

OFFICIAL

South Australian Government Cyber Security Operating Model



Government of
South Australia

Contents

1. Introduction	3
1.1 Background	3
1.2 Purpose	3
1.3 Authority.....	4
1.4 Applicability	4
2. The Operating Model Components	4
2.1 Architecture.....	4
Operating Model Architecture.....	6
2.2 Design Principles	7
2.3 Design Principles Decision Tree	8
2.4 Commercial and Operational Principles	9
2.5 Cyber Security Taxonomy	10
3. Implementation	11
3.1 Governance	11
3.2 Cyber Security Service Catalogue.....	11
3.3 Cyber Security Taxonomy and RACI	11
Appendix A: Cyber Security Service Catalogue	13
Appendix B: Operating Model RACI	17
Aboriginal Impact Statement	26
Document Approval and Control.....	27

SA Government Cyber Security Operating Model

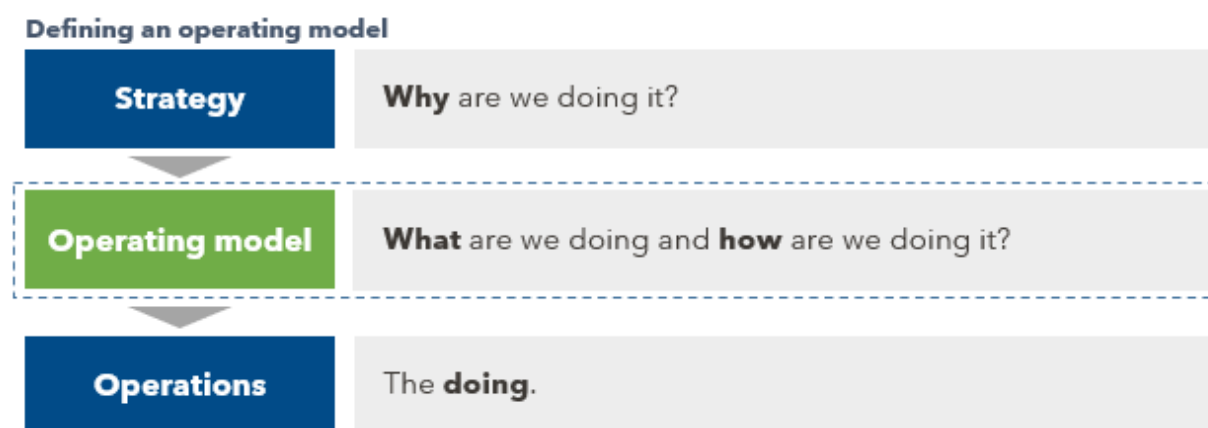
1. Introduction

1.1 Background

Governments worldwide are grappling with the escalating threat of cyber incidents as they attempt to navigate the increasingly complex landscape of digital vulnerabilities. Recent incidents in Australia have demonstrated the significant impact of inadequate cyber security and the South Australian (SA) Government is committed to ensuring appropriate measures are in place to protect against and respond to cyber risks.

The SA Government has developed (and continues to develop), a range of strategies (including framework and policy considerations) to inform the requirements and guidance for agencies and third parties to prevent, detect and respond to cyber threats. These strategies are operationalised through definition of the SA Government Cyber Security Operating Model (the Operating Model) - the people, processes and systems that work together to deliver strategy.

In simple terms the operating model provides the bridge between strategy and the day-to-day operations:



1.2 Purpose

The Operating Model provides clarity about the services, processes and activities that need to be undertaken to properly manage cyber security risk across government, as well as clearly defining the roles and responsibilities across the Office of the Chief Information Officer (OCIO) and agencies.

It introduces a standardised cyber security taxonomy, aligned to the SA Government Cyber Security Framework (SACSF) that describes what comprises cyber security services across government and assists agencies to apply that within their domain.

The Operating Model will reduce duplication of effort and create opportunities of scale through the clear definition of centralised services, as well as improving consistency and efficiency through standardised approaches.

It also creates opportunities for greater allocation of resources to areas of highest risk through the identification of information assets of state significance.

1.3 Authority

The Operating Model is a Cabinet approved document. The Premier and Cabinet Circular [PC004 ICT Digital and Cyber Security Requirements](#) outlines the authority for OCIO to provide whole of government ICT, digital and cyber security services, and the requirement for agencies to consume services from the OCIO Service Catalogue before considering standalone solutions.

1.4 Applicability

The SA Government Cyber Security Operating Model applies to:

- South Australian Government public sector agencies (agencies), that is, administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown. Refer: [Public Sector Act 2009](#).

2. The Operating Model Components

The Operating Model comprises of seven main components. These are:

- Operating Model architecture
- Design principles
- Design principles decision tree
- Commercial principles
- Cyber security taxonomy
- Cyber Security Service Catalogue
- RACI.

2.1 Architecture

The Operating Model architecture provides clear definitions of the roles and clarity in the delineation of responsibilities. The key architecture elements are:

OCIO Core – 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.

