

South Australian Cyber Security Framework

Cyber Security Program Guide



Government of
South Australia

OFFICIAL

Table of Contents

1. Introduction.....	3
1.1 Purpose of this document	3
1.2 OCIO Cyber Risk Advisory Services	4
2. Cyber Security Governance.....	5
2.1 Establishing CSP Ownership and Sponsorship	5
3. Agency Risk Profiling	8
3.1 Cyber Security Risk Appetite.....	12
3.2 Information Asset Identification and Classification	15
3.3 SACS Tier Selection	17
4. Cyber Security Program Planning.....	19
4.1 Gap Analysis.....	19
4.2 Risk Assessment	22
4.3 Agency Strategy and Roadmap	24
4.4 Team Structure and Responsibilities	25
5. Cyber Security Operations	27
5.1 Cyber Security Calendar.....	27
6. Implementation.....	30
6.1 Implementation Toolkit.....	31
6.2 Guidance and Templates	31
6.3 Governance, Risk and Compliance (GRC) Tool	32
7. Monitoring and Reporting.....	33
7.1 Annual Attestation.....	34
7.2 Continuous Improvement Activities.....	35
Appendix A: LIST OF RESOURCES	36
Appendix B: DEFINITIONS	37
Appendix C: ACRONYMS.....	39

1. Introduction

The [South Australian Cyber Security Framework \(SACSF\)](#) standardises the approach and guides the establishment, implementation, maintenance, and continuous improvement of South Australian (SA) Government agencies' cyber security management systems. At the core of the effective implementation of the SACSF is an agency's Cyber Security Program (CSP).

An agency's CSP demonstrates its ongoing commitment and approach to managing cyber security risks to their unique services by:

- Clearly defining the agency's cyber risk profile and how the identified risks are to be managed.
- Providing the structure, work program, and resourcing essential for the delivery of the security outcomes supporting the agency's vision, goals, and objectives.
- Ensuring alignment and support of the achievement of the SA Government's cyber security strategy and the government's strategic objectives.
- Ensuring adherence to applicable legal, regulatory, and contractual requirements.

1.1 Purpose of this document

This Cyber Security Program Guide has been developed to support agencies in the development of a program that addresses existing and emerging cyber security risks. This guide supplements [Section 3 - Implementation Approach](#) of the SACSF, and together with the guidelines, tools and templates, provides a starting point for any agency.

This guide provides simple steps for risk management activities, and the intended outcomes for each of the six stages shown in *Figure 1: SACSF Implementation Approach*. The structure follows the familiar Plan-Do-Check-Act (PDCA) cycle seen in many management systems and can be used to start a CSP from scratch, or to improve an existing CSP by using the guidance and tools to review what is already in place.



Figure 1. SACSF Implementation Approach

1.2 OCIO Cyber Risk Advisory Services

The Office of the Chief Information Officer (OCIO) under the Department of Treasury and Finance (DTF) provides cyber risk advisory services for agencies. This service supports agencies to develop and implement cyber security programs and interpret and apply the SACSF, including the associated guidelines and rulings, in cyber security risk management activities.

For more information, or to find out how we can help you, please send a service request via the [OCIO Services Portal](#) and tag the Strategy, Policy and Engagement Team, or contact:

Cyber Security Directorate
Office of the Chief Information Officer (OCIO)
Department of Treasury and Finance

T 1300 244 168
E cybersecurity@sa.gov.au
W security.sa.gov.au

2. Cyber Security Governance

Establishing CSP Ownership and Sponsorship

The success of a CSP requires ownership and sponsorship by senior leaders to drive change across the agency.

[Appendix C](#) of the SACSf describes the existing governance bodies and functions providing oversight of cyber security within the SA Government. It also describes the roles that will have responsibility for the ownership and coordination of an agency's CSP. The [CSP RACI Matrix](#) provides clarity around the engagement required in each step of a CSP lifecycle.



It is vital to have the right individuals assigned the ownership and the coordination of the agency's CSP, so they have the right level of authority, influence, and accountability for its successful implementation. The key CSP roles may be assigned as shown in the following table.

CSP Responsibility	Possible Assignment
CSP Owner - Responsible for the successful operation of the CSP.	Agency Security Executive (ASE), or Chief Information Security Officer (CISO), or Chief Information Officer (CIO)
CSP Coordinator - Responsible for the operations of the CSP and coordination of cyber security activities.	Information Security Manager, or Information Technology Security Adviser (ITSA), or IT Manager

Depending on the structure and the size of the agency, one individual may wear many hats provided they are clearly defined and have the appropriate authority to perform the CSP roles. Agencies should document a cyber security program governance framework or a cyber security policy that formally defines these roles and have it approved by senior leadership.

The establishment of a security committee and/or working group facilitates effective governance of the program. A charter or terms of reference (ToR) that defines its

purpose, scope, authority and responsibilities, membership, and administration should be formally approved, and the performance of the committee or group reviewed periodically to ensure it continues to be effective.

The steps described in the following table provide a guide on how to set up a security committee and a working group.

Step	Action
Identify cyber specific groups	It is important to balance governance with the scale and complexity of the CSP. Identify any existing committees within the agency. <i>Is there already a governance and reporting structure or working group that cyber can be added to instead of creating a separate group?</i> Using an existing governance committee or working group is beneficial when the stakeholders and resources are similar. In larger or more complex agencies, a standalone security governance committee may give more focus to cyber security program management.
Define committee and/or working group ToR	• Document the objectives of the committee and/or working group, specific to the scope of the CSP. • Define the reporting requirements in to and out of the group. • Agree the frequency of the meetings. • Outline the membership and their specific roles and responsibilities. For example: ○ A committee would typically involve senior executive(s) who provide formal approval and decisions raised regarding the program. ○ A working group would typically report to the committee and is responsible for tracking and reporting on: - Operational security activities. - Progress against CSP initiatives or projects (implementation/uplift of cyber security controls).
Agreement	• All members of the selected groups are to review and agree to the terms.
Schedule	• Schedule all committee/working group meetings and maintain suitable records that demonstrate effectiveness.

Related Guidance and Templates

- [SAPSF GOVSEC 1: Security Governance](#)

- [SACSF G5.0 Information Technology Security Adviser \(ITSA\) Role and Responsibilities](#)
- [TEMPLATE - Agency Security Committee Terms of Reference](#)
- [TEMPLATE - Agency Security Working Group Terms of Reference](#)
- [TEMPLATE - CSP RACI Matrix](#)
- [TEMPLATE - Cyber Security Policy](#)
- [TEMPLATE - Cyber Security Program Governance Framework](#)

3. Agency Risk Profiling

Analysing an agency's overall cyber security risk profile provides a comprehensive understanding of the threats and vulnerabilities that the agency faces. This in turn supports risk-based decision-making on what resources are required and how they will be prioritised to effectively protect the agency's most critical assets.

It is essential to first understand the context of cyber security within the agency to determine an appropriate risk appetite and to ensure that the CSP is scoped appropriately.

Context establishment considers both internal and external factors that may influence the CSP objectives. These factors include various stakeholders' needs and expectations, the industry standards, regulations, and frameworks that are applicable to the agency, the dependency and use of technology and the dependency on suppliers and other parties.

Context and scope should both be reviewed regularly to ensure that the program remains relevant.

Cyber stakeholder needs analysis

Cyber risk management is applied in the context of an agency's business processes. It is therefore important to identify the business stakeholders not just to establish their expectations within the CSP but also what they can do to support the program and therefore the security objectives.

