

OFFICIAL

Cyber Security Workforce Guide

Version 1.0



Government of
South Australia

Contents

1	Background	2
1.1	Purpose	2
2	Scope.....	2
3	SA Government cyber security services	3
3.1	Service delivery arrangements.....	3
3.2	Agency (local) security services/activities and capabilities.....	3
4	Functional structure and resourcing	5
4.1	Designing a functional structure	5
4.2	Resourcing options.....	7
4.3	Use of external service providers/contractors.....	8
5	Cyber workforce capability.....	8
5.1	Role definitions	8
5.2	Administrative Services Officer 1 (ASO1) to 2 (ASO2)	10
5.3	Administrative Services Officer 3 (ASO3) to 4 (ASO4)	11
5.4	Administrative Services Officer 5 (ASO5) to 6 (ASO6)	13
5.5	Administrative Services Officer 7 (ASO7) to 8 (ASO8)	16
5.6	Manager Administrative Services (MAS 1 to 3) to Senior Specialist/Senior Manager (SS/SM1 to 2)	19
5.7	SAES Specialist ICT (Category A and B) and SAES Level 1 to 2	23
6	Cyber workforce capability and capacity assessment	24
7	Education and training.....	26
8	Business case development.....	26
9	Additional references.....	27

1 Background

1.1 Purpose

The South Australian (SA) Government is committed to implementing robust measures to prevent, detect, and respond to cyber risks. A key enabler of this objective is the attraction and retention of a diverse, sustainable cyber security workforce that supports business agility and effective service delivery¹. A skilled and capable cyber workforce underpins the Government's capacity to protect its most critical information assets. Workforce diversity further enhances innovation, adaptability, and resilience, ensuring agencies are well positioned to meet their security obligations and respond effectively to an evolving digital and threat landscape.

This *Cyber Security Workforce Guide* supports the implementation of this strategic priority, the [South Australian Cyber Security Framework](#) (SACSF) and the [SA Government Cyber Security Operating Model](#). It addresses key challenges, risks and opportunities in cyber security workforce management across SA Government by:

- establishing a structured, scalable approach to developing and maintaining cyber security capability; and
- clarifying roles, expectations, and career pathways to support consistent workforce design and capability uplift across agencies.

This Guide also supports the Australian Government's strategic focus on developing sovereign capability by professionalising the national cyber security workforce².

2 Scope

This document covers:

- Services and activities that SA Government agencies are responsible for and must have resources and develop capabilities for.
- A baseline capability model that can be adapted and tailored by agencies to support operational requirements and constraints.
- Role definitions to promote efficiencies in role design and support an effective recruitment and selection process.
- Guidance on training and development to enable and maintain a skilled cyber workforce.
- An actionable step-by-step procedure to review an agency's workforce capacity and capability and create a business case for securing the right level of resources.

¹ Refer to Priority 3.1 of the [South Australian Cyber Security Strategy](#)

² Refer to [2023-2030 Australian Cyber Security Strategy](#)

3 SA Government cyber security services

3.1 Service delivery arrangements

The [SA Government Cyber Security Operating Model](#) defines arrangements for the provision of cyber security services to SA Government agencies. The service catalogue identifies the core³ and central⁴ services provided by the Office of the Chief information Officer (OCIO). It also identifies those that SA Government agencies are responsible for within their environment referred to as 'local services'.

Local services can be delivered under the following arrangements:

- **Stand-alone agencies:** Agencies of sufficient capability and capacity to deliver and manage their own local services.
- **Cluster agencies:** Large agencies with the capacity and capability (including sector understanding) to deliver local services to small agencies who have insufficient capacity.

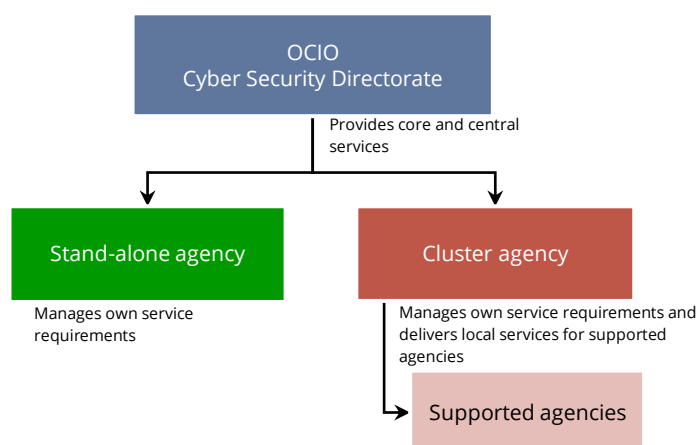


Figure 1. SA Government cyber security service delivery arrangements

3.2 Agency (local) security services/activities and capabilities

The [SA Government Cyber Security Operating Model](#) Cyber Security Service Catalogue groups agency responsibilities into the capabilities required to effectively deliver local services and activities.

Capability Area	Agency services and activities
1. Cyber security management	• Establish agency-specific cyber security strategy aligned to whole of government strategy • Establish cyber security governance practices aligned with whole of government cyber security governance structures • Attest to the agency's current state of alignment to the SACSf • Set, manage, maintain and communicate cyber security policy

³ sets the whole of government cyber strategy, statewide cyber security requirements, drives whole of government leadership and collaboration, and establishes overarching approaches and drives effectiveness in across-government cyber security risk management.