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

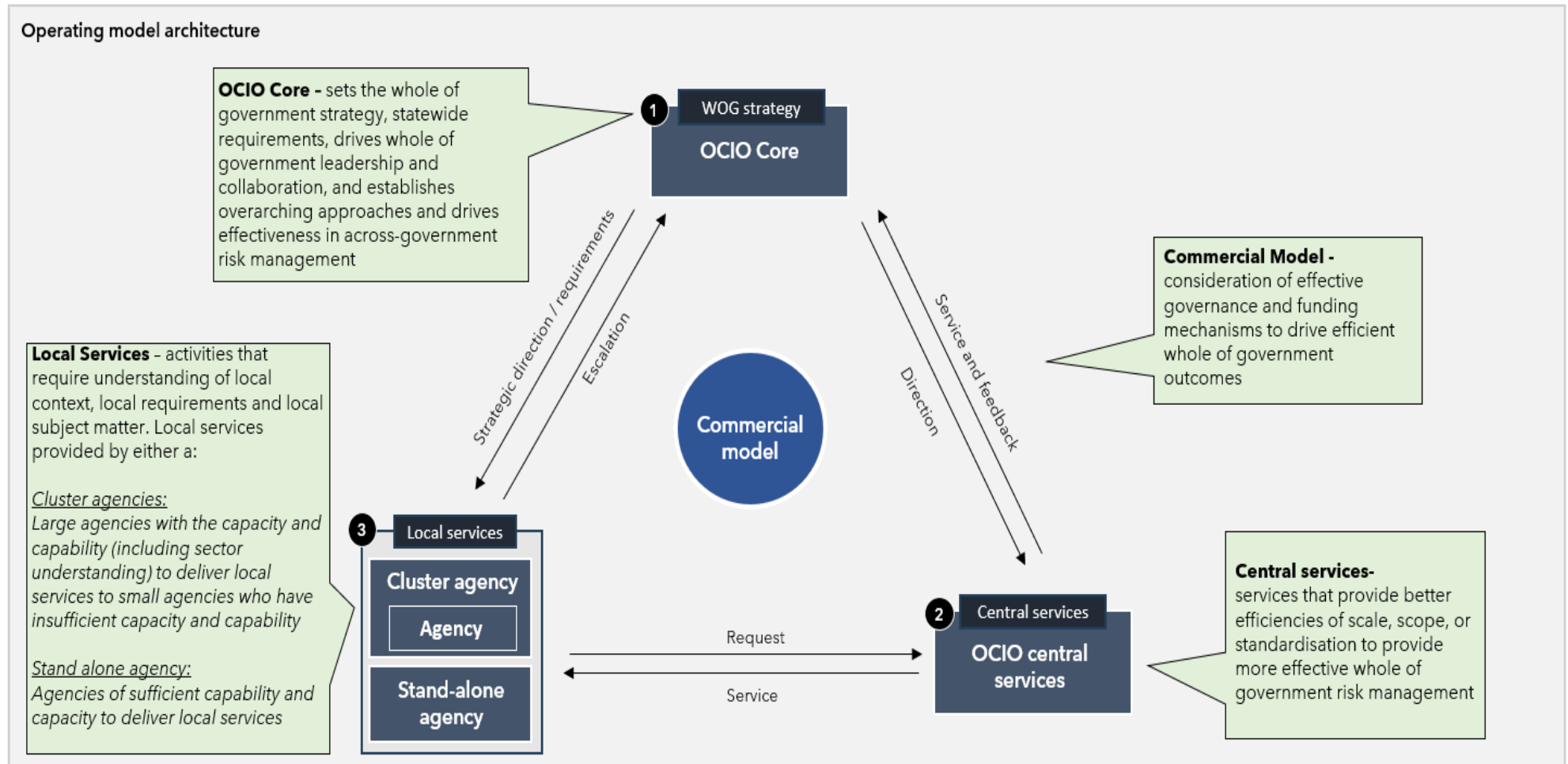
Local Services – activities that require understanding of local context, local requirements and local subject matter. Local services are provided by either:

Cluster agencies: Large agencies with the capacity and capability (including sector understanding) to deliver local services to small agencies who have insufficient capacity and capability.

Standalone agency: Agencies of sufficient capability and capacity to deliver local services.

Operating Model Architecture

This diagram shows the relationship between the Operating Model roles, describes the responsibilities of each role and demonstrates the intersection of cyber security strategy, operating model and cyber security operations between OCIO and agencies.