A stakeholders' needs analysis helps flesh out some of these internal and external factors impacting the definition of the CSP. This activity aims to:

- Clearly document stakeholders' needs and expectations around cyber security.
- Align the CSP objectives with the identified stakeholders' needs and expectations.
- Identify gaps and opportunities for improvement. *Where are expectations not currently met?*

The steps described in the table that follows provide a guide on how to perform the activity.



Step	Action
Identify stakeholders	Create a list of all stakeholders that have an interest in or may be impacted by the CSP. This may include: • Clients / citizens / end users. • Staff. • Internal departments and executive (e.g. Minister, Chief Executive, human resources, ICT services, records management, facilities, procurement, legal, risk and audit). • Other State or Commonwealth Government agencies. • Third parties including commercial parties. • Department of Treasury and Finance – Office of the Chief Information Officer. • Any relevant regulatory bodies.
Define their needs and expectations	For each stakeholder, document what their needs and expectations of the CSP are. <i>Why do they care about the CSP?</i> For example: • Clients/citizens expect that their personal data is securely managed during processing and storage. • The agency risk and governance team require a periodic review of the business risk register including cyber risks. • Other State Government agencies/sub agencies may require assurance on the security of systems your agency provides for them. • DTF-OCIO requires reporting of the CSP status in the annual SACSf attestation.
Research	Engage with your internal stakeholders. Consider sending out a questionnaire to identify or confirm your assumptions around their expectations.
Identify how requirements are currently met	For each of the stakeholders and per requirement/expectation, outline how they are being met. For example, regarding privacy: • The agency has a dedicated privacy officer and culture of awareness regarding the processing of personal data. • All agency personnel are provided annual training on cyber security and how to protect data.

Related Guidance and Templates

- [TEMPLATE - CSP Stakeholders Requirements](#)

Identifying cyber relevant regulations, standards, and contractual obligations

Another important step in establishing context for the agency is understanding the regulatory and contractual requirements that are relevant to the agency.

The objectives are to:

- Clearly document obligations regarding cyber security.
- Align the CSP objectives.
- Identify gaps and opportunities for improvement e.g. *Where are expectations not currently met?*

The following table provides a guide on how to perform the activity.

Step	Action
Identify stakeholders for compliance monitoring	As a part of the stakeholder needs analysis, determine who within your agency is responsible for monitoring: • legal and regulatory requirements with respect to cyber security. • contractual requirements on the agency (usually established via a memorandum of agreement with another State or Commonwealth agency) with respect to cyber security. Determine if there are any existing processes for monitoring these requirements (e.g. in a compliance obligations register).
Identify regulations and contractual obligations	Create or update the list of all regulations, standards, and contractual obligations in scope of the CSP. It will be worth engaging with your compliance stakeholders identified above to confirm any obligations relevant to cyber security.
Identify how requirements are currently met	For each of the requirements, outline how they are being met. For example, regarding SACSf requirements: The agency: • Has dedicated resources for cyber security. • Maintains a cyber risk register. • Reports against the SACSf annually.

Step	Action
	Has an approved security strategy / implementation roadmap.

Related Guidance and Templates

- [TEMPLATE - Security-related Regulatory Legal and Contractual Requirements](#)

Identifying critical business processes and dependencies

To help determine the most critical information assets to the agency, it is essential to understand the risks associated with the business processes in scope of the CSP and their dependencies. The agency should refer to its existing business continuity management process and leverage information from the Business Impact Analysis (BIA) to answer the following questions:

- Who do you depend on for the delivery of your services?*
- What services do they provide you?*
- What is the impact of the loss of availability of these information assets to the agency's services?*

The BIA should assist in understanding the most critical and sensitive business processes for the agency. Equally, the BIA should indicate the assets that the business units depend on to deliver those critical services, such as:

- People (staff, suppliers, and contractors).
- Data, documents, and records.
- Hardware (specialist equipment and technology).
- Software.
- Facilities.

The BIA process is not part of the CSP. Information from the BIA informs the agency's Information Asset (IA) Register. If the existing BIA process does not have the right information, the CSP Coordinator or delegate should work with the responsible team to get it amended. A BIA template is provided in this guide for agencies that might not have one.

Related Guidance and Templates

- [TEMPLATE - Business Impact Analysis \(BIA\)](#)

Defining the CSP scope

A CSP scope statement is required to clearly define the coverage and boundaries of the program. This includes the organisational aspects of the agency such as legal entities, processes or services, physical locations or sites, ICT scope such as systems, applications, network components and data.

Examples of possible scope and boundary statements are:

- *All digital information and systems used in the delivery of the following [agency] functions: [enumerate]...*
- *The development, operations, maintenance and support of [agency] ICT infrastructure and the following primary applications: [enumerate]...*
- *All ICT assets that create, store, process or transmit information and all information transmitted over [agency's] data network.*
- *All physical sites managed and maintained by the [agency] that process and store digital information assets located at: [enumerate]...*

Items that are out of scope should also be defined with a clear explanation as to why they are deemed out of scope. This may be a point in time requirement, e.g. to achieve staged roll out and implementation of the CSP.

Defining cyber security objectives

The establishment of an agency's cyber security objectives allows management to direct all cyber security activities that support the implementation of its strategic goals and address the agency's unique risk profile. The development of these objectives takes into consideration the internal and external factors established in the preceding activities. These objectives are usually documented in the agency's cyber security policy and are typically endorsed by the Agency Security Committee and signed off by the agency Chief Executive.

3.1 Cyber Security Risk Appetite

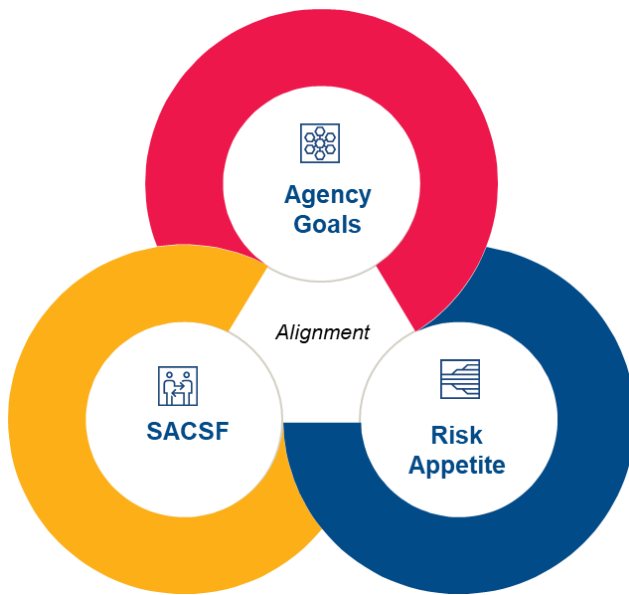
Cyber risk appetite is important in defining how an agency intends to respond to cyber security risks. It sets the framework and boundaries for the entire CSP.

Risk appetite is the type and amount of risk your agency is prepared to accept to achieve its objectives. Articulating the cyber security risk appetite of the agency explicitly defines the expectations that the agency has toward addressing cyber security risks. It promotes consistent, risk informed decision-making aligned with strategic aims and supports robust corporate governance by setting clear risk-taking boundaries.

Cyber security risk appetite should consider:

- the external business environment and core objectives of the agency.

- the risk culture of the agency.
- the risk management context, including senior leadership's responsibility for overall risk appetite, tolerance, and strategy.