⁴ services that provide better efficiencies of scale, scope, or standardisation to provide more effective whole of government cyber security risk management

Capability Area	Agency services and activities
	• Implement a cyber security program • Identify, assess and implement change • Manage agency specific cyber security projects
2. Cyber risk management and assurance	• Develop and implement a risk management framework that includes cyber security risk management processes • Identify risk and include in agency risk register • Develop agency audit and assurance plan including scope and frequency of required activities • Perform self-assessment assurance review of the cyber security program at least annually • Engage independent reviews in line with agency requirements
3. Asset management	• Identify and record information assets, assign asset ownership, and periodically review information asset identification and classification • Document processes for labelling, storing, handling and disposing of assets
4. Incident management	• Develop incident response plans aligned to cyber security incident management policy and business continuity management plans • Lead incident response for single-agency incident, including public communications • Include cyber security requirements in continuity plans, and test service recovery plans
5. Identity	• Implement authentication requirements • Provision access to information assets based on business need • Undertake periodic review of access to information assets • Revoke access once there is no longer a specific need for it
6. Vulnerability management	• Receive, triage and action threat intelligence across agency technology environment • Undertake vulnerability scanning for internal facing assets • Undertake penetration testing of agency systems as required based on risk management activities • Remediate identified vulnerabilities
7. Supply chain security	• Identify and assess inherent cyber risks with procurement and develop mitigation plans • Undertake vendor due diligence with consideration to cyber

Capability Area	Agency services and activities
	risk and select vendor Undertake contractual monitoring for cyber obligations
8. Platform security	- Design software consistent with requirements - Undertake security functionality testing and vulnerability assessments - Build, deploy and test software in segregated environments - Execute configuration and hardening activities - Provide mobile device management solutions - Provision travel devices for international travel aligned to the risks of the destination country
9. Network security	Implement and operate network security services aligned with the minimum network security expectations
10. Security operations	Develop event logging and monitoring strategy and capability, and monitor for anomalous events
11. Personnel security	- Manage background checks - Provide ongoing awareness of personnel cyber security obligations
12. Physical security	Implement physical security measures to protect assets

Table 1. Agency (local) cyber security service catalogue

4 Functional structure and resourcing

4.1 Designing a functional structure

The design of a cyber security functional structure should consider strategic, tactical, and operational needs, support current and future requirements, and enable scalability. A poorly defined structure can undermine clarity of direction, authority, and accountability, reduce the effectiveness of service delivery, negatively impact workforce morale, and ultimately weaken the agency's security posture.

Agencies should consider the following to design a fit-for-purpose structure:

- The cyber security capabilities required to protect agency assets, support strategic objectives (such as operational growth, innovation, technological change, and organisational transformation), and meet current and emerging compliance obligations.
- The digital landscape, the industry-specific threats, and the capabilities required to face emerging threats and increased likelihood of events.
- The agency's current cyber security posture and the maturity of its business processes for managing cyber risk.

- The agency's defined risk appetite and broader risk management requirements.
- Collaborations with IT, HR, administration, legal, risk, and other business units to ensure clear accountability and effective assignment of security responsibilities (for example, personnel and physical security with HR, or platform security with ICT).

Figure 2 provides a baseline model for defining and organising cyber security roles and responsibilities, grouping the 12 key capabilities from the [SA Government Cyber Security Operating Model](#) listed above, to support effective delivery of agency's services and activities. The model is scalable and may be tailored to reflect agency-specific requirements.