2.2 Design Principles

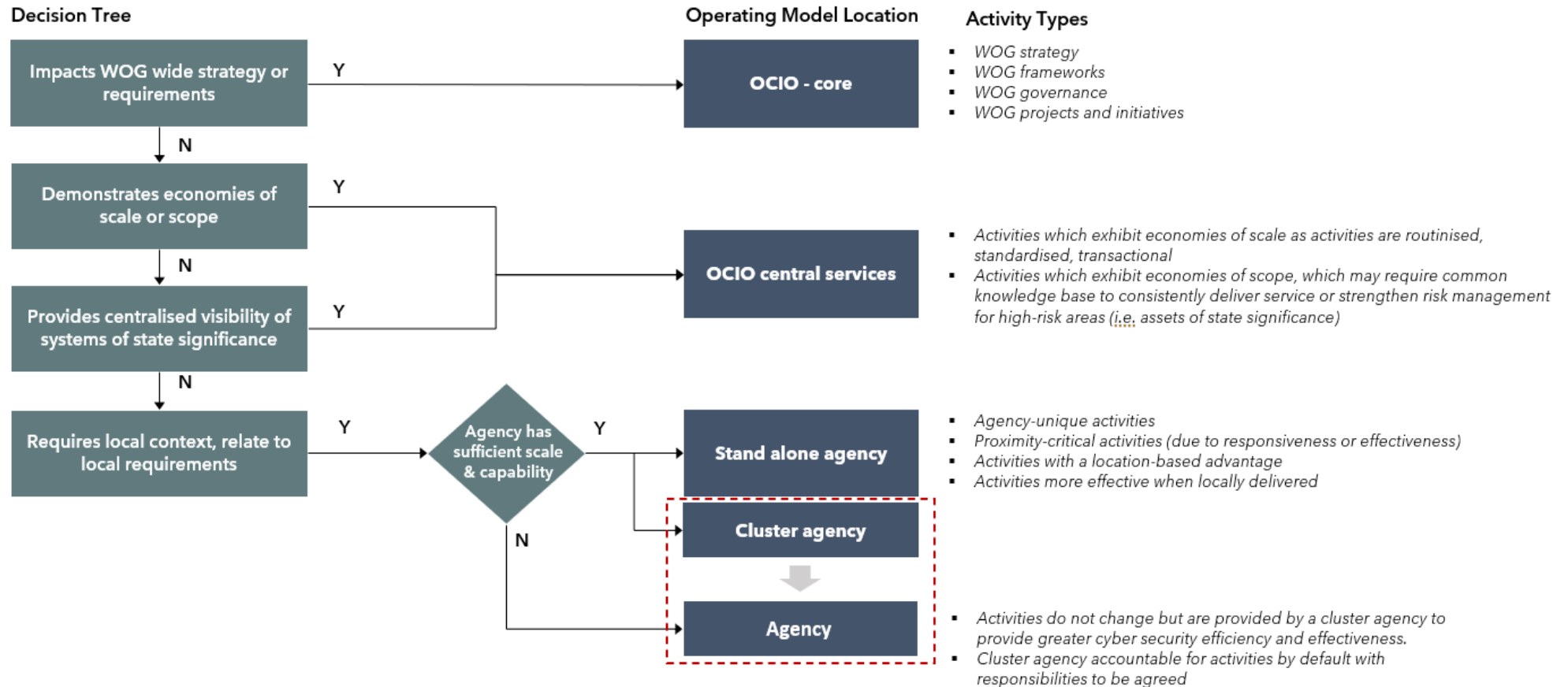
The design principles are aligned to the Operating Model architecture and provide additional context about the operational implications relating to the delineation of responsibilities.

Allocation principles

Principle	Operational implications	What this means...
OCIO Core defines key strategic considerations that impact WOG including strategy, requirements, governance and major investment	Allocation of activities related to whole of government strategy, establishing statewide requirements, driving whole of government leadership and collaboration, and establishing overarching operational or investment approaches	<i>Clarity and consistency of direction and requirements</i>
Common activities and services are performed centrally or standardised at scale	- Common activity that doesn't require local contextual / subject matter knowledge is consolidated and delivered from a single location. - Reduced duplication of activity between OCIO or across agencies.	<i>Avoided duplication of common activity</i>
Activities that strengthen WOG risk management relating to systems of state significance are managed centrally	Systems of greatest state significance (e.g. critical assets or public facing assets) are identified and are provided with proportionate attention.	<i>Greater visibility of critical assets</i>
Activities that require local context, or relate to local requirements, or require sector-related subject matter are provided locally	- Agencies continue to provide relevant local cyber security services to their agencies. - Agencies with insufficient capability or capacity are provided with context-relevant service by cluster agencies	<i>Agencies are provided the appropriate level of relevant support locally aligned to their requirements</i>

2.3 Design Principles Decision Tree

The design principles decision tree is used to determine cyber security service role location.



2.4 Commercial and Operational Principles

The Operating Model commercial and operational principles drive whole of government cost efficiencies associated with managing cyber security.

Indicative investment principles

Centralised strategy and coordination for material investment	Where investment is material, has multi-agency benefits, or impacts an agency outside the local agency, centralised governance is considered. The Digital Investment Fund is currently providing a mechanism to enable this for new funding requests.
Portfolio management is considered to effectively manage	New cyber investment needs effective portfolio management to enable effective delivery of initiatives. This includes effective management of dependencies, strong governance, and identification of opportunities to enhance whole-of-government benefits.
Effective collaboration	For material investment or investment that impacts multiple agencies, strong collaboration is incorporated into design so that solutions are relevant and enhance multi-agency benefits.

