-Service or public cloud only and internet services, **AND**	• Cyber Security Executive • 1-2 FTE dedicated to IT/Cyber Security Governance, Risk and Compliance (GRC) roles (responsible for cyber security governance and management of services to ensure information security risks are controlled), **AND** • 3-10 FTE dedicated to cyber security roles responsible for managing networks, operating infrastructure and applications, cyber security, threat detection, incident response and **connection to WA SOC.**
Over 2000 staff	**One recommended option**	
	• 1 Managed Service provider responsible for public cloud computing (Infrastructure-as-a-Service (public cloud), Software-as-a-Service, public cloud only and internet services, **AND**	• Cyber Security Executive • FTE equivalent to 0.1% of total organisational FTE dedicated to IT/ Cyber Security Governance, Risk and Compliance (GRC) roles (responsible for cyber security governance and management of services to ensure information security risks are controlled[1]), **AND** • FTE equivalent to 0.5% of total organisational FTE dedicated to roles managing operating infrastructure and applications, cyber security, threat detection, incident response and **connection to WA SOC.**

Getting assistance

If you believe that your entity lacks the necessary resources to confidently conduct this gap analysis and ascertain your operational needs, you can consult with the Cyber Security Unit of the Office of Digital Government at cyber.policy@dpc.wa.gov.au

Alternatively, you may choose to hire a supplier to perform the initial gap analysis on your behalf. In this case, you would need to create a Scope of Work statement to guide the supplier's work instructing the supplier to:

- carry out a capability gap analysis to identify your entity's cyber security needs and

[1] In organisations with multiple business units, these roles may be distributed, but should work together across business units.

- provide recommendations on how to effectively establish or expand your entity's cyber security operations.

You can procure this service through the Information and Communications Technology (ICT) Services CUAICTS2021, under Category 1 (Planning, Consultancy, and Advisory Services).

To determine information security requirements you need to be mindful of when procuring the services of ICT consultants, please refer to DGov's *Overview of Information Secure Procurement* and *WA Cyber Security Policy Implementation Guideline 3.4 Information Secure Procurement.*

4.2 Reviewing Workforce Capability

This section offers guidance on how to assess staff cyber security skills.

Skills Framework for an Innovation Age

Skills Framework for the Information Age (SFIA) is a global standard for describing skills and competencies required by professionals in information and communication technologies (ICT), software engineering and digital transformation roles.

NICE Framework

The US National Initiative for Cybersecurity Careers and Studies (NICCS) Workforce Framework for Cyber Security (NICE Framework) offers a comprehensive set of components that assist organisations in building their cybersecurity workforce at various levels and types of cybersecurity positions.

The framework is also beneficial for education, training, hiring and workforce development. For additional information, refer to the NICE Framework Resource Center.

Public Sector Commission Digital Capability Framework

The Public Sector Commission provides a digital capability guide to support systematic workforce planning for a future fit, digitally capable workforce. It aims to improve mobility across the sector for digital professionals by improving consistency in how the sector describes capability requirements. For more information, please see

International Organisation for Standardisation (ISO) standard 27021

ISO Standard 27021 sets out competency requirements for information security management systems professionals.

ANZCO codes

The Australia New Zealand Standard Classification of Occupations (ANZCO) is underpinned by a comprehensive review of JDFs used across Australia to determine capability commonalities across roles.

The purpose of ANZCO codes is to remove confusion which can often arise from variations in position titles, with the expectation that various position titles grouped under the **same code** will require **the same capabilities.**

DGov has compiled ANZCO codes for cyber security-related specialisations to aid managers in identifying the capabilities required to perform cyber security and information security related tasks.

For more information, please refer also to 4.5 Capability Profiles and Appendix 1.

Reviewing JDFs

Regularly updating job description forms (JDFs) is crucial to reflect changes in tasks or responsibilities within an entity, and to assist Policy implementation. This enables ICT managers to align roles with the evolving nature of ICT and the entity's business needs.