Aligning risk appetite with agency goals and existing policies ensures a structured approach to cyber security, balancing risk with business needs and compliance.

The security team needs to work with the agency's risk and governance team to incorporate the cyber security risk appetite statement into the agency risk management framework and risk appetite, where possible.

To develop the agency's cyber security risk appetite statement, it is important that individuals involved have the experience and understanding of

cyber security risk management practices and have a clear working understanding of the agency, its objectives, and its stakeholders. Key roles that should be involved in the development of risk appetite statements are the agency ITSA, the risk and governance team, the security committee (as defined by the agency) and the executive leadership team.

The following table provides a guide on how to perform the activity.

Step	Action
Engage with agency key stakeholders	Facilitate workshops with key stakeholders to gather insights on their perspective, concerns, and priorities regarding cyber security risks. The cyber risk acceptance criteria should be established considering the following factors/risk categories: • Agency objectives. • Legal and regulatory requirements. • Operational activities. • Technology. • Financial. • Processes. • Supplier relationships.

Step	Action
	- Human factors (e.g. related to privacy). This list is non-exhaustive, so agencies should consider other factors/risk categories based on the context of their own organisation. The agency's risk management framework is a good start to look into relevant risk categories. Note: - Risk acceptance criteria can differ depending on how long the risks are expected to exist (e.g. the risks can be associated with a temporary or short-term activity). - Ensure that the risk appetite reflects the priorities and goals of the agency. Consider the trade-offs between risk and opportunity, ensuring that the agency is not overly risk-averse or risk-seeking, but is positioned to achieve its objectives effectively.
Draft the cyber security risk appetite statement(s)	Create an initial draft of the cyber risk appetite statement that covers each of the relevant influencing factors from the perspective of cyber security. Write the statement in clear, specific terms that can be easily understood and applied across the agency. Avoid vague language and ensure that the statements are actionable. Ensure its alignment with the agency's broader risk appetite statement. Cyber security risk appetite statement could also be embedded in a broader agency risk appetite statement which considers other types of risk to the agency.
Test and seek feedback on the draft	Circulate the draft risk appetite statement among stakeholders for feedback. This may include multiple iterations to refine and clarify the content. Adjust the statement based on the feedback received, ensuring that it accurately reflects the agency's risk posture and priorities.
Obtain approval	Present the finalised risk appetite statement to senior leadership for review and approval. This could include the CISO, Chief Executive, CIO, Chief Financial Officer, Chief Technology Officer and Agency Risk Committee. The Chief Executive is expected to approve the risk appetite statement for the agency.
Communicate and implement	Once approved, communicate the risk appetite statement across the agency. Ensure that all relevant teams and departments understand and adhere to the guidelines. Embed the risk appetite statement into existing cyber security

Step	Action
	policies, procedures, and risk management frameworks to guide decision-making.
Update cyber risk documentation	Review and update the following to ensure risk mitigation strategies are aligned with the risk appetite: - the agency risk management framework and risk matrix (and/or cyber security risk matrix). - the cyber security risk register. - previously accepted risks. - risk treatment plans.

Related Guidance and Templates

- [SACSF/G8.0 Security Risk Management](#)
- [TEMPLATE - Cyber Security Risk Appetite Statement](#)

3.2 Information Asset Identification and Classification

Information assets are classified according to characteristics that the agency needs to protect namely Confidentiality, Integrity, and Availability (CIA). This helps with prioritising risk management activities and selection of security controls to preserve these characteristics.

The South Australian Protective Security Framework (SAPSF) [South Australian Information Classification System](#) assists in the determination of the appropriate confidentiality rating. The integrity and availability rating criteria are covered under the [SACSF/G6.0 Integrity and Availability Classification using the SACSF](#). The availability rating of information assets should align with the result of the BIA.

The Information Asset Register is a tool that allows the agency to centrally evaluate its information assets and identify the most valuable assets that need additional controls on top of the baseline. The register is not intended to be an inventory of every asset (such as a finance fixed asset inventory or a document register) but needs to help prioritise groups of assets that have similar value and risks.

The register should document at least the following:

- Information asset/system name and description.
- Whether the system supports business critical processes.
- Confidentiality, Integrity, and Availability classifications.
- Information asset owner, contact details and role/position.
- Date of information asset classification approval.

- Information asset classification review date.

The register may also include:

- If the system is supported by a supplier, and supplier contact details.
- If the asset stores, processes, and transmits personal information.

The Information Asset Register can leverage information from the agency BIA. It should be reviewed regularly by the asset owner and when the following triggers an update:

- introduction of a new business process or service.
- integration of a new system, application, or platform into the agency ICT environment.
- changes to an existing system, application, platform, or underlying technology and infrastructure.

The following table provides a guide on how to perform the activity.

Step	Action
Identify business processes in scope	Review the BIA with the agency stakeholders to understand the processes and assets in scope of the CSP. Each agency will typically have its own Business Continuity Management Framework or Procedure which should include requirements for the analysis of the agency's "business critical" services, functions or processes using a BIA template.
Identify the most valued information assets	From the BIA, determine the most valued assets that impact business operations if compromised.
Complete draft Information Asset Register	Enter the assets and assign a draft classification based on impact of loss (Availability) using information from the BIA. Where possible, aggregate the assets that are of a similar nature and value. Note: The register is not intended to be an inventory of each individual ICT asset. Provided the asset has the same values or subject to similar risks (e.g. stored in the same location / same system / environmental conditions) then they can be recorded as a group.
Research	Meet with asset owners (preferred) or send out a questionnaire / form to collate information regarding information assets and ask them to assign the Confidentiality, Integrity and Availability classifications or confirm any previous classification assigned. Review and challenge the classification to ensure that it is not

Step	Action
	over or under classified.
Finalise Information Asset Register	Each information asset owner must formally approve the classification. Update and finalise the Information Asset Register with information gathered from the above activities.

Related Guidance and Templates

- [SAPSF South Australian Information Classification System](#)
- [SAPSF Classification Assessment Tool](#)
- [SACSF Guideline 6.0 Integrity and Availability Classification using the SACSF](#)
- [TEMPLATE - Information Asset Classification Form](#)
- [TEMPLATE - Information Asset Register](#)

3.3 SACSF Tier Selection

Under the SACSF, each SA Government agency is required to select a tier level. The objective of the tiering model is to ensure that those with a higher cyber risk profile apply a more mature approach to cyber risk management and can demonstrate the effectiveness of their CSP to key stakeholders.

The SACSF outlines some of the characteristics of agencies within each tier level. Key considerations for determining the tier level are:

- the complexity of the technology environment.
- the cyber security risk appetite of the agency.
- the criticality of services provided by the agency.
- the classification of information held by the agency.

Tier One	Simple technology environment (e.g. <200 staff)	Moderate or higher appetite for cyber security risk	Extended outage would have only minor impact	Official
Tier Two	Common use technology environment (e.g. <500 staff)	Moderate or lower appetite for cyber security risk	> 1 week outage would have catastrophic consequences	Official
Tier Three	Complex technology environment (e.g. >500 staff)	Low appetite for cyber security risk	> 48 hour outage would have catastrophic consequences	Official: Sensitive
Tier Four	Highly complex technology environment (e.g. >2,000 staff)	Very low appetite for cyber security risk	> 4 hour outage would have catastrophic consequences	Protected or higher

These characteristics are not definitive and should be used as a guide only. Agency Chief Executives must approve and are accountable for their agency's tier selection.