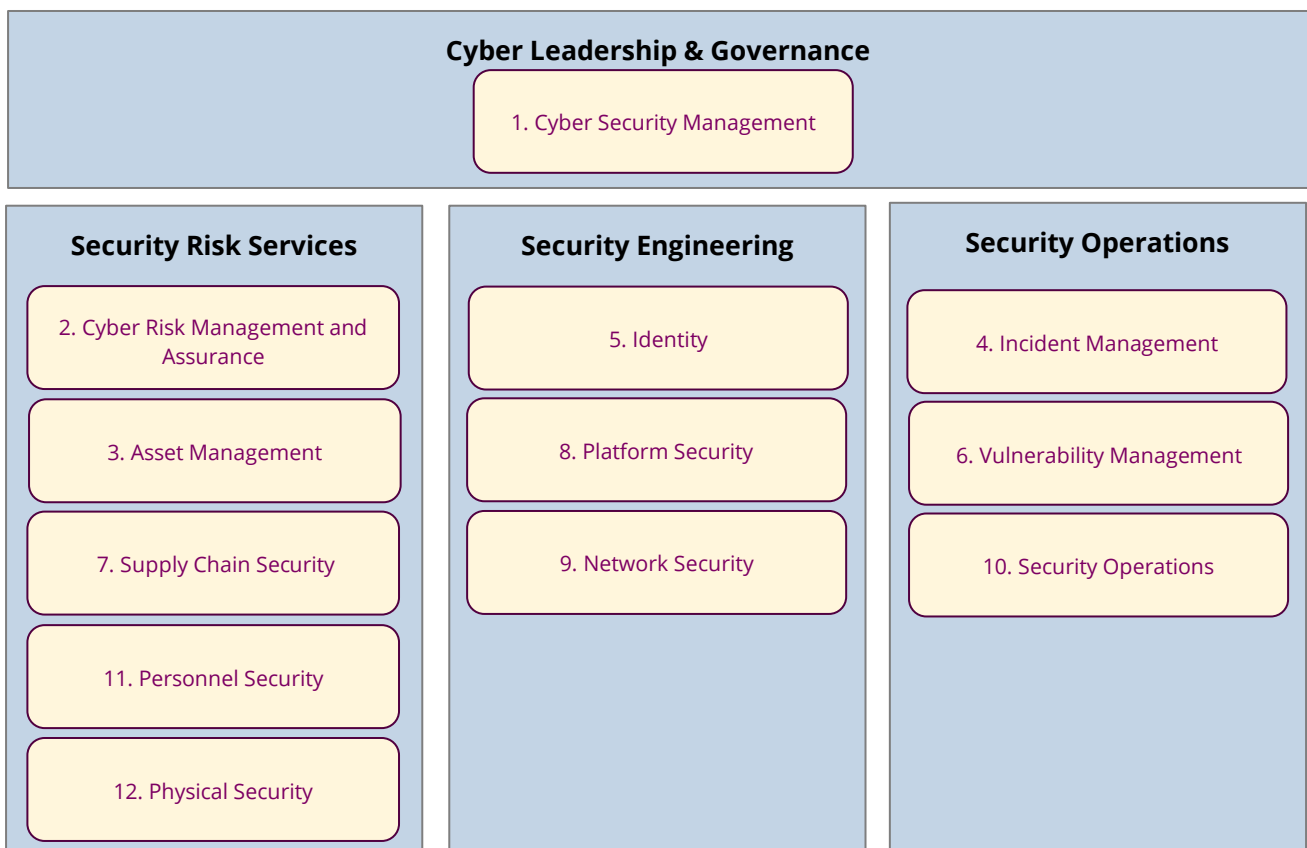


Figure 2. Cyber capability-based structure

- **Cyber Leadership and Governance** support the setting of strategic direction, oversight, and accountability framework for cyber security across the agency. This capability group ensures that cyber security is effectively governed, aligned with whole-of-government requirements, and integrated into organisational decision-making and risk management.
- **Security Risk Services** supports the establishment, operations, and assurance of the agency's cyber security risk management in alignment with agency and whole-of-government requirements.
- **Security Engineering** supports the design, implementation, testing, and assurance of technical security controls across agency platforms, networks, systems, and applications, ensuring security is embedded by design aligned with agency and business requirements.

- **Security Operations** supports the provision of operational insights into threat activity, trends, and control effectiveness to inform risk management and governance processes and the ongoing monitoring, detection, and operational response to cyber security events across the agency's technology environment.

Establishing and maintaining a functional structure based on this basic model supports consistency in role design, job evaluation and compensation creating transparency and fairness across government.

Security management should work with the HR team to apply workforce design principles to design a cyber security functional structure with the right level of capacity and capability for the agency. These principles include identifying and prioritising essential skills and expertise to meet the capability requirement, tiering to support career progression, and building flexibility to adapt to emerging threats and technologies.

4.2 Resourcing options

Agencies must assess their resourcing needs based on operational demands, maturity levels, and long-term sustainability. A strategic approach to resourcing means balancing internal expertise with external support to optimise efficiency, capability, and oversight. Not all cyber security activities require full-time internal staffing, especially where the activity requires specialist skills. Some skill sets are best utilised for short-term initiatives and in these cases, agencies should consider leveraging external expertise to enhance their security capabilities including:

- Collaborating with other agencies that have staff with relevant cyber security experience.
- Engaging service providers or contractors for specialised security capabilities.
- Hiring contractors or consultants for short-term, project-based engagements.

Although each agency may obtain cyber security services from other agencies and third parties, agencies remain accountable for the implementation of these services and activities and are required to:

- Ensure that the services and activities are in line with the cyber security program and supports the agency's strategy.
- Apply the cyber security risk appetite to meet the needs and expectations of stakeholders in alignment with organisational risk appetite.
- Understand cyber security risks and integrate oversight into management reporting.
- Obtain assurance that all agency security requirements are met by the resource(s) used, whether internal or external.

4.3 Use of external service providers/contractors⁵

When utilising external service providers, independent consultants or contractors for core cyber security operations, agencies should ensure:

- The services are clearly defined and cover scope, response times, reporting requirements and frequency of reporting.
- Resource competency requirements are clearly defined in the contract and evidence obtained, as necessary, for the activities being performed.
- Third party employees, consultants or contractors are onboarded according to standard agency processes and commensurate with the activities being performed. This includes:
 - Required background screening / security clearances based on the information that they are likely to access.
 - Agency induction (covering information security obligations, acceptable use etc.).
 - Site induction and work, health and safety (especially relating to secure zones, data centre access and lone working).
 - System access and identity management.
- There is an agency 'business owner' who is accountable for the activities performed and for the oversight of the third party's activities such as:
 - **Assessing performance.** Review service delivery against service level agreements (SLA) and key performance indicators (KPIs).
 - **Revalidating and assessing resources over time.** Conduct periodic reviews of capacity and capability requirements.
 - **Succession and knowledge management.** Ensure continuity if personnel change during the engagement.
- Third party employees, consultants or contractors are offboarded according to standard agency processes and commensurate to the activities being performed.

5 Cyber workforce capability

5.1 Role definitions

The following role definitions table complements the Stream Work Level Definitions and Characteristics from the [Commissioner of Public Sector Determination 5 Classification and Remuneration Attachment 2 - Classification Standards: Administrative Services Stream](#) and aims to:

⁵ Refer to Cyber.gov.au: [How to Manage Your Security When Engaging a Managed Service Provider \(October 2021\).pdf](#) for additional guidance.

- Establish a common framework for key cyber security roles across agencies promoting a shared language, enabling efficient secondments, career mobility, and lateral job changes within and between agencies.
- Strengthen recruitment processes by providing clearly defined roles and responsibilities, ensuring alignment with agency needs and facilitating efficient hiring decisions.
- Provide visibility to professional development pathways ensuring agencies can build and sustain a resilient cyber security workforce.

The table describes the following elements for each role grade and capability group:

- **Key Duties / Responsibilities** – Core duties associated with the role aligned with the agency services and activities described in [Section 3.2](#).
- **Technical Skills and Experience** – The level of capability and expertise required to perform the role effectively such as threat analysis, risk management, and incident response.
- **Attributes** – Key behavioural and interpersonal skills that support effective performance such as analytical thinking, problem-solving, adaptability, resilience, attention to detail, and communication.