Please refer to examples of JDFS provided in Appendix 2.

Review your entity's governance and management processes to ensure they have been adjusted to include the new staff.

4.3 Improving Workforce Capability

To properly implement the Policy, further skills may be required and staffing levels adjusted. This could mean upskilling staff, recruiting new staff, bringing in external specialists, or outsourcing some Policy tasks to a Managed Service Provider (MSP).

Upskilling existing employees

Some capability gaps may be addressed by training existing staff.

The Office of Digital Government (DGov) recommends the following training for ICT staff:

- TAFEcyber E8 Assessor course
- SOC Analyst Induction - Security Analyst Induction - WA Cyber Security Unit (DGOV Technical)
- Azure VM Basic Training - Azure Basics - WA Cyber Security Unit (DGOV Technical)

Please see 3.2 Cyber Security Training Guidelines for more information.

Recruiting employees

Office of Digital Government Cyber Pool

The Office of Digital Government has created and is continuously renewing a pool of cyber security professionals (levels 4, 5 and 6) who have been interviewed by DGov and Government sector cyber security specialists.

The pool is intended to assist WA Public Sector entities in making permanent or fixed-term appointments and will operate for a period of 24 months. For more information, please contact cyber.policy@dpc.wa.gov.au

See Appendix 2 for details of the relevant job descriptions.

Procuring Short-term contractors the Department of Finance Services

If your entity needs cyber security experts on a short-term basis due to cost constraints, you can procure short term cyber security contractors.

Create a Scope of Work statement detailing the required operational capability and hire short-term contractors in accordance with the Western Australian Procurement Rules.

The Department of Finance (DoF) offers two methods of short-term temporary contractors:

1) Through Information and Communications Technology (ICT) Services CUAICTS2021 (Category 3)
2) Through Personnel Services CUATPS2019 (Category D)

More information on how to choose between the two approaches is provided here: ICT Services versus Temporary Personnel (www.wa.gov.au)

1) ICT Services CUAICTS2021

There are three categories in this section. Only **Category 3 – Operations and Management Services** enables managers to procure operational capability. DoF **has** described the roles in this section with reference to ANZCO.

DoF has advised that the purpose of the CUAICTS2021 Category 3 is not for the short-term hire of personnel, but only for the engagement of specific ICT roles to deliver a “time based” service or outcome for which ICT is essential.

2) Temporary Personnel Services CUATPS2019

There are 4 categories in this section. Only **Category D (ICT)** applies to procuring short-term staff with ICT expertise.

Please note that DoF **did not** describe the roles in this section with reference to ANZCO. To facilitate the understanding of required capability, DGov has mapped Temporary Personnel Services roles to ANZCO codes.

The Department of Finance-prescribed Category D (ICT) positions mapped to ANZCO codes and position descriptions

Category of personnel prescribed in the Category D (ICT) of the Temporary Personnel Services CUATPS2019	ANZCO Code (Capability)	ANZCO position description variations
Analyst/Programmer	261311	Analyst Programmer
	26112	Systems Analyst
Asset and Service Coordinator	135199	ICT Managers NEC (Not Elsewhere Classified)
	135119	IT Service Delivery Manager
Application/Business Analyst	261111	Business Analyst (ICT)
Business Intelligence Analyst		Business Consultant (ICT)
		Business Systems Analyst
		ICT Business Analyst
Build and Deploy Officer	135112	ICT Project Manager
		ICT Development Manager
		ICT Security Project Manager
Communications Engineer/Technician	263311	Telecommunications Engineer
	263312	Telecommunications Network Engineer
		Telecommunications Specialist
	313199	Computer systems technician
Data Analyst	224114	Data Analyst
Database Developer	261312	Database developer
Desktop Support	313112	Systems Support Officer
Digital Information Security Officer	26115	ICT Security Consultant
		Cyber Security Advice and Assessment Specialist
		Cyber Security Adviser
		Cyber Security Consultant
		ICT Security Adviser
	262116	Information Security Analyst
		Cyber Security Analyst
		ICT Security Analyst