Related Guidance and Templates

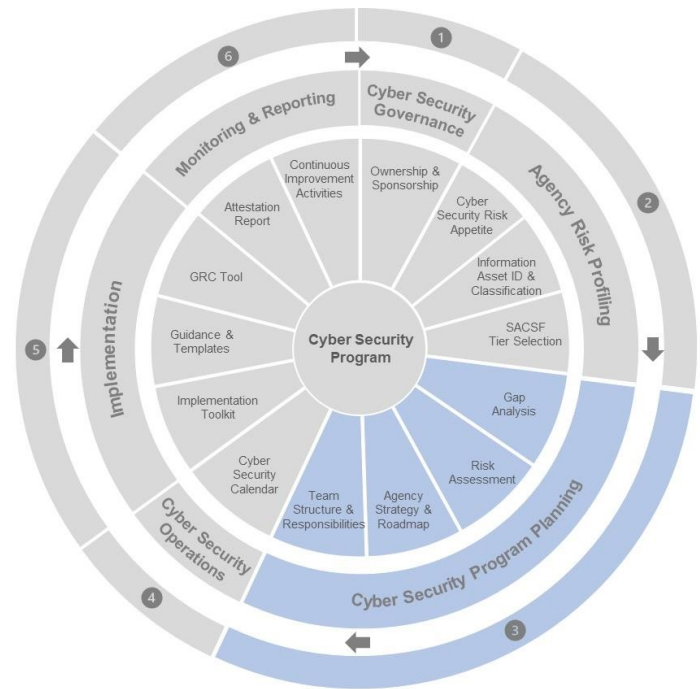
- **TEMPLATE - Minute to CE for Tier Selection** (SA Government agencies can contact cybersecurity@sa.gov.au for access)

4. Cyber Security Program Planning

4.1 Gap Analysis

Once the CSP scope, security objectives and risk profile have been defined, it is essential for the agency to conduct a gap analysis to establish its current cyber security capabilities. The gap analysis should be comprehensive enough to:

- Define how stakeholder needs and expectations are being met.
- Be used as an input to cyber risk evaluation.
- Identify gaps in requirements for cyber security.
- Determine the maturity of each control.
- Prioritise an improvement plan / roadmap.



The gap analysis should be performed against the requirements of the SACS. This analysis can be guided by leveraging the [SACS Implementation Toolkit](#) to identify the degree to which the agency has met each of the requirements of the framework for their tier level, and the program of work to implement the requirements. The implementation toolkit provides mappings between the SACS and other common industry standard security frameworks for ease of control identification.

Some agencies provide ICT services to other agencies. The agencies providing services must supply enough information about their CSP to the receiving agencies to enable them to perform a gap analysis. Agencies that receive services from other agencies must identify where controls may sit with other agencies as part of their gap analysis. Furthermore, it is important for agencies that receive technology services to understand their obligations for implementing controls related to the information assets they are responsible for.

The following table provides a guide on how to perform the activity.

Step	Action
Create the agency gap analysis worksheet	The SACS Implementation Toolkit is a starting point for the gap analysis. Where there are requirements to demonstrate performance against other regulatory requirements or industry standards, the agency can expand the gap analysis to cover

Step	Action
	controls within other standards such as ISO 27001, NIST, or the Information Privacy Principles, or PCI-DSS.
Assign ownership	In the gap analysis worksheet, clearly define which role is responsible for the requirements and controls so that they can be included in the interviews (see next steps below). They may be from another department or a different business unit or may be a supplier. Agencies should also consider whether sufficient workforce capability and capacity exist to implement and sustain applicable controls. The <i>SA Government Cyber Security Workforce Guide</i> provides a structured methodology for assessing workforce capability and capacity gaps and identifying actions required to address resource and skills deficiencies.
Conduct document review	Collate and review the content of all relevant policies, procedures, and guidelines available. Assess whether they adequately cover the specific security control requirements.
Conduct interviews	Conduct interviews with key personnel across the agency who have specific roles and responsibilities, this may include roles such as: a) Procurement (third party management and contractual obligations). b) Human resources (security awareness, screening, onboarding and offboarding). c) Agency risk and governance (risk framework, governance, and reporting, may also cover business continuity). d) Legal (relevant legislation and reporting). e) IT and Helpdesk (incident management, IT operations). Security team (security governance, operations, training, and reporting).
Identify accountable third parties	For controls that are managed outside your agency, highlight these and identify: a) Any relevant contractual agreements or memorandum of understanding. b) Any reference to standards or agreement as to what they are responsible for. c) Evidence of third-party risk assessment. The objective is to understand how well the third-party

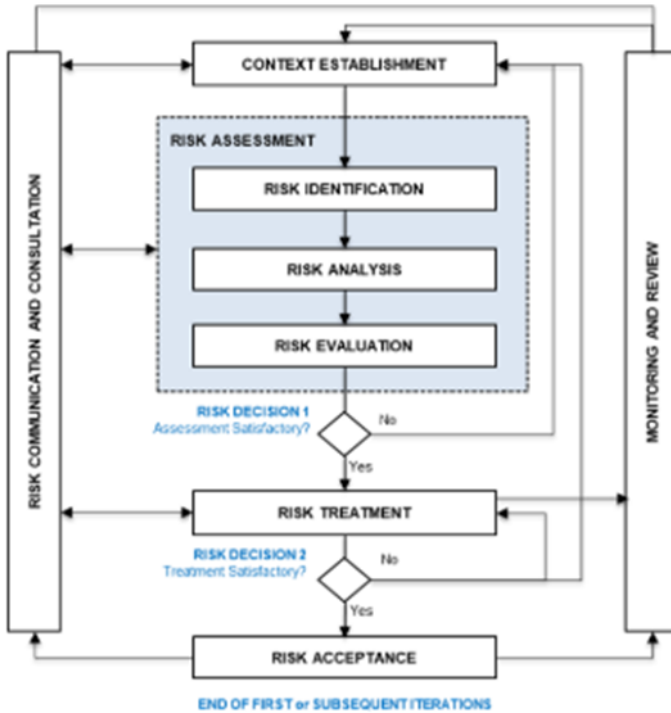
Step	Action
	dependencies are understood and are being managed and answering the following questions: • <i>Is their role clear and agreed to by all parties?</i> • <i>Have you confirmed your assumptions in what they provide? and</i> • <i>Have you validated or obtained assurances for what they provide?</i>
Finalise the gap analysis	Summarise the findings from the interviews and highlight where controls are applicable and not applicable to the agency environment. For those that are applicable, assess if they are: - Not in place / ad hoc. - In development / In progress. - Partially implemented. - Fully implemented. If some controls are quantified (subject to regular reporting and metrics), add this in your notes against the implementation status. Note: This can align to a preferred capability maturity model, as required.

Related Guidance and Templates

- [TEMPLATE - SACSf v2.0 Implementation Toolkit](#)
- SA Government Cyber Security Workforce Guide (SA Government agencies can contact cybersecurity@sa.gov.au for access)

4.2 Risk Assessment

The diagram from ISO/IEC 27005 *Information security, cybersecurity, and privacy protection — Guidance on managing information security* provides a visual representation of the cyber risk management process.



Cyber risk assessments should be conducted systematically, iteratively, and collaboratively, drawing on the knowledge and views of personnel throughout the agency. Some of the key roles that should be involved and consulted in the risk assessment are the agency ITSA, the information asset owner, the agency risk and governance team, the agency security committee (as defined by the agency) and executive leadership team.