Indicative operational principles

Centralised or standardised services are used by default where available	Where provided, centralised or standardised services are used by default. Exceptions are managed by local leadership for each agency.
Funding of ongoing operational costs is considered	Where new central services capability is created, ongoing operational costs need to be considered at a whole of government level.
A streamlined service delivery model for central services is defined and communicated	Central services should define a streamlined service delivery model to increase services uptake and enhance efficient delivery of services.

2.5 Cyber Security Taxonomy

The Operating Model cyber security taxonomy is organised into 14 key domains and associated activities. It describes what comprises cyber security services across SA Government and is aligned to the SACSF.

High level summary of key activities

1. Provide leadership, set requirements and policy, and determine roles	2. Identify, assess and manage cyber security risks	3. Perform audit and assurance	4. Manage Information Asset Identification and Classification	5. Manage incidents	6. Maintain resilience and service continuity	7. Manage access to information
1.1 Establish cyber security vision and strategy 1.2 Manage cyber security frameworks and requirements 1.3 Manage cyber security policy and procedures 1.4 Manage cyber security governance 1.5 Manage organisational structure and staff responsibilities 1.6 Manage cyber security projects and investment	2.1 Document risk management appetite 2.2 Establish risk management framework 2.3 Document and review risks	3.1 Design audit and assurance program 3.2 Implement audit and assurance activities	4.1 Identify and record assets 4.2 Classify assets including identification of assets of state significance 4.3 Assign asset owners 4.4 Undertake ongoing asset management	5.1 Document cyber security incident management 5.2 Identify and report events 5.3 Respond to incidents 5.4 Review incident management activities	6.1 Establish resilience and service continuity plans 6.2 Review resilience and service continuity plans	7.1 Design and implement authentication requirements 7.2 Provision access 7.3 Review access 7.4 Terminate access
8. Manage threats and vulnerabilities	9. Manage suppliers	10. Develop secure software	11. Manage network communications	12. Manage mobile devices and teleworking	13. Manage robust ICT systems and operations	14. Manage personnel security, training and physical security
8.1 Design and implement vulnerability requirements 8.2 Design vulnerability management strategy aligned to requirements 8.3 Identify vulnerabilities 8.4 Remediate vulnerabilities 8.5 Monitor and review vulnerability activities	9.1 Establish procurement policy 9.2 Undertake pre-contracting activities 9.3 Select vendor and enter contract 9.4 Monitor ongoing contractual obligations 9.5 Terminate contract	10.1 Design secure software 10.2 Build, deploy and test secure software	11.1 Design and implement network security requirements	12.1 Establish mobile and teleworking procedures 12.2 Provision device management 12.3 Manage international travel risk	13.1 Manage change 13.2 Manage backups 13.3 Manage system configuration and hardening 13.4 Manage event logging and monitoring 13.5 Manage system redundancy	14.1 Manage personnel security 14.2 Manage training and awareness 14.3 Manage physical security

The implementation responsibilities between OCIO and agencies for each of the cyber security taxonomy activities are described in more detail in **Appendix B: Operating Model RACI**.

3. Implementation

3.1 Governance

To ensure the benefits of the Operating Model are realised, effective governance oversight of the design, operating and commercial principles will be carried out using existing SA governance arrangements outlined in the [South Australian Government ICT, Digital and Cyber Security Governance Framework](#). These include:

- Cyber Security Advisory Group
- Architecture Review Group
- CIO Steering Committee
- Senior Leadership Committee

Other mechanisms that will have governance oversight of the Operating Model include:

- Cabinet Submission costing comment review process
- Digital Investment Fund Board and Advisory Group

This will ensure that future cyber security services are delivered by the appropriate entities in accordance with the Operating Model and reduce duplication of effort and create opportunities of scale through centralised services and standardised approaches.

3.2 Cyber Security Service Catalogue

The service catalogue outlined in **Appendix A: Cyber Security Service Catalogue** describes the future state of cyber security services in SA Government.

The current state cyber security service catalogue is described on the [OCIO Extranet](#). New core and central services will be added iteratively as they are commissioned.

The [OCIO Services Portal](#) enables agencies to submit a request for a service.

Agencies can refer to the cyber security service catalogue to determine the scope of their responsibility for cyber security service delivery within their domain.

3.3 Cyber Security Taxonomy and RACI

While the cyber security service catalogue describes which entities are responsible for the delivery of specific cyber security services, the taxonomy and RACI provides a more granular breakdown of cyber security responsibilities for SA Government more generally and is aligned with the SACSF.

Elements of the taxonomy and RACI may not relate to specific services that can be requested but rather assigns responsibility for cyber security functions within the taxonomy. Entities can use the RACI to easily clarify the scope of their responsibility.

The Operating Model has been designed to be adopted and modified for use within the agency context, enabling entities to fully articulate the scope of their responsibility for resourcing and capacity planning purposes.