		Malware analyst
		Cyber Threat Analyst
		Cyber Security Vulnerability Assessor
		Cyber Security Researcher or Vulnerability Researcher
Enterprise/Solutions Architect	262117	Enterprise Security Architect
		Cyber Security Architect
		ICT Security Architect
Help Desk Support	313112	ICT Help Desk Officer
Online Services Officer		ICT Customer Support Officer
Service Desk Analyst/Officer		ICT Help Desk Technician
		Network Support Technician
		Systems Support Officer
Network Administrator/Engineer	263111	Computer Network and Systems Engineer
		Computer Network Engineer
		Computer Systems Integrator
Infrastructure Service Coordinator	263112	Network Administrator
		Network Specialist
		LAN Administrator
		Network Support
	263113	Network Analyst
.NET Architect/Developer		Network Architect
		Network Consultant
		Network Designer
		Network Strategist
Project Manager ICT	135112	ICT Project Manager
		ICT Development Manager
		ICT Security Project Manager
Software Developer	261312	Developer programmer
		Software Developer
		Software Programmer
Technical Application Specialist		Applications Developer
		Cyber Security Developer
		Database Developer

		Database Programmer
		ICT Developer
		ICT Programmer
		Network Programmer
Systems Administrator	262113	Systems Administrator
		Systems Manager
Test Analyst	263213	ICT Systems Test Engineer
		Systems Tester
		Test Analyst
Web Administrator/Developer	313113	Web Administrator
		Web master

Cyber Security Specialisations

The Department of Finance has advised that although the Temporary Personnel Services CUA (CUATPS2019) Category D - ICT does not explicitly list cyber security specialisations, all cyber security specialisations listed above can be procured using the Temporary Personnel Services CUA (CUATPS2019) Category D - ICT as they fall broadly within the intention of its scope.

Recruiting external temporary contractors (Managed Service Providers)

If the size of the organisation makes it challenging to justify a business case to employ staff, consider engaging an external Managed Service Provider (MSP) to provide you with the required capability.

Suppliers offer two types of cyber security services:

- Managed Detection and Response (MDR) and
- Managed Security Services Providers (MSSPs).

Managed Detection and Response

MDR encompasses threat hunting, monitoring, and incident response. In case of a security breach, the service provider collaborates with customers to resolve the issue and recover. MDR response capabilities can range from full to limited, depending on the vendor.

Benefits of MDR include:

- Cost-effectiveness compared to an in-house cyber security team
- Continuous threat hunting and response
- Oversight and maintenance of tools and technology
- ICT workforce optimisation
- Enhanced security configuration.

MDR might be necessary if your entity requires, but does not have, an internal Security Operations Centre (SOC), lacks trained cyber security staff, or has fully outsourced ICT work.

For more information on detection and response, please see Policy Implementation Guidance for WA Cyber Security Policy domains 4 (Detect), 5 (Respond) and 6 (Recover).

Managed Security Services Provider

MSSP or SOC-as-a-service provide network event monitoring and send validated alerts to other tools or the organisation's security team. MSSP may also other services, including technology management, upgrades, compliance, and vulnerability management.

Benefits of MSSP include:

- Provision of stop-gap services
- ICT workforce optimisation
- Cheaper than MDR.

MSSP might be sufficient if your entity relies on the WA SOC, handles non-sensitive data, requires basic security tasks, and/or operates under budget constraints.

Managed service providers can be procured using Information and Communications Technology (ICT) Services CUAICTS2021 Category 3 – Operations and Management Services.

To determine information security controls please refer to DGov's *Overview of Information Secure Procurement* and WA Cyber Security Policy Implementation Guideline 3.4 Information Secure Procurement.

4.5 Capability Profiles

Level 4

Cyber Security Analyst

Assists in the ongoing development and maintenance of information systems risk and security controls to protect the information assets of WA Public Sector entities. Provides support for cyber security situational awareness.

