OFFICIAL

SACSF/G8.0

GOVERNMENT GUIDELINE ON CYBER SECURITY

SACSF Guideline 8.0 - Security risk management

Introduction

South Australian (SA) Government agencies are required to manage risk 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.

Security 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.

Applicability

This guideline applies to:

- all SA Government agencies and personnel operating on behalf of the agencies.

Scope

Manage security risks and support a positive security culture, ensuring clear lines of accountability, strategic planning, assurance and review, and proportionate reporting.

Risk management is the process that an agency must take 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.

Risk management is covered under the 21 policy statements that underpin the principles of: Governance, Information, Personnel and Physical. This guideline may be used by agencies without existing risk management frameworks in place. The guideline is a high-level overview of risk management, and how to apply it to cyber security within an agency.

The SACSF policy statement in line with this guideline is:

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.

Expectations

In order to assist with implementation of the SACSF, each of the 21 policy statements are listed along with tier specific expectations and guidance. Under the set of supporting expectations set in Policy Statement 1.3: Risk Management, the following should be used in the process to support cyber security risk management processes;

- 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; and are periodically reviewed by the Agency Security Committee.
- Cyber security risks are assessed and documented for all projects undertaken by the agency
- Cyber security risks are documented in a cyber security risk management tool maintained by security personnel and periodically reviewed by the Agency Security Committee.

Considerations

Cyber security is founded on risk management. Agencies should manage risk to reduce their 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. Agencies are to identify and evaluate their cyber security risks and determine the required risk treatment activities in line with business requirements.

Good 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 be committed to embedding risk management principles and practices into:

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

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

OFFICIAL

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 agencies level of risk tolerance
- develop and implement controls to provide reasonable assurance that the organisational objectives will be achieved.

The senior leadership team within an agency is responsible for ensuring that all 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.

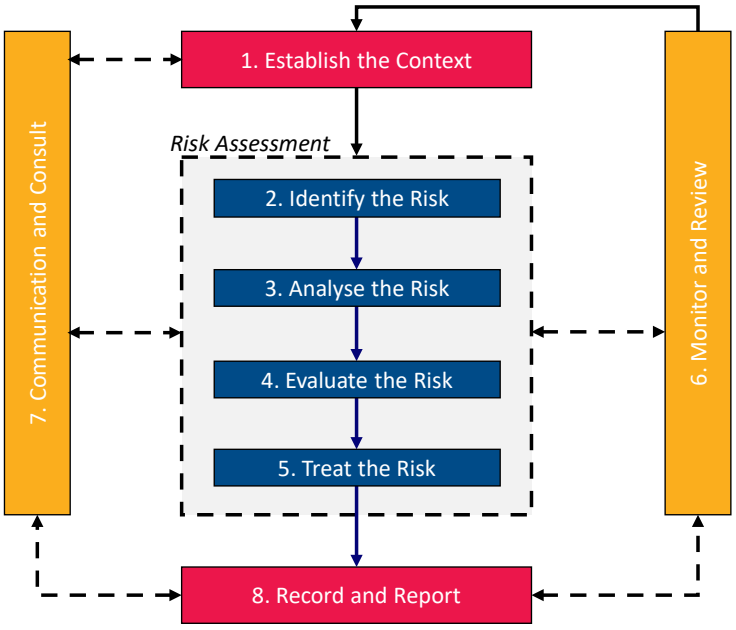
Agencies should consider incorporating cyber security risks into their existing risk management framework or processes. Effective integration with organisation processes ensures that risk management protects and creates value.

Risk management

Risk management follows a logical and systematic method for assessing, 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.

OFFICIAL

These steps include identifying, analysing, evaluating, treating, monitoring and communicating risks associated with an activity, function or process in a way that would better prepare an agency for unexpected business impacts should the risk eventuate.

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 acceptable or not
- identifying options for controlling and treating unacceptable levels of risk.

Security risk assessments are required before the implementation of a new service or system and when major changes occur.

Risk assessments

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

Effective risk identification 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 CSP. 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 enabled business processes and activities to deliver agency outcomes.
Systems and software	Information systems which support agency operations. This may be cloud based systems, servers or computers.
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 or external third party providers.

OFFICIAL

Refer to the *Security Risk Assessment Workshop Facilitation Guide* in Security SA for more information, including questions to ask when assessing risks and the role of the workshop facilitator.

Risk types and treatment

- An **uncontrolled risk** is one that has been identified and not yet treated.
- A **residual risk** is one which remains after treatments have been applied.

Risk treatment involves identifying the range of options for treating intolerable risks, assessing options for treatment, preparing risk treatment plans, and implementing such plans. Risk treatment options may include:

- Accept – a reason should be given for accepting the risk, based on the agency's risk appetite.
- 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 a third party supplier (insurance, etc.).
- Avoid – a description of how the risk will be avoided must be given.

The SACSF and supporting guidance may be used as an initial reference for the mitigation of cyber risks.

The treatment plans adopted should be documented and their implementation tracked as part of the corrective actions process (refer to the example Security Risk Assessment). This corrective action 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.

Accepting risks

Once risk analysis is performed, risk priorities, consequences, actions, plans, uncontrolled risks 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.

It is important that stakeholders and decision makers are made aware of the nature and extent of any risk. Risks should be documented in a Risk Register that is monitored and reviewed regularly.

Controlling risks

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

These controls take the form of regular monitoring and review to access the actual performance against required performance, enabling the agency to gauge the effectiveness and appropriateness of the risk management methodology.

A treatment plan (refer to the example in Appendix C of the SACSF Guideline 8.0 Security risk management) typically includes the following information about the control measures:

- identified vulnerability - a description of the risk
- current risk rating - uncontrolled
- recommended treatment – a description of how the risk will be treated
- owner – assignee/s to own the risk treatment
- target date – date for the treatment to be in effect
- implemented treatment – description of the risk treatment once implemented
- status – not yet started, in progress, completed
- revised residual rating – updated once the risk has been treated.

Documenting risks

Risks should be documented in a risk register that is regularly reviewed by the agency security committee and management.

Aligning risk management to 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 will need to define what level of management response is required for each risk before and after risk treatments are applied. This is based on the risk appetite, which is further aligned by the level of risk the agency is willing to accept under the SACSF Tier selection.

References, links and additional information

- South Australian Cyber Security Framework (SACSF)
- South Australian Protective Security Framework (SAPSF) Executive Guide
- Security Risk Assessment Workshop Facilitation guide
- Security Risk Assessment template
- ISO 31000:2018 Risk Management – Guidelines
- StateNet Conditions of Connection (SCoC)
- SA Government Risk Management Guide

OFFICIAL

Document control

ID	SACSF/G8.0
Version	1.0
Classification/DLM	OFFICIAL
Compliance	Discretionary
Original authorisation date	December 2022
Last approval date	December 2022
Next review date	December 2023