The RACI outlined in **Appendix B: Operating Model RACI** describes the future state for the delivery of the elements outlined in the cyber security taxonomy in accordance with the Operating Model commercial and operating principles.

The current state Operating Model RACI is described on the [OCIO Extranet](#) and is available as a tool for agencies to use to determine their responsibilities. It will be amended iteratively when new central capabilities become available.

Appendix A: Cyber Security Service Catalogue

The service catalogue describes the cyber security services delivered across the 3 roles described in the Operating Model: Core, Central and Local Services. They align to the whole of government cyber security taxonomy, and design principles.

OCIO Core Service Catalogue

Capability		Services / Activities
1	Cyber Strategy & Requirements	- Establish cyber security vision and strategy - Establish and maintain the South Australian Cyber Security Framework (SACSF) - Establish and communicate minimum expectations for all cyber security capabilities - Manage and maintain standardised SACSF policies and procedures templates - Establish cyber security requirements to manage supplier cyber risks
2	Cyber Governance & Leadership	- Establish and operate whole of government cyber security governance structures - Manage and maintain standardised cyber security position descriptions, organisational structures, and staff responsibilities - Manage whole of government cyber security projects
3	Core Cyber Risk	- Provide standardised cyber risk management tools, guidance and assistance - Identify Systems of State Significance (SoSS) - Provision of Governance, Risk and Compliance (GRC) tooling

OCIO Core Services – 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

OCIO Central Service Catalogue

Capability		Services / Activities
1	General Cyber Support	Provide advice and guidance to assist agencies to understand and implement the SACSF
2	Cyber Assurance	- Develop systems of state significance audit and assurance plan including scope and frequency of required activities - Perform independent assurance reviews of systems of state significance at least annually
3	Incident Response	- Develop and maintain frameworks, plans and capabilities to support the control agency for cyber crises - Undertake assessment to classify incidents - Coordinate incident response for multi agency-incident or Cyber Crisis, including public communications - Manage cyber security incident response specialists (e.g. internal capability or third parties) to support incident response activities - Coordinate consequence management activities across all types of incidents - Conduct post incident reviews for multi-agency incidents
4	Resilience	- Provide standardised support to enable cyber crisis simulation testing and review activities - Test resilience of systems of state significance
5	Threat Intelligence	- Create, receive and manage cyber threat intelligence for threats to SA government - Provide cyber threat intelligence to agencies on a proactive basis, as well as during incidents - Monitor deep and dark web (DDW) sources for evidence of SA government compromised accounts or stolen data - Hunt for cyber threats across SA government systems
6	Attack Surface Management	- Provide tooling to support vulnerability management - Undertake vulnerability scanning for internet facing assets - Undertake penetration testing of systems of state significance
7	Supply Chain Security	- Provide supplier cyber security risk advice for across government technology procurements, and procurements with an inherent cyber risk rating of high or extreme - Provide supplier cyber security risk advice for procurements providing systems of state significance - Provide general supplier cyber security risk management advice as required
8	Cyber Training & Awareness	- Develop and execute standardised cyber security and awareness training - Develop and execute phishing campaigns

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

Agency(Local) Service Catalogue (1/2)

Capability		Services / 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 - Implement a cyber security program - Identify, assess and implement change - Manage agency specific cyber security projects
2	Cyber Risk Management & 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	- Document 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

Agency (Local) Service Catalogue (2/2)

Capability		Services / Activities
7	Supply Chain Security	- Identify and assess inherent cyber risks with procurement and develop mitigation plans - Undertake vendor due diligence with consideration to cyber 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

Local Services – activities that require understanding of local context, local requirements and local subject matter. Local services provided by either:

Cluster agencies: Large agencies with the capacity and capability (including sector understanding) to deliver local services to small agencies who have insufficient capacity and capability.

Standalone agency: Agencies of sufficient capability and capacity to deliver local services.