Level 5

Senior Cyber Security Analyst

Assists in the ongoing development, implementation and maintenance of information systems risk and security controls to protect the information assets of WA Public Sector entities. Provides incident response support and collaborates with DGov to restore functionality.

Senior Cyber Security Specialist

The Senior Cyber Security Specialist is responsible for assisting in designing and implementing programs of work to increase the WA Government entity's cyber security maturity.

In the context of the WA Government's digital transformation priorities, the Senior Cyber Security Specialist will support the successful implementation of the WA Government Cyber Security Policy to support the Digital Strategy for the WA Government.

Cyber Security Tester

Undertakes cyber security and technical vulnerability testing of entity's systems, networks, and applications. Coordinates with the DGov's cyber security testing program, strategies, work plans, technology/tools, and associated program documentation. Works with internal and external stakeholders to execute the security testing program. Contributes to policy support and advice and contributes to projects to deliver expected outcomes within agreed timeframes.

Cyber Communications and Awareness Specialist

The Cyber Communications and Awareness Specialist is responsible for assisting in designing and implementing programs of work to increase the WA Government entity's cyber security maturity.

In the context of the WA Government's digital transformation priorities, the Cyber Communications and Awareness Specialist will support the successful implementation of the WA Government Cyber Security Policy to support the Digital Strategy for the WA Government.

Level 6 or Level 7

Principal Cyber Security Analyst

Leads the ongoing development, implementation and maintenance of information systems risk and security controls to protect the information assets of WA Public Sector entities. Provides incident response support and collaborates with DGov to restore functionality.

Principal Cyber Security Specialist

The Principal Cyber Security Specialist is responsible for assisting in designing and implementing programs of work to increase cyber security maturity.

In the context of the Government's digital transformation priorities, the Principal Cyber Security Specialist (Infrastructure) will support the successful implementation of the WA Government Cyber Security Policy to support the Digital Strategy for the WA Government.

Senior Cyber Security Tester

The Senior Cyber Security Tester is responsible for undertaking cyber security and technical vulnerability testing of entity's systems, networks, and applications.

In the context of the Government's digital transformation priorities, the Senior Cyber Security Tester will identify vulnerabilities and provide remediation advice to enable the safe and secure delivery of WA Government digital services, supporting the Digital Strategy for the WA Government.

Chief Information Security Officer

A key strategic role that researches and evaluates contemporary and emerging technology in the agency operations context to facilitate high-level decision making with respect to technological capabilities to be established for public sector ICT delivery.

If you require assistance developing job description forms, please contact cyber.policy@dpc.wa.gov.au

4.6 Training

Essential Eight Assessment Course

The Australian Signals Directorate (ASD) in partnership with TAFEcyber. provides an Essential Eight Assessment Course. The course is designed to assess understanding of ASD's key cyber security incident mitigation controls.

The course helps staff interested in developing their cyber security operations and ICT skills to:

- understand the intent and application of the Essential Eight
- learn how to use ASD-designed tools
- accurately assess implementation of the Essential Eight
- define an action plan to address any security weaknesses.

In WA, the course is facilitated North and South Metropolitan TAFEs.

ISO

The International Organisation for Standardisation (ISO) provides Information Security certification. ISO/IEC 270001 is a globally accepted standard for information security management systems (ISMS) and defines ISMS requirements. ISO/IEC 27001 provides guidance for establishing, implementing, maintaining, and continually improving an information security management system.

Tertiary Education

Australian universities offer Bachelors, Master's or PhD level qualifications in the following areas:

- Cyber security
- Computer science

- Computer information systems
- Business administration
- Information assurance
- Informatics.

NICCS

The National Initiative for Cybersecurity Careers and Studies' (NICCS) NICE Framework assists employers to develop their cybersecurity workforce. Topics include:

- Core qualifications for executives
- Managerial and operational workforce needs
- Conveying risk to stakeholders
- Technical skills.