Cyber risk assessments enable agencies to identify high risk areas that should be prioritised in the agency's CSP. As agencies mature

their cyber risk assessment process, risk assessments may evolve to focus on individual systems that aggregate to a whole-of-agency view.

A risk assessment or re-assessment can be triggered by the following:

- Periodic review.
- Change in services or business processes.
- New information assets.
- Significant changes to assets.
- Outcomes of the BIA.
- Incidents or near-miss events.
- Changes to contracts, regulations, and standards.
- Threat intelligence.
- Implementation of new controls.
- Machinery of government changes.

The [SACSF/G8.0 Security Risk Management](#) provides more information on this activity. The following table summarises points to consider for each step.

Step	Action
Assess risks	1. Based on the agency risk profile and information assets in scope of the CSP, identify any known vulnerabilities or gaps in controls (output of gap analysis). 2. Identify cause events for each relevant risk identified and determine how likely they are to occur based upon: • Outcomes of cyber threat intelligence. • Experiences and past events (incidents). • Observation. • Confidence in the controls (or control maturity) – outcome of gap analysis. 3. Determine the consequence should the risk events occur using the risk framework. 4. Calculate the overall risk rating.
Draft a Risk Treatment Plan (RTP)	1. Based on the risk framework, determine a RTP for each risk (e.g. <i>Is it within risk appetite?</i>) and determine whether the agency should: • Mitigate the risk (reduce risk likelihood or impact by implementing controls or countermeasures). • Transfer (to a third party). • Accept the risk and monitor over time. • Avoid the risk and stop doing the activity that lends to the risk event. 2. Identify information security controls that reduce the likelihood and/or consequence of the risk events. 3. Prioritise remediation, based on effectiveness of the controls, benefits and resources available to the agency, and draft the cyber security strategy. 4. Ensure that key stakeholders are consulted in these activities and responsibilities for the treatments are agreed upon.
Approval	• Obtain approval from senior leadership on the outcomes of the risk assessment and RTP. • Senior leadership should formally acknowledge and approve any accepted risks. • Senior leadership to review and approve the cyber security strategy and provide adequate resources.

Step	Action
Risk monitoring	Maintain a risk register and ensure that progress against the treatment plan and the following are tracked: • New / changed risks. • Closed / accepted risks.

Related Guidance and Templates

- [SACSF/G8.0 Security Risk Management](#)
- [TEMPLATE - Security Risk Register](#)
- [TEMPLATE - Security Risk Assessment Report](#)
- [TEMPLATE - Security Exemption Request Form](#)
- [TEMPLATE - Security Exemption Register](#)
- [Security Risk Assessment Workshop Facilitation Guide](#)

4.3 Agency Strategy and Roadmap

Using the findings from the gap analysis and risk evaluation, create the agency security strategy and roadmap.

The strategy should summarise where the agency is currently at in terms of its security capabilities. It needs to consider internal and external strategic drivers (e.g. the agency's strategic objectives, emerging technologies and the current and future ICT environment, and the threat landscape) to define where it needs to be as the target future state. The strategy should be pragmatic and achievable within a reasonable timeframe based on the risk appetite, budget and resource allocation allowed by the agency.

The work program should take into consideration:

- The strategic cyber security objectives of the agency in alignment with the SACSF.
- The SACSF tier selected by the agency including selection justification.
- The cyber security risk appetite of the agency.
- The cyber security governance model to be used by the agency including the key cyber security responsibilities of functions within the agency.
- The scope, boundaries, and exclusions of the CSP.
- The interested parties (e.g. stakeholders) that require the agency to implement robust cyber security controls.
- Applicable legal, regulatory, and contractual requirements of the agency.

The priority of implementation should consider:

- Whether a control is 'mandatory'.
- The impact of the control in managing a risk event. *Does it help to significantly reduce the likelihood or consequence of the risk event, or mitigate multiple risk events?*
- Current capabilities and capacity.
- Ease of implementation e.g. *Are there any 'quick wins' you can get across the line?*

Approval from the highest levels of management will help with buy-in and support for its implementation.

Related Guidance and Templates

- [TEMPLATE - Cyber Security Strategy and Roadmap](#)
- [TEMPLATE - Cyber Security Work Program](#)
- [TEMPLATE - Cyber Security Strategy on a page](#)

4.4 Team Structure and Responsibilities

The successful implementation and ongoing operation of a CSP depends on having appropriately defined cyber security roles, responsibilities, capability and capacity across the agency. Agencies must ensure they have access to the resources, skills and expertise required to deliver and sustain cyber security activities in alignment with their risk profile, business objectives and SACSf obligations.

The *SA Government Cyber Security Operating Model* (the Operating Model) provides the cyber security service catalogue and taxonomy that agencies can use to identify the cyber security services and activities required to support their CSP. The Operating Model should be used together with the *SA Government Cyber Security Workforce Guide* (the Workforce Guide) to determine the cyber security functions, workforce capability and organisational structures required to support the delivery of these activities.

The Workforce Guide provides detailed guidance on:

- Designing cyber security team structures.
- Identifying required cyber security functions and capability areas.
- Defining cyber security roles and responsibilities.
- Assessing workforce capability and capacity.
- Identifying workforce and skills gaps.
- Conducting training needs analyses.
- Developing workforce uplift and resourcing strategies.
- Building business cases for additional capability or capacity.

Once workforce requirements, roles and capability needs have been identified, agencies should document ownership and accountability arrangements for cyber security activities. The [Agency Cyber Security RACI Template](#) provides a structured

mechanism for assigning responsibility and accountability for agency cyber security services and activities based on the Operating Model. Agencies should tailor the template to reflect their organisational structure, service delivery arrangements and workforce model.

The Agency Cyber Security RACI Template should be used in conjunction with the Workforce Guide. While the Workforce Guide assists agencies in determining the workforce capability, capacity and organisational structures required to deliver cyber security services, the RACI template assists agencies in formally assigning ownership and accountability for those services and activities. Together, these artefacts help ensure that cyber security responsibilities are clearly defined, appropriately assigned and supported by personnel with the required skills, experience and authority.

Workforce capability and capacity requirements, together with associated responsibility assignments, should be reviewed periodically and whenever significant changes occur to the agency's risk profile, operating environment, organisational structure, technology landscape or CSP.