Appendix B: Operating Model RACI

1. Provide leadership, set requirements and policy, and determine roles

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
1.1	Establish cyber security vision and strategy					
1.1.1	Establish whole of government cyber security vision and strategy		R/A		I	[I] (Cabinet)
1.1.2	Establish agency-specific cyber security strategy aligned to whole of government strategy				R/A	
1.2	Manage cyber security frameworks and requirements					
1.2.1	Establish and maintain the South Australian Cyber Security Framework (SACSF)	✓	R		I	A (Cabinet)
1.2.2	Ensure agency senior leadership sponsor the implementation of a cyber security program consistent with cyber strategy and SACSF	✓			R/A	
1.2.3	Attest to the agency's current state of alignment to the SACSF	✓			R/A	I (Cabinet)
1.2.4	Provide advice and guidance to assist agencies to understand and implement the SACSF		C	R/A	I	
1.2.5	Establish a program of work to maintain alignment to the SACSF	✓			R/A	
1.3	Manage cyber security policy and procedures					
1.3.1	Manage and maintain a standardized set of SACSF policies and procedure templates, and provide guidance		R/A	I	I	
1.3.2	Set, manage, maintain and communicate cyber security policy	✓			R/A	
1.4	Manage cyber security governance					
1.4.1	Establish whole of government cyber security governance structures and terms of reference		R/A	I	I	
1.4.2	Participate in relevant whole of government governance forums and committees		R/A	R	R	
1.4.3	Establish an Agency Security Committee with a direct report to senior leadership	✓			R/A	
1.5	Manage organisational structure and staff responsibilities					
1.5.1	Manage and maintain a standardised templates and position descriptions relating to organisational structure and staff responsibilities, and provide guidance		R/A		I	
1.5.2	Develop agency cyber security organisational structure embedded into agency governance framework	✓			R/A	
1.5.3	Formally assign cyber security roles and responsibilities with appropriately skilled and experienced resources	✓			R/A	
1.5.4	Ensure agency senior leadership are champions of cultural change	✓			R/A	

1.6	Manage cyber security projects and investment					
1.6.1	Manage whole of government cyber security projects		R/A	C/I	C/I	
1.6.2	Manage agency specific cyber security projects		I		R/A	
1.6.3	Ensure agency senior leadership participate in cyber security projects and initiatives				R/A	

2. Identify, assess and manage cyber security risk

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
2.1	Document risk management appetite					
2.1.1	Document risk management appetite	✓			R/A	
2.2	Establish risk management framework					
2.2.1	Provide standardised cyber risk management tools, guidance and assistance		R/A		I	
2.2.2	Develop and implement a risk management framework that includes cyber security risk management processes	✓			R/A	
2.3	Document and review operational risks					
2.3.1	Identify risk and include in agency risk register	✓			R/A	
2.3.2	Undertake period review of risks by the Agency Security Committee	✓			R/A	

3. Perform audit and assurance.

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
3.1	Design audit and assurance program					
3.1.1	Develop agency audit and assurance plan including scope and frequency of required activities	✓			R/A	
3.1.2	Develop systems of state significance audit and assurance plan including scope and frequency of required activities			R	C/I	A (Cabinet)
3.2	Implement audit and assurance activities					
3.2.1	Perform self-assessment assurance review of the cyber security program at least annually	✓			R/A	
3.2.2	Engage independent reviews in line with agency requirements	✓			R/A	
3.2.3	Undertake technical reviews of critical systems where applicable	✓			R/A	

3.2.4	Perform independent assurance reviews of systems of state significance at least annually			R	C/I	A (Cabinet)
-------	--	--	--	---	-----	-------------

4. Manage Information Asset Identification and Classification

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
4.1	Identify and record assets					
4.1.1	Provide access to tooling and guidance to identify and classify assets	✓	R/A		I	
4.1.2	Identify and record information assets				R/A	
4.1.3	Notify OCIO of internet facing assets			I	R/A	
4.2	Classify assets including identification of assets of state significance					
4.2.1	Classify information assets that support critical processes	✓			R/A	
4.2.2	Identify systems of state significance (SoSS)	✓	R		C/I	A (Cabinet)
4.3	Assign asset owners					
4.3.1	Assign asset ownership	✓			R/A	
4.3.2	Understand ownership responsibilities for information assets	✓			R/A	
4.4	Undertake ongoing asset management and maintenance					
4.4.1	Periodically review information asset identification and classification	✓			R/A	
4.4.2	Periodically review asset ownership	✓			R/A	
4.4.3	Document processes for labelling, storing, handling, and disposing of assets	✓			R/A	

5. Manage Incidents

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
5.1	Document cyber security incident management					
5.1.1	Establish policy and requirements for cyber crises	✓	A/R	I	I	
5.1.2	Develop and maintain frameworks, plans and capabilities to support the control agency for cyber crises		C	A/R	I	
5.1.3	Document incident response plan aligned to cyber security incident management policy				R/A	
5.1.4	Develop cyber security incident management procedures aligned to business continuity management plans	✓			R/A	
5.1.5	Identify and document responsibilities for cyber security incident management	✓			R/A	

5.2	Identify and report incidents					
5.2.1	Detect event				R/A	
5.2.2	Undertake initial incident assessment and classification				R/A	
5.2.3	Notify OCIO Watch Desk	✓		I	R/A	
5.2.4	Undertake assessment to classify incidents			R/A	C	
5.3	Respond to incidents					
5.3.1	Execute response consistent with incident response plan	✓			R/A	
5.3.2	Lead incident response for single-agency incident, including public communications			C/I	R/A	
5.3.3	Coordinate response for incidents managed under the Control Agency for Cyber Crisis Incident Management Framework , including public communications			R/A	C/I	
5.3.4	Lead agency-specific response for incidents managed under the Control Agency for Cyber Crisis Incident Management Framework				R/A	
5.3.5	Coordinate consequence management activities across all types of incidents			R	A/C/I	
5.3.6	Manage cyber security incident response specialists (e.g. internal capability or third parties) to support in response activities			C/I	R/A	
5.4	Review incident management activities					
5.4.1	Test incident management plans	✓			R/A	
5.4.2	Conduct post incident reviews	✓		I	R/A	
5.4.3	Conduct post incident reviews for incidents managed under the Control Agency for Cyber Crisis Incident Management Framework			R/A	C/I	