These describe typical characteristics of the role grade and are not meant to be exhaustive. In developing a role description, the set of duties may incorporate duties from more than one cyber capability group. The duties in each of the role grade range may vary in terms of scope and complexity to differentiate one level (e.g. ASO1) to the other (e.g. ASO2).

5.2 Administrative Services Officer 1 (ASO1) to 2 (ASO2)

Roles at these levels operate at a **foundation level, focusing on awareness and supported delivery**. They emphasise task-based support, close supervision, and learning through guided participation in cyber security activities.

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
Key Duties / Responsibilities	- Support basic administrative and coordination activities that enable effective operation of security governance processes - Perform simple tasks to inform the development and review of policies, standard operating procedures, and relevant governance artefacts - Assist with simple cyber security initiatives or short-term tasks	- Support basic documentation and recording of cyber risks and evidence - Perform simple tasks to support information asset identification including updating registers - Assist with basic cyber risk-related activities in procurement, such as communicating routine security requirements - Support routine personnel and physical security tasks and awareness activities	- Assist with routine access-related tasks by following documented instructions and providing required information - Support application of basic technical security controls and operational activities under close supervision - Maintain records and documentation related to access and system security activities	- Assist with vulnerability tracking, documentation, and follow-up activities under supervision - Support incident response activities by recording information, escalating issues as directed, and following documented procedures - Support routine monitoring and administrative activities for security operations
Technical Skills and Experience	- Awareness or basic understanding of agency operations and governance concepts - Basic skills in research, information gathering, and use of standard templates, registers, and record keeping tools - Basic written and verbal communication skills and	- Awareness or basic understanding of agency operations, risk management and asset management concepts - Awareness or basic understanding of personnel and physical security obligations - Basic skills in information gathering, and use of	- Awareness or basic understanding of access management - Awareness or basic understanding of network fundamentals - Ability to follow instructions to support routine access and control activities	- Awareness or basic understanding of vulnerability management, incident response, and monitoring concepts and terminologies - Ability to maintain security incident, vulnerability, and monitoring information following established procedures

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	ability to maintain accurate records and documentation with attention to detail - Basic skills coordinating and organising project tasks	standard templates, registers, and record keeping tools - Basic written and verbal communication skills	- Ability to maintain accurate records related to access and system security tasks	- Ability to support simple routine monitoring and operational activities with accuracy and reliability
Attributes	- Willingness to learn, seek guidance, and apply feedback to build capability and confidence - Demonstrates reliability and a conscientious approach to completing assigned tasks - Demonstrates integrity, discretion, and respect for confidentiality and security requirements - Ability to communicate clearly and professionally in routine situations - Ability to work effectively as part of a team and contribute positively to a supervised work environment - Adaptability to change and resilience when working within structured processes and priorities			

5.3 Administrative Services Officer 3 (ASO3) to 4 (ASO4)

Roles at this level focus on **developing capability through supported practice**. They apply established cyber security policies, processes and tools in routine scenarios, contribute to governance and operational activities, and build skills under regular guidance and supervision.

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
Key Duties / Responsibilities	- Support cyber security program activities by maintaining documentation, collating metrics, and assisting with reporting and administrative tasks under direction - Assist with or contribute to policy, standards, and procedure development and maintenance	- Assist with identifying and recording cyber risks, maintaining registers, and supporting assurance and self-assessment activities - Identify and record information assets, support classification activities, and periodic reviews - Apply cyber risk considerations to	- Support access provisioning and documentation processes in line with defined identity and access requirements - Conduct routine access reviews and assist with issue identification and escalation - Assist with secure platform and application design, operations, and basic	- Conduct vulnerability scanning and basic analysis tracking remediation actions - Support monitoring activities and escalation of anomalous security events - Support detection and initial handling of cyber incidents recording incident information and following

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Assist with or contribute to delivery of cyber security initiatives and project activities under routine supervision	- procurement activities, supporting supplier assurance activities and documentation - Assist with personnel and physical security reviews, and awareness activities in routine scenarios	- validation activities under guidance - Assist with operational network security tasks and documentation	- documented response procedures - Assist with coordination, documentation, and post-incident review activities
Technical Skills and Experience	- Working knowledge of agency operations and agency cyber security governance structure and processes, and ability to apply them in routine scenarios - Experience supporting the development and review of standard operating procedures, and guidance materials - Demonstrated ability to perform research, information gathering, and maintain accurate documentation - Effective written and verbal communication skills, with the ability to analyse data and articulate insights - Experience assisting in the delivery of minor cyber	- Working knowledge of agency operations and agency cyber security risk management processes and ability to apply them in routine scenarios - Understanding of baseline security controls to mitigate common security risks - Experience supporting security risk assessments, information asset management, and assurance activities, or personnel and physical security activities - Ability to collect, analyse, and maintain evidence, documentation, and registers with minimal supervision - Effective written and verbal communication skills, with the ability to articulate risks	- Working knowledge of cyber security risks and controls relevant to security engineering - Understanding of agency access management policies, standards and procedures, and ability to apply them in routine scenarios - Experience supporting application of technical security controls and operational activities - Experience supporting secure platform and application design, operations, and validation activities - Demonstrated ability to maintain records related to access and system security tasks with accuracy and reliability	- Working knowledge of cyber security risks and controls relevant to agency security operations - Understanding of agency cyber security incident management, vulnerability management, and security monitoring requirements and procedures, and ability to apply them in routine scenarios - Experience following up vulnerability management activities - Experience supporting detection and handling of cyber incidents - Experience performing routine monitoring and administrative support for security operations activities - Demonstrated ability to maintain security incident,