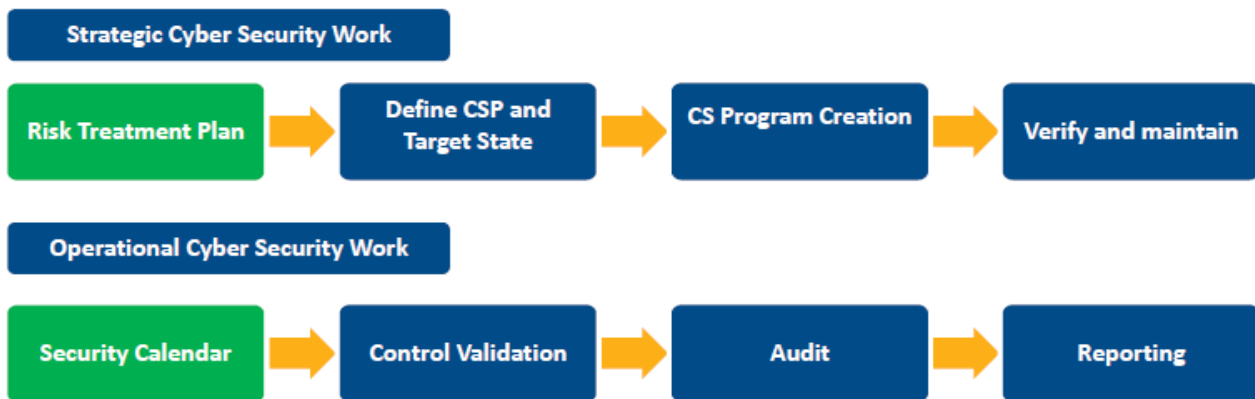
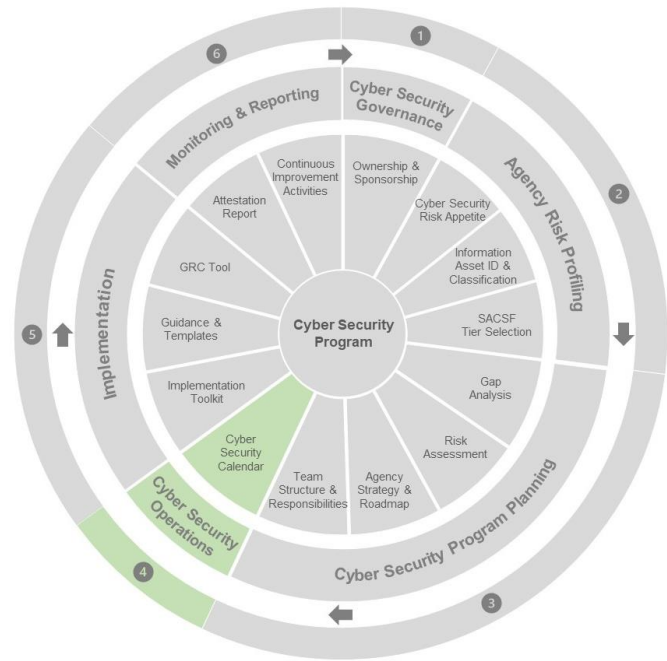
Related Guidance and Templates

- SA Government Operating Model (*SA Government agencies can contact cybersecurity@sa.gov.au for access*)
- SA Government Cyber Security Workforce Guide (*SA Government agencies can contact cybersecurity@sa.gov.au for access*)
- [TEMPLATE - Agency Cyber Security RACI](#)

5. Cyber Security Operations

Cyber security operations refer to the ongoing management of 'business as usual' (BAU) security activities. These are typically monitored through the agency's cyber security calendar.

These are activities that are already in place and monitored through reporting and are subject to continual improvement. This excludes projects or initiatives to implement new controls or enhance immature controls.



5.1 Cyber Security Calendar

As part of an agency's cyber security operations, a cyber security calendar (also referred to as an information security calendar, information assurance calendar or similar) should be developed to support ongoing operational tasks. This calendar will form a key component of the agency's annual attestation of its current alignment to the SACS.

The security calendar should be reviewed and updated by the security team to ensure:

- Cyber security activities are documented and assigned a task owner.
- Activities are scheduled as per the documented policies and procedures.
- Scheduled activities are completed as planned.
- Upcoming activities are confirmed, and resources identified, as necessary (e.g. if an external audit is required, this will need pre-planning).
- Any overdue activities are monitored or justified.

The calendar helps to map out the security team's schedule for the year, define resource requirements and highlight 'busy' periods for the team.

This should be reset and reviewed periodically to ensure it is achieving the desired outcomes for the CSP.

Step	Action
Review the security calendar	1. Review your existing security calendar against the documented policies and procedures and the SACSF requirements. The security calendar template includes recommended BAU activities. These activities need to align with the scope of responsibilities of the agency security team. 2. Update task owners and frequency, as necessary. 3. Update the planned dates for each activity. Note: This should be conducted at least annually.
Resources	Determine from the BAU activities whether the team has enough capacity to complete the activities when planned. • <i>Do you need additional resources?</i> • <i>Is this all the time or for specific periods / activities?</i> • <i>Do you have the required skill sets to complete the activities?</i> • <i>Do you need external support to complete the activities (e.g. audit)?</i>
Update the security strategy	Highlight resource requirements within the strategy (consider both competency and capacity requirements).
Maintenance	1. Maintain the security calendar during the working group meetings to determine BAU activities that: • Are coming up / due. • Require external resourcing (e.g. penetration testing / audit). • Are overdue. 2. Record decisions such as whether an activity can be deferred without impacting control assurance and confirm root cause for delays or cancelled activities. 3. On completion of new controls, add associated activities to the calendar, as necessary. The calendar can be monitored via MS Planner or MS List and be associated with a Power BI Dashboard.

Related Guidance and Templates

- [TEMPLATE - Security Calendar](#)

6. Implementation

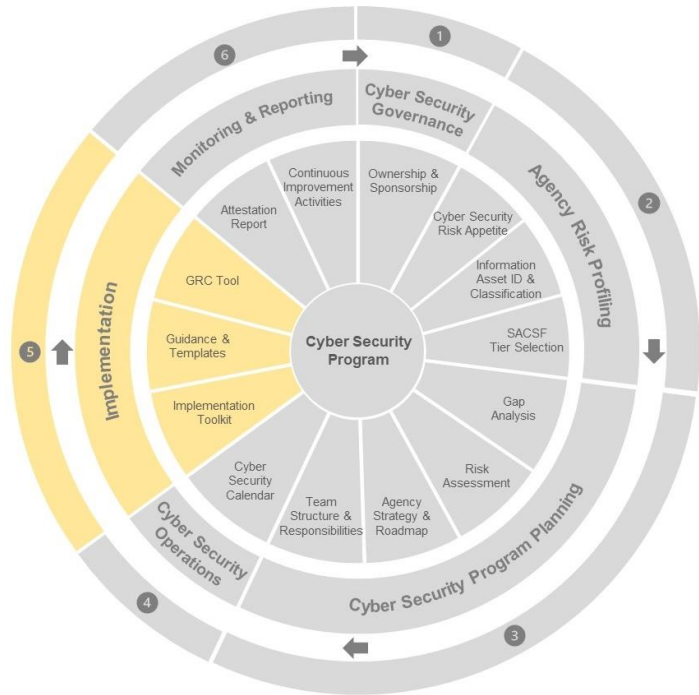
[Figure 2](#) provides a visual of how implementation of operational cyber security and security projects and initiatives come together.

The operational cyber security activities are guided by the cyber security calendar. This artefact defines the day-to-day activities that must be performed to support the CSP objectives. Control effectiveness is monitored via defined measures and metrics and some form of review. The results of these, along with any insight from observations, incidents or near misses and threat intelligence, are used to identify operational risks and issues which are then reported to appropriate roles for action and/or decision.

The agreed initiatives (or projects) are outlined within the work program and clearly define priorities to meet the CSP objectives over a defined period (usually 2-3 years). These projects / initiatives are prioritised based on:

- the approved Risk Treatment Plan (RTP).
- risk appetite.
- events / incidents.
- agency objectives.

Like any other project plan, these are also monitored and reported following the agency's governance structure. Any new implemented controls from these projects / initiatives are then moved over to the standard operations (under the cyber security calendar) when complete.