SANS Institute

The SANS Institute provides training and certification in cyber security operations, including:

- Layers of offensive testing
- Defensive architecture and monitoring
- Forensics and incident response
- Cloud security
- Leadership.

5. Additional Resources

Additional resources for developing a Cyber Security Incident Operations team include:

- Guidelines for Cyber Security Roles | Cyber.gov.au
- Australian Signals Directorate (ASD) - ASD Cyber Skills Framework
- Azure VM Basic Training - Azure Basics - WA Cyber Security Unit (DGOV Technical)
- Crowstrike - MDR vs MSSPs: Uncovering Key Differences - CrowdStrike
- DGov Job Description Forms - Cyber.Policy@dpc.wa.gov.au.
- International Organisation for Standardisation (ISO) - ISO/IEC 27001:2022 - Information security management systems — Requirements
- National Initiative for Cybersecurity Careers and Studies (NICCS) - Workforce Framework for Cybersecurity (NICE Framework) | NICCS (cisa.gov)
  North Metropolitan TAFE - Essential Eight Training Program | North Metropolitan TAFE (northmetrotafe.wa.edu.au)
- South Metropolitan TAFE - Essential 8 Assessment Course | South Metropolitan TAFE (southmetrotafe.wa.edu.au)
- WA Government - Digital Capability: A Guide for Agencies (www.wa.gov.au)
- WA Government - ICT Services versus Temporary Personnel (www.wa.gov.au)
- WA Government - Information and Communications Technology Services CUAICTS2021 (www.wa.gov.au)

- SOC Analyst Induction - Security Analyst Induction - WA Cyber Security Unit (DGOV Technical)
- SANS Institute - Cyber Security Roles | SANS Institute
- Skills Framework for the Information Age | Australian Public Service Commission (apsc.gov.au)
- Workforce Framework for Cybersecurity (NICE Framework) | NICCS (cisa.gov)
- ASD - Puzzles and challenges | Australian Signals Directorate (asd.gov.au)

Appendix 1

ANZCO Code (Capability)	ANZCO Position Title variations (Cyber security specialists)
Cyber Security Specialists	
262115	Cyber Security Advice and Assessment Specialist
	Cyber Security Adviser
	Cyber Security Consultant
262116	Cyber Security Analyst
	Cyber Security Vulnerability Assessor
	Cyber Security Researcher or Vulnerability Researcher
	Cyber Threat Analyst
262118	Cyber Security Operations Manager
	Cyber Security Incident Responder
261312	Cyber Security Developer
Architects/Engineers – Technical, Enterprise, Network and Solutions	
262117	Cyber Security Architect
261315	Cyber Security Engineer
262111	Computer Network and Systems Engineer
2632211	Computer Systems Auditor
263111	Computer Systems Integrator
313199	Computer Systems Technician
263112	Network Administrator
	Network Specialist
	Network Support
	Network Support Technician
263113	Network Analyst
	Network Consultant
	Network Designer
	Network Strategist
261312	Network Programmer
135199	Network Manager
Systems Integration and Application Specialists (Infrastructure and Systems Administration)	
262113	Systems Administrator
261112	Systems Analyst

261313	Systems Architect
263211	Systems Auditor (ICT)
262113	Systems Manager
313112	Systems Support Officer
263213	Systems Tester
261316	DevOps Engineer
	Cloud Computing Engineer
	Continuous Integration Engineer
261399	Infrastructure/Software/App Development
232214	Spatial Analysts
Enterprise Information Security Management	
224999	Information Management Co-ordinator
541211	Information Officer
262116	Information Security Analyst
261315	Information Security Engineer
Cyber threat specialists	
262116	Information Security Analyst
	Cyber Security Analyst
	ICT Security Analyst
	Malware analyst
	Cyber Threat Analyst
	Cyber Security Vulnerability Assessor
	Cyber Security Researcher or Vulnerability Researcher

Appendix 2

Senior Cyber Security Analyst, Level 5

About the Role and Responsibilities

Senior Cyber Security Analysts are responsible for analysing data collected from various cyber security defence tools and supporting continuous improvement of Security Operational capabilities to mitigate cyber security threats. Senior Security Specialists will draw on their expertise of cyber security threats, incident management and will support agencies in meeting the requirements of the WA Cyber Security Policy.