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	security initiatives and project activities - Experience working in an administrative or support role, and completion of relevant coursework, training or study in cyber security, risk, project management, or a related discipline (desirable)	and issues and contribute to report development - Experience working in a risk and compliance role, and completion of relevant coursework, training or study in ICT, cyber security, risk, or a related discipline (desirable)	- Experience working in an entry level technical role, or completion of relevant coursework, training, or study in ICT, cyber security, or a related discipline (desirable).	vulnerability, and/or monitoring information with accuracy and reliability - Experience working in an entry level technical role, or completion of relevant coursework, training, or study in ICT, cyber security, or a related discipline (desirable)
Attributes	- Willingness to develop skills through feedback, learning, and supported practice - Demonstrates initiative and accountability in completing assigned tasks and responsibilities - Applies attention to detail and sound judgement in handling information and security matters - Demonstrates integrity, discretion, and compliance with security and confidentiality requirements - Communicates professionally and respectfully with internal stakeholders - Works collaboratively with colleagues and contributes constructively to team outcomes - Adapts to changing priorities and maintains resilience in a structured operational environment			

5.4 Administrative Services Officer 5 (ASO5) to 6 (ASO6)

Roles at this level operate as **independent practitioners**. They apply professional judgement to deliver cyber security activities of moderate complexity, contribute to policy and control development, coordinate assurance and operational activities, and provide advice within defined areas of responsibility.

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
Key Duties / Responsibilities	- Develop, maintain and implement significant agency cyber security policies, standards, procedures, and	- Undertake cyber risk assessments, support development of risk treatments, contribute to	- Implement and review identity and access management controls, including access	- Analyse significant vulnerability and threat information, prioritise findings using risk-based

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	associated plans and programs - Undertake significant governance activities requiring the use of analytical skills, preparation and presentation of output or provision of guidance or advice pertaining to security to various stakeholders - Control and co-ordinate projects and work programs across teams within the agency and/or to external agencies to deliver security outcomes under limited direction	assurance activities, and provide sound advice and recommendations to mitigate security risk - Facilitate classification of information assets supporting critical processes, advise asset owners on obligations, and integrate asset information into cyber risk management activities - Undertake supplier cyber risk assessments and due diligence, support security activities in procurement and contract management activities and provide ongoing assurance - Provide sound advice on personnel and physical security, undertake assessments and exemption reviews and deliver targeted awareness activities under limited direction	provisioning, periodic reviews and issue resolution of significant systems and applications - Support secure configuration, operation and assurance of platforms and applications, including documentation and validation activities - Implement network security controls and support operational assurance and remediation activities - Analyse technical security issues and provide informed advice within the defined technical domains	approaches, and coordinate remediation activities track progress and escalate overdue or high-risk items - Develop and maintain security monitoring use cases and detection content (e.g., SIEM queries/rules, EDR alerts), including tuning to reduce false positives and improve coverage - Monitor security events and logs, investigate anomalous activity, and prepare operational reporting (e.g., incident trends, alert volumes, response performance, vulnerability status) - Perform incident triage, assessment and classification, coordinate response activities across ICT and business stakeholders in line with incident response plans and escalation pathways - Conduct investigation activities to confirm impact and scope (e.g., log analysis, endpoint artefacts), and recommend containment,

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
				eradication and recovery actions - Lead post-incident reviews, lessons learned and continuous improvement activities
Technical Skills and Experience	- Significant knowledge of agency cyber security governance structure and processes and how it applies to agency environment - Experience supporting cyber security program activities including developing and maintaining artefacts, collating metrics, and reporting - Experience contributing to the development and maintenance of cyber security policies, procedures, and guidance materials - Experience assisting in the delivery of cyber security initiatives and project activities - Ability to analyse information, exercise professional judgement, and provide informed advice within defined areas of responsibility	- Significant knowledge of agency risk management policies, standards and procedures, and how it applies to agency's security environment - Sound knowledge of cyber security frameworks, standards, and controls, and their application within government context - Experience identifying and recording cyber risks, maintaining registers, and supporting assurance and self-assessment activities - Experience identifying and recording information assets, supporting classification activities, and periodic reviews - Demonstrated ability identifying and communicating cyber risk considerations for procurement activities and	- Significant security engineering knowledge and competence gained through experience, training or education - Experience in access provisioning and documentation processes in line with defined identity and access requirements - Experience conducting access reviews and assisting with issue identification and escalation - Experience in secure platform and application design, operations, and validation activities in accordance with applicable security standards - Demonstrated ability performing operational network security tasks - Ability to analyse information, exercise professional judgement, and	- Significant security operations knowledge and competence gained through experience, training or education - Experience conducting vulnerability scanning and analysis and tracking remediation actions - Experience supporting monitoring activities and escalation of anomalous security events - Experience detecting and handling cyber incidents, and recording incident information following defined procedures - Demonstrated ability coordinating, documenting, and assisting with post-incident review activities - Ability to analyse information, exercise professional judgement, and

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Strong written and verbal communication skills, including preparation of reports, briefings, and guidance materials	- supporting supplier assurance activities - Experience in personnel and physical security reviews and delivery of security awareness activities - Ability to analyse information, exercise professional judgement, and provide informed advice within defined areas of responsibility	- provide informed advice within defined areas of responsibility	- provide informed advice within defined areas of responsibility
Attributes	- Demonstrates professional judgement, accountability, and reliability in delivering outcomes - Proactively identifies issues and contributes to continuous improvement - Balances attention to detail with an understanding of broader business and risk context - Works effectively both independently and as part of a multidisciplinary team - Communicates confidently and constructively with stakeholders at various levels - Demonstrates integrity, ethical behaviour, and commitment to public sector values - Remains adaptable and composed when managing competing priorities or emerging risks			

5.5 Administrative Services Officer 7 (ASO7) to 8 (ASO8)

Roles at this level provide **senior technical and professional leadership**. They lead complex cyber security activities, oversee governance, risk and operational outcomes, influence strategic decisions, and provide authoritative advice to senior stakeholders across the agency.

