

SACSF Guideline – Cyber security risk management

SACSF/G8.0

Across Government Guideline

Purpose

South Australian (SA) Government agencies are required to manage cyber security risks to reduce the likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes. Absolute security is unaffordable, often unachievable, and may impede business objectives and/or efficiencies.

Risk management forms an essential part of the South Australian Cyber Security Framework (SACSF), which was developed to standardise and guide the approach for establishing, implementing, maintaining and continually improving the cyber security posture of SA Government agencies.

Scope

The SACSF applies to SA public sector agencies (as defined in section 3(1) of the [Public Sector Act 2009](#)) and to any other person or organisation that is generally subject to the direction of a Minister of the Crown; all of which are referred to in this guideline as “Agencies”.

This guideline supports the implementation of the following SACSF policy statement:

- **SACSF Policy Statement 1.3 Risk Management** – The agency must take steps to identify, understand, assess and manage cyber security risks to its critical processes and information assets.

Cyber security risk management processes must be embedded within the agency's risk management framework and align to the risk appetite of the agency.

Senior leadership must be aware of current and emerging cyber security risks to the agency.

Guideline detail

Cyber security risk management is the processes that an agency undertakes to identify, understand, assess and manage risks to its critical processes and information assets. Cyber security risk management processes should be embedded within the agency's risk management framework and align to the risk appetite of the agency. Senior leadership should be aware of current and emerging cyber security risks to the agency.

Agencies should manage risks to reduce their likelihood and/or mitigate their business consequences, balancing the cost of security with its outcomes.

This guideline is a high-level overview of risk management, and how to apply it to cyber security within an agency.

The following processes should be in place within an agency to support cyber security risk management:

- Senior leadership has documented the agency's risk appetite.
- A risk management framework is in place and includes cyber security risk management processes.
- Cyber security risks are documented in an agency risk register or a cyber security risk management tool and are periodically reviewed by the Agency Security Committee.
- Cyber security risks are assessed and documented by suitably skilled personnel for all projects where cyber security risk exists.

Governance

Effective governance is important for strategic and operational risk management within the agency. The aim is not to eliminate risk, but to reduce or prepare for the uncertainty should it occur.

Agencies should incorporate cyber security risk management into their existing risk management framework or processes. Effective integration with organisation processes ensures that risk management protects and creates value.

Agencies should seek to embed risk management principles and practices into:

- organisational culture
- decision-making processes
- management of business information systems
- strategic and operational planning of programs, projects and activities
- anticipating and responding to changing social, environmental, and legislative conditions
- business, procurement and financial processes.

Risk management is designed to:

- identify potential events and risks that may significantly affect an agency's ability to achieve its strategic goals or maintain its operation
- assess and evaluate those risks against the agency's level of risk tolerance
- develop and implement controls to provide reasonable assurance that the organisational objectives will be achieved.

Cyber security risk management is applied to mitigate risks associated with the loss of confidentiality, integrity, and availability for critical information assets.