Directorate:

Reports to:

Branch/Section: Cyber Security Unit/Technical Supervises: 0 FTE

Cyber Security tasks

- Monitors, assesses and assist in the continual improvement of the performance of information systems security services and controls.
- Coordinates between internal and external partners with respect to the delivery of information security services.
- Identify and analyse cyber threats, investigate security breaches, assess operational impacts, assisting with incident management, and prioritise risk treatments to enhance organizational cybersecurity.
- Coordinates, performs and support scheduled security scans, reviews and compliance testing to ensure adherence to information security policies, standards and procedures and identify and execute against opportunities for improvement.
- Delivers information security awareness and education, based on standards, trends and alerts from appropriate industry and security monitoring services.
- Provides information security policy, technical and operational advice to relevant stakeholders.
- Assists in the development and maintenance of information security policies, standards, procedures and frameworks including but not limited to incident response plans, escalation playbooks and disaster recovery procedures.
- Provides guidance and support to junior staff.

Corporate Responsibilities

- Exhibits accountability, professional integrity and respect consistent with DPC Values, the Code of Conduct, and the public sector Code of Ethics.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Work Health and Safety Act 2020
- Undertakes other duties as required.

Work Related Capabilities (Selection Criteria)

1. Well-developed conceptual and analytical skills with the ability to apply these to the treatment of modern cyber security threats and resolve complex problems.

2. Working experience in the identification and resolution of information security incidents, against appropriate security frameworks (for example MITRE ATT&CK), principals, policies, and standards.
3. Working knowledge of information security technologies, such as vulnerability management, authentication and access control, next-gen firewalls, data leakage protection, endpoint protection, SIEM and relevant cloud security solutions.
4. Well-developed written communication skills and interpersonal, and the ability to consult with internal and external stakeholders.
5. Experience working as part of multidisciplinary and cross functional teams and can understand the organisations objectives and align operational activities accordingly.

Desirable

- Possession of or progression towards a relevant tertiary qualification.
- Possession of relevant industry certifications for security (e.g. Security+, CC, SC-200, CSX-P, GSOC, CISSP).
- Knowledge and experience in providing information security services within a government or large corporate environment.

To be eligible for permanent appointment to the role, employees must also be eligible to live and work in Australia indefinitely. Employees engaged on fixed term appointments need a valid work visa for the duration of their contract.

Appointment is also dependent on a 100-point identification check and Criminal Records Screening Clearance.

Principal Cyber Security Analyst, Level 6

About the Role and Responsibilities

Directorate:

Reports to:

Supervises: 2 FTE Location: Perth Metro

Principal Cyber Security Analysts are responsible for the coordination of the cyber security incident response, threat Intelligence and supporting the continuous improvement security operations capabilities to mitigate cyber security threats. Principal Cyber Security Analysts will draw upon their expertise of cyber security threats, cyber situational awareness, incident management and will support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security Tasks

Leadership and Management

- Leads and motivates staff within the Team to coordinate Cyber Security Threat Intelligence and Incident Response activities.
- Promotes a culture supportive of innovation and continuous business process improvement.
- Provides information security policy, technical and operational advice on Cyber Security Threat Intelligence and Incident Response capabilities and processes.

- Works collaboratively with team members and peers to process threat intelligence and incident response workflows effectively and efficiently.
- Management of objective based initiatives to expand cyber security capabilities to the team and peers.
- Develops and maintains information security standards, policies and procedures.