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
Key Duties / Responsibilities	- Lead the development, implementation and	- Lead agency cyber risk management and assurance	- Lead security architectures, standards, and roadmaps	- Establish a vulnerability management strategy and

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	continuous improvement of agency cyber security policies, standards, procedures and plans, ensuring alignment with agency and whole of government strategic direction - Provide advice on significant security-related policy matter - Manage cyber security governance processes, including performance metrics setting, evidence management, monitoring of decisions and actions and executive reporting - Manage delivery and prioritisation of cyber security initiatives and programs, providing authoritative advice to senior stakeholders on matters of high complexity and risk - Evaluate the results of cyber program activities against stated objectives	activities, including provision of expert advice ensuring risks are identified, assessed, treated and reported in line with established frameworks and risk appetite - Manage information asset management practices, including identification of critical and high-risk assets, ownership accountability, and integration with cyber risk and assurance activities - Lead supply chain cyber security risk management, embedding security requirements into procurement and contract management processes and overseeing assurance and remediation of high-risk suppliers - Oversee personnel and physical security controls relevant to cyber risk, ensuring compliance, effectiveness and targeted uplift where required	development and implementation, ensuring alignment with agency objectives and whole-of government requirements - Lead identity and access management governance and control effectiveness, ensuring alignment with policy, risk appetite and minimum authentication requirements - Lead secure platform and application security practices, including assurance of secure configuration, resilience and alignment with business impact and risk assessments - Oversee network security capability, performance and assurance outcomes across the agency	lead vulnerability scanning, penetration testing, and assurance activities translating them into actionable risk treatment and control improvement activities - Establish and implement a comprehensive logging and monitoring strategy and lead security monitoring operations, ensuring effective alerting, triage, escalation, and investigation - Establish and enforce operational standards, procedures, and controls to ensure security operations are delivered consistently, efficiently, and in alignment with agency and whole-of-government requirements - Lead threat hunting and threat intelligence activities in collaboration with central cyber and intelligence functions to anticipate and mitigate emerging threats - Lead the development, testing, and continuous improvement of incident response plans and procedures aligned to

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
				organisational resilience and business continuity requirements - Manage the identification, triage, investigation, and coordinated response to cyber security incidents, ensuring timely containment, remediation, and recovery
Technical Skills and Experience	- Advanced knowledge of cyber security governance, including alignment to agency and whole-of-government policies and frameworks - Significant experience developing, maintaining and implementing agency cyber security policies, standards, procedures, and plans and programs - Highly developed verbal and written communication skills, including executive-level briefings and reports - Demonstrated experience leading complex cyber security activities, initiatives, or capability uplift programs	- Advanced knowledge of cyber security risk management practices including alignment to agency and whole-of-government policies and frameworks - Demonstrated ability to provide authoritative advice on cyber risk, control effectiveness, and security posture to senior stakeholders - Significant experience managing various assurance activities, reporting and monitoring to senior stakeholders - Experience integrating cyber security considerations into broader business, technology, and risk contexts	- Advanced knowledge of security engineering principles and practices, including identity and access management (IAM), platform and application security, and network security, aligned to agency and whole-of-government policies, standards, and risk appetite - Demonstrated ability to provide authoritative advice to senior stakeholders on secure identity, access management, platform and application architecture, network security design, and control effectiveness in complex environments - Strong ability to analyse complex technical security issues, exercise professional	- Advanced knowledge of security operations concepts and tooling, including SIEM/SOAR, EDR/NDR, log pipeline design, alert tuning, and use of MITRE ATT&CK, threat intelligence, and detection engineering practices - Demonstrated ability to provide authoritative advice on incident response performance, vulnerability and exposure risk, and security monitoring effectiveness - Significant experience leading security operations functions and coordinating cross-agency stakeholders and providers to manage incidents, contain threats, and drive remediation of

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Tertiary qualifications in a relevant discipline and/or professional certifications (desirable) in cyber security (e.g. ISO 27001, CISM, CISA)	- Tertiary qualifications in a relevant discipline and/or professional certifications (desirable) in cyber security, risk, or assurance (e.g. ISO 27001, CRISC, CISSP, risk or audit related certifications)	- judgement, and drive improvement of security engineering controls, standards, and practices across the agency - Tertiary qualifications and/or relevant professional certifications (desirable), such as identity and access management, cloud security, network security, or application security certifications	- vulnerabilities (including third-party and shared services dependencies) - Tertiary qualifications and/or relevant professional certifications (desirable), such as incident response (e.g., GCIH/GCFA), threat intelligence (e.g., GCTI), SOC/SIEM engineering, vulnerability management
Attributes	- Demonstrates leadership, accountability, and sound decision-making under pressure - Takes ownership of outcomes and drives continuous improvement and capability uplift - Strong capability in stakeholder engagement, influencing decisions, and managing competing priorities. - Builds trust and credibility with senior stakeholders through expertise and professionalism - Leads collaboratively and supports the development of others - Maintains strategic focus while managing operational and delivery considerations - Demonstrates integrity, resilience, and commitment to effective public sector governance			

5.6 Manager Administrative Services (MAS 1 to 3) to Senior Specialist/Senior Manager (SS/SM1 to 2)

Roles at this level have **enterprise accountability for cyber security outcomes**. They set strategic direction, define risk appetite, establish governance and assurance frameworks, and provide executive leadership and assurance to agency executives, central governance bodies and government.