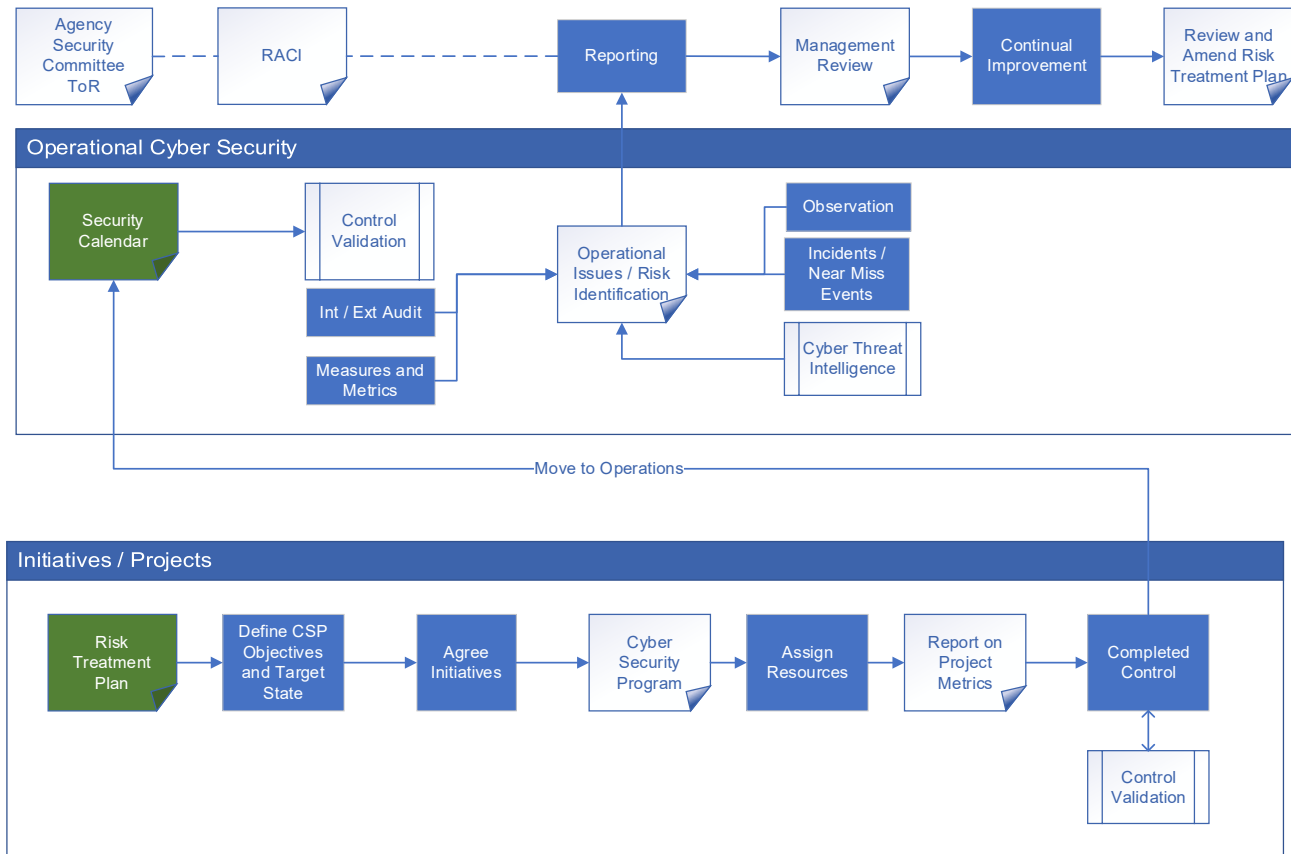


Figure 2. Link between operational security and initiatives / projects

OCIO under DTF provides various technology and cyber security services and solutions across the SA Government. Agencies can benefit from collaborating with OCIO to implement central services and solutions (refer to the [OCIO Service Catalogue](#)) to uplift their cyber security capability.

Part of OCIO's services is providing cyber risk advisory services to agencies on the interpretation and application of the SACSf requirements and the definition and implementation of a CSP. OCIO's Cyber Security Directorate provides the following resources to assist agencies to implement their CSP and the SACSf.

6.1 Implementation Toolkit

The [SACSf Implementation Toolkit](#) is an Excel workbook designed to analyse gaps in the agency's current cyber security practices with the risk tier level's requirements. It can also be used to monitor and report ongoing implementation status of initiatives and action plans to close the SACSf gap and key industry security standards.

6.2 Guidance and Templates

OCIO develops and publishes various guidelines, standards, rulings, and templates to assist agencies in implementing the SACSf.

- [SACSF Guidelines](#) provide more information on the application of the SACSF policy statements and requirements. They provide examples of best practice and can help an agency determine how best to implement controls and what actions are needed to manage risks.
- [SACSF Standards and Rulings](#) pertain to specific application of security policy that must be adhered to by all agencies.
- The CSP Guide (this document) is a supplement to the implementation approach described in the SACSF and is intended to provide agencies with additional information on the “what”, “why” and “how” of each stage in the implementation cycle.
- [Templates](#) are artefacts that provide a starting point for agencies to develop their own documents.

Related Guidance and Templates

- [SACSF Implementation Resources](#)

6.3 Governance, Risk and Compliance (GRC) Tool

A Governance, Risk and Compliance (GRC) tool is an effective way of simplifying the process of continuously identifying, assessing, and mitigating risks while ensuring compliance with policies, standards, and regulations. OCIO is seeking to deploy a cyber GRC tool across SA Government agencies to manage monitoring of whole-of-government cyber risks and reporting of compliance with the SACSF and other relevant industry standards.

7. Monitoring and Reporting

Regular monitoring and reporting are key to helping the agency continually improve its CSP. By reviewing progress against the strategy and the effectiveness of security measures, the agency can identify areas for improvement and adjust over time. This ensures the program stays aligned with the agency's needs, meets stakeholder expectations, and keeps pace with the ever-changing cyber risk landscape.

DTF through OCIO has its own objectives to obtain assurance from agencies that they are meeting the requirements of the SACSf. This is achieved through the annual attestation (as outlined below) which is consolidated with the attestation report for the SAPSF.

In addition to this, agencies must determine the needs of all stakeholders in terms of providing assurance and reporting against their security strategy and roadmap, and security operation activities. You can refer to the result of the stakeholders' needs analysis in [Section 2](#) of this document which should have identified the reporting needs of the agency security committee, senior leadership, audit and risk committee and other key internal and external stakeholders.

Through understanding the organisation's risk profile, critical assets and known risks, the agency should clearly define:

- What needs to be monitored and measured (processes and controls).
- The methods to be used for measures and metrics reporting.
- Schedule for measures and metrics reporting.
- When and how results are to be evaluated.

The outcomes of the measures and metrics are inputs into the continual improvement process (discussed below).

Performance of the CSP can be evaluated through the following:

Activity	Objective
Audit	To provide information on whether the CSP conforms to the agency's own requirements for cyber security and is effectively implemented and maintained.



Activity	Objective
	Agencies should seek to have their CSP included within the scope of the agency's internal audit program.
Capability maturity assessment	To provide an overview of the current maturity of implemented controls using an agreed Capability Maturity Model (CMM) as the benchmark.
Scheduled tests	To validate the effectiveness of key controls and identify any unknown vulnerabilities or gaps in its implementation.
Measures and metrics	To provide assurance through regular reporting to executive on the CSP objectives and key controls.
Management review	To ensure the whole strategy remains relevant and effective for the agency. A detailed review, at least annually, will bring together all the findings from audits, incidents, CMM, risk management, cyber threat intelligence, and measures and metrics to identify opportunities for improvement. The annual review should also include examining the CSP itself, with a review of the risk appetite statement, governance, roles, tiering, etc. It should report on the progress of the strategy and roadmap, and policy requirements implementation.