Threat Intelligence & Incident Response Coordination

- Priorities and diagnoses information security breaches, undertakes root cause analysis, and assists in security incident investigation, resolution, and prevention.
- Lead strategic cyber threat intelligence efforts, direct high-impact security investigations, evaluate critical operational risks, and design risk mitigation strategies to strengthen organizational cybersecurity resilience.
- Gather real-time threat intelligence to maintain an accurate operational picture and coordinate with sharing of threat intel to relevant parties.
- Monitors, assesses, and assist in the continual improvement of the performance of information systems security services and controls.

Corporate Responsibilities

- Exhibits accountability, professional integrity and respect consistent with DPC Values, the Code of Conduct, and the public sector Code of Ethics.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Work Health and Safety Act 2020
- Undertakes other duties as required.

Work Related Capabilities (Selection Criteria)

1. Well-developed conceptual and analytical skills with the ability to apply these to the treatment of modern cyber security threats and resolve complex problems.
2. Considerable experience in the identification and resolution of information security incidents, against appropriate security frameworks (for example MITRE ATT&CK), principals, policies, and standards.
3. Considerable experience in the use of information security technologies, such as vulnerability management, authentication and access control, next-gen firewalls, data leakage protection, endpoint protection, endpoint forensics, threat enrichment, SIEM and relevant cloud security solutions.
4. Well-developed written communication skills and interpersonal, and the ability to consult with internal and external stakeholders.
5. Experience working as part of multidisciplinary and cross functional teams and can understand the organisations objectives and align operational activities accordingly.

Desirable

- Possession of or progression towards a relevant tertiary qualification.
- Possession of relevant industry certifications for security (e.g. Security+, CC, SC-200, CSX-P, GSOC, CISSP).
- Knowledge and experience in providing information security services within a government or large corporate environment.

To be eligible for permanent appointment to the role, employees must also be eligible to live and work in Australia indefinitely. Employees engaged on fixed term appointments need a

valid work visa for the duration of their contract. Appointment is also dependent on a 100-point identification check and Criminal Records Screening Clearance.

Senior Cyber Security Specialist Level 5

Directorate:

Branch/Section:

Supervises: 0 FTE

About the Role and Responsibilities

Senior Cyber Security Specialists are responsible for supporting the design, implementation and assurance of cyber security controls that protect information systems from cyber security threats. Cyber security specialists will draw on their expertise of cyber security threats, vulnerabilities, governance, and cyber security frameworks to support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security Tasks

- Designs, configures, or contributes the implementation of cyber security controls for information systems and system components.
- Performs security assessments, reviews and compliance testing to ensure adherence to information security policies, standards and procedures and identify opportunities for improvement.
- Contributes to the development and maintenance of information security policies, standards, procedures, and frameworks.
- Assists in the delivery of information security awareness and education, based on standards, trends and alerts from appropriate industry and security monitoring services.
- Maintains awareness of emerging cyber security trends/issues to provide contemporary and practical cyber security advice to key stakeholders.
- Contributes to the preparation of reports, briefing notes, and correspondence for internal and external stakeholders.
- Provides guidance and support to junior staff.

Corporate Responsibilities

- Exhibits accountability, professional integrity and respect consistent with DPC Values, the Code of Conduct, and the public sector Code of Ethics.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Work Health and Safety Act 2020
- Undertakes other duties as required.

Work Related Capabilities (Selection Criteria)

1. Experience in contributing to cyber security programs in enterprise IT environments, including cloud computing environments, using industry standard security

frameworks (for example: ASD Essential 8, ASD ISM, NIST Cyber Security Framework, the ISO/IEC 27000-series.)
2. Working experience in the identification, configuration, or management of ICT digital and information security risks, including cybersecurity and third-party vendor risks, relevant to complex enterprise environments including hybrid cloud.
3. Experience performing research, analysis, and review of complex cyber/technology problems, and developing evidence-based options, and recommended solutions to resolve problems and mitigate risks.
4. Well-developed communication skills, including written and oral communication, negotiation, influencing and interpersonal skills.
5. Experience working as part of multidisciplinary and cross functional teams and can understand the organisations objectives and align operational activities accordingly.