6. Maintain resilience and service continuity

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
6.1	Establish resilience and service continuity plans					
6.1.1	Include cyber security requirements in continuity plans	✓			R/A	
6.1.2	Undertake business impact assessments	✓			R/A	
6.1.3	Develop IT service recovery plans	✓			R/A	
6.2	Review resilience and service continuity plans					
6.2.1	Test continuity and service recovery plans	✓			R/A	

6.2.2	Provide standardised support to enable cyber crisis simulation testing and review activities			R/A	I	
6.2.3	Test resilience of systems of state significance			R/A	C/I	I (Cabinet)

7. Manage access to information

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
7.1	Design and implement authentication requirements					
7.1.1	Establish and communicate minimum authentication expectations including password standards		R/A	I	I	
7.1.2	Establishing trusted identity relationships between agencies			R/A		
7.1.3	Set authentication requirements aligned to minimum authentication expectations	✓			R/A	
7.1.4	Implement authentication requirements	✓			R/A	
7.2	Provision access					
7.2.1	Document processes to provision access	✓			R/A	
7.2.2	Provision access to information assets based on business need	✓			R/A	
7.3	Review access					
7.3.1	Undertake periodic review of access to information assets	✓			R/A	
7.4	Terminate access					
7.4.1	Revoke access once there is no longer a specific need for it	✓			R/A	

8. Manage Threats and Vulnerabilities

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
8.1	Manage intelligence and hunt for threats					
8.1.1	Create, receive and manage cyber threat intelligence for threats to SA government			R/A	I	
8.1.2	Provide cyber threat intelligence to agencies on a proactive basis, as well as during incidents			R/A	C/I	
8.1.3	Receive, triage and action threat intelligence across agency technology environment				R/A	
8.1.4	Monitor deep and dark web (DDW) sources for evidence of SA government compromised accounts or stolen data			R/A	C/I	
8.1.5	Hunt for cyber threats across SA government systems			R/A	C/I	
8.2	Design and implement vulnerability management expectations					
8.2.1	Establish and communicate minimum vulnerability management expectations	✓	R/A	I	I	

8.2.2	Establish vulnerability management strategy aligned to minimum expectations	✓			R/A	
8.3	Identify vulnerabilities					
8.3.1	Provide tooling to support vulnerability management			R/A		
8.3.2	Undertake vulnerability scanning for internet facing assets			R/A		
8.3.3	Undertake vulnerability scanning for internal facing assets				R/A	
8.3.4	Undertake penetration testing of agency systems as required based on risk management activities			C	R/A	
8.3.5	Undertake penetration testing of systems of state significance			R	A/C	
8.4	Remediate vulnerabilities					
8.4.1	Remediate identified vulnerabilities	✓			R/A	
8.5	Monitor and review vulnerability activities					
8.5.1	Notify material vulnerabilities in systems of state significance			C	R/A	I (SLC)

9. Manage suppliers and acquisition of technology

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
9.1	Establish procurement policy					
9.1.1	Establish whole of government procurement policy		I		I	R/A (Procurement SA)
9.1.2	Establish cyber security requirements to manage third party risks	✓	R/A	I	I	I (Procurement SA)
9.1.3	Establish policy and procedures aligned to procurement policy and cyber third-party risk requirements	✓			R/A	
9.1.4	Establish panel rules and secondary procurement process with respect to managing Cyber Security risks				R/A	
9.2	Undertake pre-contracting activities					
9.2.1	Undertake business requirements assessment and identify proposed technology requirements	✓			R/A	
9.2.2	Complete pre-qualification checklist to identify an information security risk with the proposed agency led procurement	✓			R/A	
9.2.3	Perform inherent cyber security risk tiering assessment across agency led procurements				R/A	I (Procurement SA)
9.2.4	Identify cyber security requirements across the agency led procurement as part of specification development	✓			R/A	
9.2.5	Provide third party cyber security risk advice as required			R/A		
9.2.6	Determine an evaluation plan that aligns with the Cyber Security requirements determined during specification development				R/A	

9.3	Select vendor and enter contract					
9.3.1	Undertake vendor due diligence with consideration to cyber risk and select supplier (excluding systems of state significance)	✓			R/A	
9.3.2	Where a vendor is interacting with a system of state significance, undertake supplier assessment with consideration to cyber risk			C	R/A	
9.3.3	Engage contract with vendor including agreement to cyber security obligations	✓			R/A	
9.3.4	For procurement activities relating to the acquisition of systems or software, undertake risk assessment of the system or software	✓			R/A	
9.4	Monitor ongoing contractual obligations					
9.4.1	Assessment and provision of secure access to the supplier				R/A	
9.4.2	Assessment and provision of secure access to the supplier where access is provided to the central tenancy			R	A	
9.4.3	Undertake contractual monitoring for cyber obligations (excluding contracts which impact systems of state significance)	✓			R/A	
9.4.4	Undertake ongoing contractual monitoring activities for cyber risks for contracts which impact systems of state significance			C	R/A	
9.5	Terminate contract					
9.5.1	Execute supplier transition out plan for cyber security requirements				R/A	
9.5.2	Obtain assurance the supplier has performed their cyber security offboarding obligations				R/A	