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
Key Duties / Responsibilities	- Provide oversight through establishment and stewardship of agency cyber security governance arrangements, including security committees, reporting frameworks, and escalation pathways to senior leadership and whole-of-government forums - Set and maintain cyber security strategy by defining objectives, risk appetite, priorities and performance measures, and ensuring continual improvement - Oversee cyber security program delivery, including approval, prioritisation and resourcing of cyber initiatives and projects based on risk, and monitoring progress, outcomes and benefits realisation - Approve and oversee policy, capability and operating model design ensuring cyber security roles, responsibilities, structures and competencies are defined and implemented	- Ensure effective cyber risk management ensuring including cyber risk management capability development, risk appetite implementation, and risk assurance and reporting - Provide executive assurance to agency leadership, central governance bodies and government on cyber security posture, capability maturity and risk exposure - Ensure enterprise information asset governance to support effective security risk management - Set strategic direction for supply chain cyber security, ensuring assurance over third-party risk exposure and remediation of systemic risks - Set strategic direction for personnel and physical security controls relevant to cyber risk and assures workforce capability, compliance and uplift - Provide executive assurance and attestation on the	- Set strategic direction for security architectures, standards and roadmaps that balance risk, cost, and business outcomes - Oversee the definition and adoption of enterprise security reference architectures, standards and patterns (including Zero Trust) - Accountable for enterprise platform and application security posture, ensuring environments are securely designed, configured, operated, and resilient in line with business impact assessments and availability requirements - Oversee effective identity and access management (IAM) activities including policy, assurance, exception management, and alignment with applicable requirements - Establish governance for secure-by-design delivery: design reviews, risk decisions, assurance and exception management	- Establish and govern the agency's security operations capability, including incident management, security monitoring, and vulnerability management, aligned to SACSf, SAPSF and whole-of-government requirements - Provide oversight and accountability for the identification, triage, investigation, and coordinated response to cyber security incidents, including executive decision support during high-impact events - Act as the primary escalation authority for significant cyber security incidents and operational security matters, engaging senior executives, central agencies, and external stakeholders as required - Oversee the performance, assurance, and continuous improvement of security operations services, including internal teams, shared services, and third-party providers

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Engage externally and across government, representing the agency in whole-of-government cyber security forums, and ensuring alignment with central policy, standards and reporting requirements - Own and attest to the agency's alignment to the SACSf and other compliance obligations, providing leadership accountability for compliance and reporting	agency's alignment to SACSf and other compliance obligations including endorsement of self-assessments, independent reviews, driving remediation and maturity uplift activities and monitoring risk outcomes	- Provide strategic oversight and assurance of network security capability, resilience and investment priorities	- Integrate security operations outcomes into enterprise risk management, governance, assurance, and reporting, providing clear visibility of operational risk, trends, and control effectiveness
Technical Skills and Experience	- Demonstrated experience setting and implementing strategic direction at business or enterprise level to achieve security objectives - Proven ability to establish and sustain governance frameworks and accountability structures and mechanisms - Proven track record building teams, developing capability, and establishing sustainable operating models, governance and delivery pipelines	- Strong understanding of the interaction between cyber risk, business strategy, investment, and transformation - Extensive knowledge of risk management strategy and proven ability to establish, operate and continually improve security risk management processes at an enterprise and whole-of-government level - Significant experience leading an assurance function and providing executive assurance to agency leadership, central	- Significant experience leading security engineering functions, including governance and assurance of IAM controls, secure configuration of platforms and applications, and oversight of network security capability, performance, and remediation activities - Experience overseeing secure-by-design practices, including architecture and design reviews, risk-based security decisions, assurance activities, and exception management	- Strong understanding of risk-based vulnerability and exposure management, including prioritisation, remediation oversight, and assurance reporting - Demonstrated experience establishing, governing, and assuring security operations functions and integrating security operations outcomes into enterprise risk management, governance, assurance, and reporting frameworks - Proven ability to provide authoritative advice to executives on cyber threats, incident impact, control

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Demonstrated capability leading large-scale programs, influencing system-wide outcomes, and managing complex stakeholder environments - Experience operating in a South Australian Government or comparable environment, including familiarity with agency and whole-of-government governance arrangements - Experience contributing to whole of government initiatives, cross agency programs, or sector wide cyber security uplift activities - Tertiary qualifications in a relevant discipline and/or executive-level credentials in cyber security, risk, governance or leadership (desirable)	- governance bodies, and government - Experience operating in a South Australian Government or comparable environment, including familiarity with agency and whole-of-government risk management processes - Tertiary qualifications in a relevant discipline and/or executive-level credentials in cyber security, risk, governance or leadership (desirable)	- Demonstrated oversight of network security capability, performance, remediation activities, and assurance outcomes - Experience integrating security engineering outcomes into enterprise risk management, governance, assurance, and investment decision-making processes - Tertiary qualifications in a relevant discipline and/or executive-level credentials in ICT, cyber security, risk, governance or leadership (desirable)	- effectiveness, and operational risk exposure - Experience overseeing security monitoring and detection capabilities, including logging strategies, alerting, escalation, investigation, and continuous improvement of detection effectiveness - Demonstrated leadership in managing cyber security incidents, including executive decision support, coordination across internal and external stakeholders, and post-incident assurance and remediation - Tertiary qualifications in a relevant discipline and/or executive-level credentials in ICT, cyber security, risk, governance or leadership (desirable)
Attributes	- Demonstrates leadership and enterprise accountability for outcomes, decisions and risk - Strategic thinking and influence on senior stakeholders to align priorities, investment and delivery with risk appetite - Highly developed communication skills, demonstrating authority and clarity in executive, board and ministerial contexts - Ability to build and sustain trusted relationships across the agency and whole-of-government, negotiating outcomes in complex stakeholder environments - Leads through ambiguity and crisis, remaining composed under pressure and enabling coordinated executive decision-making			

	Cyber Governance and Leadership	Security Risk Services	Security Engineering	Security Operations
	- Ability to drive culture change and capability uplift by empowering leaders, setting expectations and holding the organisation to account - Demonstrates integrity, ethical judgement and commitment to public sector values, governance and transparency			

5.7 SAES Specialist ICT (Category A and B) and SAES Level 1 to 2

Refer to the [South Australian Executive Service \(SAES\) Competency Framework](#) or the agency HR Team.