Desirable

- Possession of or progression towards a relevant tertiary qualification.
- Possession of relevant industry certifications for project management or IT Service Delivery (e.g. PRINCE2, PMP, Project+, ITIL Foundations) • Possession of relevant industry certifications for security (e.g. Security+, SC-200, SC300, CC, CISM, CRISC, CISSP).

To be eligible for permanent appointment to the role, employees must also be eligible to live and work in Australia indefinitely.

Employees engaged on fixed term appointments need a valid work visa for the duration of their contract. Appointment is also dependent on a 100-point identification check and Criminal Records Screening Clearance.

Principal Cyber Security Specialist, Level 6

Directorate:

Branch/Section:

Supervises: 0 FTE

About the Role and Responsibilities

Principal Cyber Security Specialists are responsible for contributing to the design, implementation and assurance of cyber security programs that protect information systems from cyber security threats. Principal Cyber security specialists will draw on broad experience in cyber security threats, governance or infrastructure/architecture security, and cyber security frameworks to support agencies in meeting the requirements of the WA Cyber Security Policy.

Cyber Security Tasks

- Designs, configures, or contributes to the implementation of cyber security controls for information systems and system components with a focus on Microsoft Cloud (Azure, Entra, Office 365, Defender) and hybrid cloud

environments. Examples include implementing security solutions, performing remediation activities, Essential 8 controls and system hardening.
- Performs security assessments, reviews and compliance testing to ensure adherence to information security policies, standards and procedures and identify opportunities for improvement.
- Contributes to the development and maintenance of information security policies, security guidelines and standards to support the WA Cyber Security Policy to address other emerging issues.
- Maintains awareness of emerging cyber security trends/issues to provide contemporary and practical cyber security advice to Government and agencies.
- Building and maintaining positive working relationships with WA Government agencies, as well as inter-jurisdictional and private sector partners.
- Contributes to the preparation of reports, briefing notes and correspondence for internal and external stakeholders.
- Provides guidance and support to junior staff.

Corporate Responsibilities

- Exhibits accountability, professional integrity and respect consistent with DPC Values, the Code of Conduct, and the public sector Code of Ethics.
- Takes reasonable care to protect your own safety and health at work, and that of others by co-operating with the safety and health policies and procedures of the Department and complying with all provisions of the Work Health and Safety Act 2020
- Undertakes other duties as required.

Work Related Capabilities (Selection Criteria)

1. Considerable experience in contributing to cyber security programs in enterprise IT environments, including cloud computing environments, using industry standard security frameworks (for example: ASD Essential 8, ASD ISM, NIST Cyber Security Framework, the ISO/IEC 27000-series.)

2. Practical experience in the implementation or administration of common enterprise security technologies, for example: End Point Detection and Response, SIEM systems, Endpoint Management, vulnerability scanners, patch management platforms and application allow-listing tools.

3. Experience performing research, analysis, and review of complex cyber/technology problems, and developing evidence-based options, and recommended solutions to resolve problems and mitigate risks.

4. Well-developed communication skills, including written and oral communication, negotiation, influencing and interpersonal skills to engage and build effective relationships with internal and external stakeholders.

5. Experience working as part of multidisciplinary and cross functional teams and can understand the organisations objectives and align operational activities accordingly.

Desirable

- Possession of or progression towards a relevant tertiary qualification.
- Possession of relevant industry certifications for project management or IT Service Delivery (e.g. PRINCE2, PMP, Project+, ITIL Foundations)
- Possession of relevant industry certifications for security (e.g. Security+, SC-200, SC300, CC, CISM, CRISC, CISSP).

To be eligible for permanent appointment to the role, employees must also be eligible to live and work in Australia indefinitely.

Employees engaged on fixed term appointments need a valid work visa for the duration of their contract. Appointment is also dependent on a 100-point identification check and Criminal Records Screening Clearance.