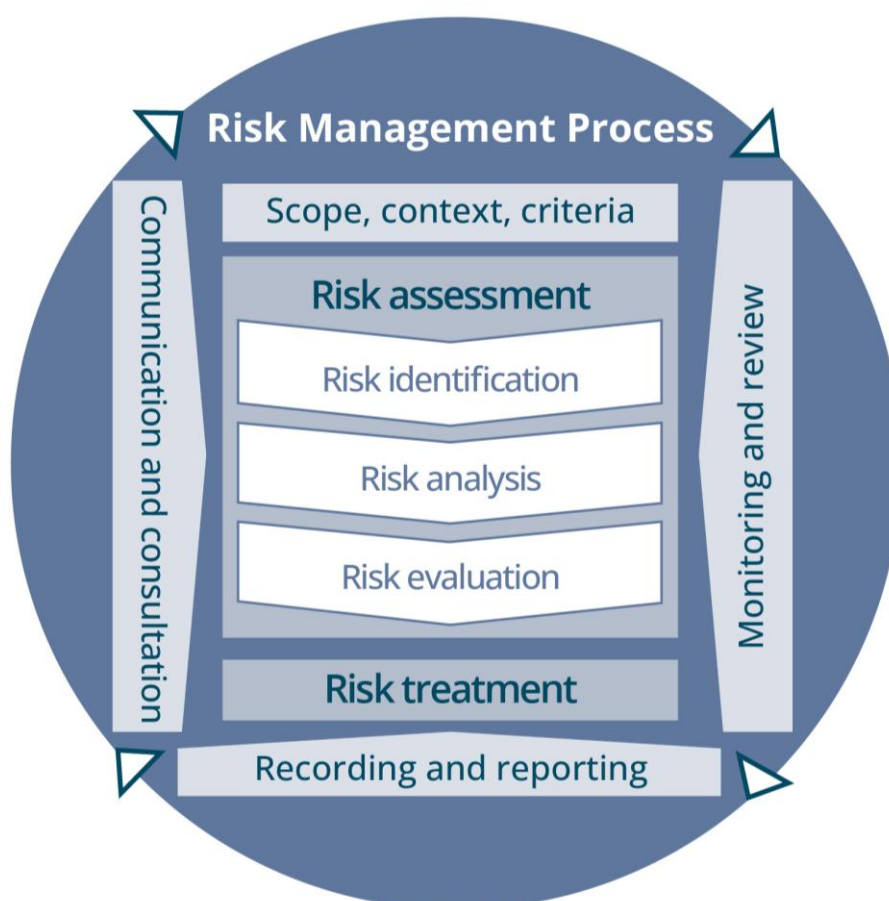
The senior leadership team within an agency is responsible for ensuring that risk management processes are in place (including those related to cyber security), risks and opportunities are assessed and evaluated, and actions are taken to address the risks.

Security risk management

Risk management follows a logical and systematic method for identifying, assessing, evaluating, treating, monitoring, and communicating risks associated with the information assets documented within the agency's information asset register.

ISO 31000:2018 Risk Management – Guidelines (ISO 31000) can be used as a standard approach to risk management, in the absence of an established risk management framework within the agency.

The key elements of the ISO 31000 risk management process are set out below.



Risk management is an iterative process which consists of steps to enable continual improvement in decision-making and the treatment of risk.

Risk management requires:

- establishing the business context within which risks are to be considered
- identifying and analysing risks
- evaluating whether the level of risk is tolerable or not

- identifying options for controlling and treating intolerable levels of risk.

Risk assessments

A risk assessment should be conducted systematically and collaboratively, drawing on the knowledge and views of personnel throughout the agency.

Effective risk assessment is a collaborative process involving senior management, the business/process owners and cyber risk practitioners.

Risk assessments are to be performed when significant changes occur to the agency or information assets within the scope of the agency's cyber security program. These significant changes may be the introduction or modification of assets including:

Asset	Description
Business processes and activities	Actions undertaken by an agency to deliver agency outcomes.
Information	Important information which is stored within business information systems that enable business processes and activities to deliver agency outcomes.
Systems and software	Information systems which support agency operations. For example, operating systems, applications, or cloud-based systems.
Hardware and infrastructure	Additional hardware and infrastructure which supports the operation of systems and software.
Sites and facilities	Physical locations where the agency undertakes or otherwise supports business operations.
Personnel	People who action and deliver on agency operations. These may be employees, contractors, volunteers, or external third-party providers.

Refer to the [Cyber Security Program Guide](#), [Security Risk Assessment Workshop Facilitation Guide](#) and [Security Risk Assessment Report](#) for more information on conducting risk assessments.

Risk analysis and evaluation

Cyber security risk analysis should be undertaken using the agency's risk management framework. Most risk management frameworks define a risk matrix that can be used to determine the severity of the impact of a risk by assessing the likelihood and consequence.

The risk level, or severity of the identified risk, can then be evaluated against the agency risk appetite to determine if it is tolerable or not, and determine the priority for any treatments.