10. Develop secure software

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
10.1	Design secure software					
10.1.1	Document minimum software development practices		R/A	I	I	
10.1.2	Document requirements for software development consistent with cyber security expectations	✓			R/A	
10.1.3	Design software consistent with requirements				R/A	
10.2	Build, deploy and test software					
10.2.1	Undertake security functionality testing and vulnerability assessments				R/A	
10.2.2	Build, deploy and test software in segregated environments				R/A	

11. Manage network communications

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
11.1	Design and implement network security requirements					
11.1.1	Establish and communicate minimum network security expectations		R/A			
11.1.2	Implement and operate network security services aligned with the minimum network security expectations	✓			R/A	

12. Manage mobile devices and teleworking

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
12.1	Establish mobile and teleworking procedures					
12.1.1	Establish baseline requirements and guidelines for teleworking and mobile device management	✓	R/A	I	I	
12.1.2	Establish teleworking procedures	✓			R/A	
12.1.3	Establish mechanisms for protecting information stored on mobile devices	✓			R/A	
12.2	Provision device management					
12.2.1	Provide mobile device management solutions	✓			R/A	
12.2.2	Provision devices consistent with mobile device and teleworking requirements				R/A	
12.3	Manage international travel risk					
12.3.1	Provision travel devices for international travel aligned to the risks of the destination country				R/A	
12.3.2	Provide cyber security advice to relevant personnel on international travel risks			C	R/A	C (DPC SERM)

13. Manage robust ICT systems and operations

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
13.1	Manage change					
13.1.1	Identify, assess and implement change	✓			R/A	
13.2	Manage backups					
13.2.1	Develop and manage backup strategies	✓			R/A	
13.2.2	Execute backup strategy as required	✓			R/A	
13.3	Manage system configuration and hardening					

13.3.1	Establish standardised configuration and hardening expectations		R/A	I	I	
13.3.2	Execute configuration and hardening activities	✓			R/A	
13.4	Manage event logging and monitoring					
13.4.1	Develop event logging and monitoring requirements and guidelines		R/A	I	I	
13.4.2	Develop event logging and monitoring strategy and capability	✓			R/A	
13.4.3	Monitor for anomalous events	✓			R/A	
13.5	Manage system redundancy					
13.5.1	Plan for system redundancy as part of system design consistent with business impact assessments	✓			R/A	

14. Manage personnel security, training and physical security

Ref	Activity	SACSF	Responsibility			
			OCIO Core	OCIO Services	Agency	Other
14.1	Manage personnel security					
14.1.1	Manage background checks	✓			R/A	
14.1.2	Administer and process Commonwealth Government clearance requirements				A	R/I (SERM)
14.1.3	Assess and manage the ongoing suitability of personnel in relation to their role				R/A	
14.1.4	Provide ongoing awareness of personnel cyber security obligations				R/A	
14.2	Manage training and awareness					
14.2.1	Develop and execute standardised cyber security and awareness training		C	R/A	I	
14.2.2	Undertake cyber security skills gap assessment to identify targeted training needs	✓			R/A	
14.2.3	Provide training to personnel	✓			R/A	
14.2.4	Develop and execute adversary attack simulations (for example phishing)			R	A/I	
14.2.5	Remediate results of adversary attack simulation campaign				R/A	
14.3	Manage physical security					
14.3.1	Implement physical security measures to protect assets	✓			R/A	

Aboriginal Impact Statement

The needs and interests of Aboriginal people have been considered in the development of this policy. There is no specific impact on Aboriginal people.

For more information:

Strategy, Policy and Engagement, Cyber Security
Office of the Chief Information Officer
cybersecurity@sa.gov.au
www.security.sa.gov.au

Document Approval and Control

Version and confidentiality

Reference	Details
File Number	A5055682
Version	1.0
Status	Final

File name and location

File name	Document location
SA Cyber Security Operating Model	Objective

Revision history

Revision version	Revision date	Summary of change	Author
------------------	---------------	-------------------	--------

Document sign off

Title	Name	Date signed	Signature
Chief Information Officers Steering Committee	Members	6/11/2024	N/A
Senior Leadership Committee	Members	27/03/2025	N/A
SA Government Cabinet	Ministers	23/06/2025	N/A

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](https://creativecommons.org/licenses/by/4.0/). To attribute this material, cite the Office of the Chief Information Officer, Department of Treasury and Finance, Government of South Australia, 2025.