6 Cyber workforce capability and capacity assessment

The [Appendix A - Cyber Workforce Assessment Tool](#) assists agencies with assessing their capability and capacity to deliver agency responsibilities (as outlined in [Section 3.2](#)) and identify improvements.

Step	Action
Assess capacity and identify gaps	Use the Capacity Assessment tab for this activity. The worksheet provides the services/activities under each of the 12 cyber security capability domains. Treat the services/activities listed as a baseline. Some might not be relevant (e.g. software development) while some may need to be added (e.g. service management) depending on the agency ICT environment. 1. Determine whether each cyber security service or activity is being performed according to required frequencies in policies, procedures, or standards (e.g., SACSF). 2. Identify which roles or teams currently perform the work. Consider existing resources across the agency that may already have responsibility for the activity such as: • Human resources • Project management office • Procurement • Corporate risk and audit • Communications and engagement • Records and information management • IT operations • IT service desk • Facilities and security. Engage with key stakeholders in these areas to confirm their current responsibilities and understanding of expectations, establish a shared agreement to clarify ownership, and prevent duplication of effort. 3. Identify the risks arising from misalignment such as unmet demand for security services, gaps in process or security controls, duplication of effort, and other constraints that could significantly impact the delivery of the service/activity. 4. Identify if there are resourcing uplifts that have been planned and budgeted and expected to fill known gaps.
Assess capability and identify gaps	Use the Capability Assessment tab for this activity. The worksheet provides the recommended cyber security role/capability level for the key responsibilities under each of the 12 cyber security capability domains. The recommended

Step	Action
	capability reflects the complexity of the task consistent with the role definitions in Section 5.1. 1. For each of the key responsibilities under each service/activity, identify the personnel currently assigned to perform it. Include activities performed by other business units, agencies or third parties consistent with what was determined in the Capacity Assessment tab. 2. Identify mismatches and highlight the following: • Junior personnel taking on responsibilities typically assigned to more experienced staff. • Highly qualified individuals performing tasks that could be delegated to others. • Gaps in assigned activities. 3. Identify the risks arising from misalignment such as inefficiencies, missing competencies and constraints that could significantly impact the performance of the service/activity.
Identify needs	1. Both sections of the template include a column to identify any existing projects or initiatives that may already have been approved (with budget allocated) but have yet to be implemented. Provide information on these projects and initiatives. 2. For any additional capacity or capability gaps identified, identify the action proposed to close the gap. Increasing capacity to deliver the services/activities may include: • identifying available internal resources that could support unmet or unclear requirements • seeking collaboration and support from an internal team or cluster agency • developing a business case for additional role(s) or temporary resource (refer to Section 4.2 for guidance on resourcing options) Uplifting capability to effectively perform the services/activities may include: • providing training or upskilling personnel to meet the requirements of the role (refer to Section 7 for guidance on education and training and the agency's personal development plan process)

Step	Action
	- identifying responsibilities that can be delegated to the right level - developing a business case for the reclassification of role(s), restructuring the team or hiring additional resources.

7 Education and training

Cyber security professionals are expected to regularly update their skills and knowledge through ongoing education and training, ensuring alignment with their roles, responsibilities, and the evolving cyber threat landscape. Agencies should support a culture of continuous improvement and resilience in cyber security capability by proactively identifying and promoting education pathways and supporting staff access to professional development that is most relevant to their current and future needs.

Performing a skills assessment to map the team's current competencies against the role descriptions and any future requirements provide a starting point and assists with identifying skills gaps. By creating a personnel or team development plan from the assessment, the agency can:

- Align team skills development with personal development plans and career goals.
- Identify knowledge silos and implement knowledge-sharing or mentorship programs within the team, agency or across government.
- Transition team members into different roles when needed, improving overall resilience.
- Determine whether permanent hires, contract roles, or managed services offer the most efficient and sustainable solution for addressing the skills or capability gap.

8 Business case development

The ability to uplift an agency's cyber security capability is constrained without securing the right level of investment in its workforce. Defining the services/activities that the team needs to fulfill and providing clear expectations of each role establishes a defined benchmark that supports a strong business case for required resources and training.

To build a cyber security business case, agencies must start by understanding their delivery capacity and capability to implement and sustain a cyber security uplift alongside other organisational priorities. This means assessing not just what resources are available, but how those resources are being utilised across existing BAU operations, transformation programs, and compliance initiatives. With this baseline perspective, decision-makers can identify areas that require investment in skills, services, or technology to prevent failures in delivery or the risk of burnout.

The business case should highlight:

- The cyber security program and its feasibility given the current capacity and capability levels.
- The current state of resourcing and risk associated with it.
- The various resourcing options and the pros and cons of each.
- The recommended course of action.

[Appendix B: Cyber Workforce Resourcing - Business Case Template](#) has been developed to assist agencies with this activity. Agencies should consult with their project management office for additional advice and guidance to provide a successful justification for resourcing uplifts.

9 Additional references

- [Australian Signals Directorate Cyber Skills Framework v2.0](#)
- [Australian Cyber Workforce Playbook v.10](#)
- [SFIA - A Framework for Cyber Security Skills](#)

Document Control

Approved by	CIO Steering Committee	Version	1.0
Approved date	24 September 2026	Next review date	September 2028
Original date of approval	24 September 2026	Compliance	Optional
Contact person	Cyber Strategy, Policy and Engagement - Cyber Security Directorate Office of the Chief Information Officer		
Contact email	cybersecurity@sa.gov.au		

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite the Office of the Chief Information Officer, Department of Treasury and Finance, Government of South Australia, 2026.