Risk appetite

Risk appetite is the amount of risk that an agency is willing to accept in pursuit of its business objectives. The agency Chief Executive is required to approve the cyber security risk appetite statement for their agency. This statement defines, at a high level, the appetite that the agency has for cyber security risks.

Agencies need to define what level of management response is required for each risk before risk treatments are applied. The risk appetite may define that all risks below a certain level are tolerable, or that all above a certain level are unacceptable. Some agencies may also assign other management actions for risks at certain levels – for example, they may need to be reported to an executive or agency committee.

See the [Cyber Security Program Guide](#) for more information on how to define the agency security risk appetite.

Risk treatment

Risk treatment is the process of identifying options for treating intolerable risks, assessing the options for relative value, preparing risk treatment plans, and implementing and assessing the effectiveness of the risk treatment plans. If there is remaining residual risk following treatment, then it must be assessed to understand if it is an acceptable level of risk or not.

Risk treatment options may include:

- Reduce – a set of controls that will reduce the risk must be defined.
- Transfer – a plan to move or share the risk treatments and controls with another party or supplier (insurance, etc).
- Avoid – a description of how the risk will be avoided must be given – this usually refers to not undertaking the activity that the risk relates to.
- Accept – a reason should be given for accepting the risk, based on the agency's risk appetite.

The SACSF and supporting guidance may be used as a reference for controls to support cyber security risk treatment plans.

The treatment plans adopted should be documented and their implementation tracked. This monitoring process should exist in the agency, to provide executive oversight of actions taken and enable responsible parties to be held accountable for actioning the treatment of risks. Risk treatment plans should be implemented within a suitable timeframe determined by the risk rating.

A risk treatment plan (refer to the example in the [Security Risk Register template](#)) typically includes the following information:

- identified risk
- current risk level
- recommended treatment – a description of how the risk will be treated
- impact on risk – how the risk treatment will reduce the risk level
- target residual risk level – considering the expected change in likelihood and consequence
- risk treatment owner – assignee/s to own the risk treatment
- target date – date for the treatment to be in effect
- implementation status – not yet started, in progress, completed.

Documenting risks

Cyber security risks should be documented in a [risk register](#) that is regularly reviewed by the agency security committee and management.

Accepting risks

Once risk analysis is performed, risk levels, risk priorities, business impacts, treatment plans, and residual risks are summarised and provided to management for acceptance.

Acceptance of risk is based on a number of factors including the agency's security risk appetite, and whether the cost of mitigating the risk, or benefit of taking the risk, outweighs the potential negative impact.

The informed acceptance of risk supports decision-making for the agency. For this reason, it is important that stakeholders and decision makers are made aware of the nature and extent of any risk.

Accepted risks should be documented in a risk register that is monitored and reviewed regularly.

Monitoring risks

Once risks have been analysed and risk treatments have been accepted, the management of controls to treat the risk begins.

Management of implemented controls should include [regular monitoring](#) and review to assess the actual performance against required performance, enabling the agency to gauge the effectiveness and appropriateness of the risk management methodology.

Aboriginal Impact Statement

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

Related Documents

- [South Australian Cyber Security Framework \(SACSF\)](#)
- [South Australian Protective Security Framework \(SAPSF\)](#)
- [SACSF Cyber Security Program Guide](#)
- [SACSF Security Risk Register TEMPLATE](#)
- [SACSF Security Risk Assessment Report TEMPLATE](#)
- [SACSF Security Risk Assessment Workshop Facilitation Guide](#)

Document Control

Approved by	CIO Steering Committee	Version	1.1
Approved date	25 November 2025	Next review date	November 2027
Original date of approval	December 2022	Compliance	Optional
Contact	Office of the Chief Information Officer, Cyber Security Directorate		
Contact email	cybersecurity@sa.gov.au		

Licence



With the exception of the Government of South Australia brand, logos and any images, this work is licensed under a [Creative Commons Attribution \(CC BY\) 4.0 Licence](#). To attribute this material, cite the Office of the Chief Information Officer, Department of Treasury and Finance, Government of South Australia, 2025.