Related Guidance and Templates

- [TEMPLATE - Security Metrics Monitoring](#)
- [TEMPLATE - Cyber Security Management Report](#)
- [TEMPLATE - CSP Self-Assessment](#)

7.1 Annual Attestation

Each agency is to provide an annual attestation to DTF which details its current state of alignment to the SACSf, together with the plan to meet or maintain alignment to the requirements of the agency's selected tier level. Where agencies have implemented compensating controls in place of SACSf requirements, agencies must include these as part of their attestation.

It is expected that the attestation report is endorsed by the agency security committee, reviewed by senior leadership, and approved by the Chief Executive, however this may vary based on agency governance structure.

The annual attestation is currently managed through the iApply platform.

7.2 Continuous Improvement Activities

To complete the cycle, once a full management review has taken place the agency should:

- Revise / adapt the security strategy and work program.
- Make necessary changes to the CSP.

After making changes to the CSP or security strategy, monitor the results to ensure the implemented actions have effectively mitigated the identified risks or vulnerabilities. This follow-up ensures that adjustments have the desired impact.

The agency should respond to issues raised through audits, tests, the CMM or measures and metrics reports to:

- Take action and control the issue or vulnerability raised. This may lead to re-prioritisation of the initiatives within the security strategy and work program.
- Conduct a root cause analysis, if necessary, to understand the underlying factors contributing to the issue.
- Investigate whether similar gaps or vulnerabilities exist elsewhere or could arise in the future.

The agency should also:

- Ensure that all actions, changes, and improvements are documented and communicated to relevant stakeholders. This helps maintain transparency and accountability within the agency.
- Establish a formal feedback loop where insights from teams (e.g. IT, security, and operations) can continuously inform ongoing improvements. This ensures that practical experiences and challenges are captured and addressed.
- Regularly assess whether the agency's resources (budget, personnel, tools) are aligned with the current cyber security priorities. This can ensure that adequate resources are allocated to address identified gaps or risks.

Related Guidance and Templates

- [TEMPLATE - Security-Related Issues and Actions Register](#)

Appendix A: LIST OF RESOURCES

1. [Agency Security Committee Terms of Reference](#)
2. [Agency Security Working Group Terms of Reference](#)
3. [CSP RACI Matrix](#)
4. [Cyber Security Policy](#)
5. [CSP Stakeholder Requirements](#)
6. [Security-related Regulatory Legal and Contractual Requirements](#)
7. [Business Impact Analysis \(BIA\)](#)
8. [Cyber Security Risk Appetite Statement](#)
9. [Information Asset Classification Form](#)
10. [Information Asset Register](#)
11. Minute to CE for Tier Selection (SA Government agencies can contact cybersecurity@sa.gov.au for access)
12. [SACSF v2.0 Implementation Toolkit](#)
13. [Cyber Security Strategy and Roadmap](#)
14. [Cyber Security Work Program](#)
15. [Cyber Security Strategy on a page](#)
16. [Cyber Security Program Governance Framework](#)
17. SA Government Operating Model (SA Government agencies can contact cybersecurity@sa.gov.au for access)
18. SA Government Cyber Security Workforce Guide (SA Government agencies can contact cybersecurity@sa.gov.au for access)
19. [TEMPLATE - Agency Cyber Security RACI](#)
20. [Security Risk Assessment Report](#)
21. [Security Risk Register](#)
22. [Security Exemption Request Form](#)
23. [Security Exemption Register](#)
24. [Security Calendar](#)
25. [Security Metrics Monitoring](#)
26. [Cyber Security Management Report](#)
27. [CSP Self-Assessment](#)
28. [Security-Related Issues and Actions Register](#)

Appendix B: DEFINITIONS

Term	Definition
Agency	South Australian public sector agencies (as defined in section 3(1) of the Public Sector Act 2009 and any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to as 'Agencies').
Classification	The process by which information assets are labelled according to their business importance and sensitivity. Classification markings are used to indicate the value of the information.
Critical Process	Agency processes that, if not performed, would eventuate in the highest level of risk to the agency. This could include meeting critical needs of the agency or satisfying mandatory regulations and requirements.
Critical Service	Services that, if compromised, would result in significant damage to the physical, social, or economic wellbeing of the State. Critical services are not typically ICT services; they are services that an agency delivers to the community on behalf of the State.
Cyber Security	Measures relating to the confidentiality, availability and integrity of information that is processed, stored, and communicated by electronic or similar means (synonymous with ICT Security).
Cyber Security Program (CSP)	The agency's structured program for managing cyber security risks through governance, risk management, planning, implementation, monitoring, reporting and continuous improvement activities.
Exemption	Approval for exclusion from the implementation or use of a mandated document outlined in the South Australian Cyber Security Framework (SACSF).
Governance	System of decision-making, directing and controlling, through rules, relationships, policies, standards, systems, and processes.
Guideline	Additional, detailed advice on how to apply a policy. A statement of desired, good, or best practice.
Incident	Any event which is not part of the standard operation of a service, and which causes or may cause an

Term	Definition
	interruption to, or a reduction in, the quality of that service and/or loss or corruption of information resulting in a breach or privacy or security.
Information Assets	Any information or asset supporting the use of the information that has value to the agency, such as collections of data, processes, ICT, people, and physical documents.
Risk Appetite	The level of risk the agency is willing to accept. Agencies will need to define what level of management response is required for each risk level, for example: • Extreme/High Risk – Senior leadership response. • Moderate Risk – Agency Security Committee response. • Low Risk – Security management response.
Risk Assessment	A systematic process used to identify, analyse and evaluate cyber security risks and determine appropriate treatments.
Risk Profile	An outline of the risks to which an organisation, or business unit within an organisation, is exposed. Most risk profiles identify specific risks, associated mitigation strategies and an overall assessment or grading of each risk.
Risk Register	A repository used to record risks, owners, treatments, status and monitoring activities.
Agency Security Committee	A management group that acts as the coordinator and adviser for all security aspects in relation to the scope of the agency's Cyber Security Program and/or Security Plan.
Stakeholder Needs Analysis	An activity used to identify stakeholder cyber security requirements, expectations and opportunities for improvement.
Strategy	A long-term plan of action designed to achieve a particular goal.
Supplier	Suppliers are defined as any individual, contractor, business partner, or agent not directly employed by a South Australian Government agency.

Term	Definition
Third-Party Risk	Risk arising from suppliers, service providers or partner organisations that provide services or manage information assets for the agency.

Appendix C: ACRONYMS

Term	Definition
BIA	Business Impact Analysis
CISO	Chief Information Security Officer
CSP	Cyber Security Program
GRC	Governance, Risk and Compliance
ICT	Information and Communication Technology
ITSA	Information Technology Security Adviser
NIST	National Institute of Standards and Technology
PCI-DSS	Payment Card Industry Data Security Standard
PDCA	Plan-Do-Check-Act
SACSF	South Australian Cyber Security Framework
SAPSF	South Australian Protective Security Framework

Document Control

Objective ID	A7919331
Version	1.1
Approval by	Government Chief Information Security Officer
Approval date	15 September 2026
Next review date	September 2028
Contact	cybersecurity@sa.gov.au

Licensed under a [Creative Commons Attribution 4.0 International Licence \(CC BY 4.0\)](#), excluding the Government of South Australia brand, logos, and images. © Office of the Chief Information Officer, Department of Treasury and Finance, 2026.