South Australian Protective Security Framework

GOVSEC3:

Security monitoring

OFFICIAL

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Contents

PURPOSE **3**

CORE REQUIREMENT 3 ..... **3**

SUPPORTING REQUIREMENTS **3**

TERMINOLOGY **4**

DEFINITIONS **4**

ACRONYMS **5**

GUIDANCE **6**

SECURITY MATURITY 6

Security culture *6*

MONITORING SECURITY MATURITY 6

Gathering evidence of security maturity *6*

Assessing progress to security goals and maturity targets *7*

Amending the security plan *7*

DOCUMENT CONTROL **7**

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Purpose

1. Security maturity is a meaningful way of measuring an agency's overall security capability in line with the risk environment and the agency's risk tolerances. Maturity recognises the inherent differences between agencies, functions, risk environments and security risks, and acknowledges the journey agencies may need to take to achieve their security goals and objectives, while helping to identify areas for improvement.
2. This policy ensures that agencies develop and implement processes to routinely monitor and assess their security maturity in line with the security goals of their security plan. An agency's security maturity includes the ability to actively respond to changes in the agency's security risk environment, including to new and emerging threats or vulnerabilities, to ensure the ongoing protection of its people, information and assets.

Core Requirement 3

Monitor security maturity against the security plan

Supporting Requirements

3. To monitor security maturity against the security plan, agencies[1] must:

   I. seek, identify and document evidence of the agency's security maturity

   II. assess progress to achieving the security goals and maturity targets of the security plan

   III. amend the security plan in accordance with changes to the risks, threats, vulnerabilities or criticalities of the agency

[1] This policy applies to all South Australian 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 policy as "Agencies".

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Terminology

Term	Meaning
MUST	Use of the word **must** (or **required** or **responsible for**) indicates a requirement or action of the policy to which all agencies must adhere or undertake
MUST NOT	Use of the words **must not** indicates an action prohibited by this policy
SHOULD	Use of the word **should** (or **recommended**) indicates an action that agencies ought to undertake, unless prevented by legitimate circumstances or justification
SHOULD NOT	Use of the words **should not** (or **not recommended**) indicates an action which agencies should avoid, unless legitimate circumstances prevent another course of action being taken
MAY	Use of the word **may** indicates an action which is completely optional, but may be provided as a suggestion or considered best practice

Definitions

Term	Definition
agency	as per the definition of *public sector agency* (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 policy as “Agencies”.
controls	see **risk treatment**
employee	see **personnel**
function	the purpose or role an agency undertakes on behalf of the Government of South Australia
mitigation	see **risk treatment**
personnel	all people that an agency employs (including contracted employees)
protection	the treatments, mitigations or controls implemented to prevent or minimise the likelihood, of compromise to an agency’s people, information or assets
resources	an agency’s people, information and assets
risk tolerance	the amount of level of risk an agency is comfortable taking after risk treatments have been applied to achieve and objective or manage a security risk
risk treatment	considered, coordinated and efficient actions and resources that mitigate or lessen the likelihood or negative consequences of a security risk
security maturity	a measure of an agency’s security capability within its risk environment and risk tolerances, while acknowledging progression toward security outcomes
security plan	how an agency articulates how its security risks have been identified, prioritised and will be managed in line with the agency’s objectives
security risk	something that can result in compromise, loss, unavailability or damage to an agency’s resources, including causing harm to people.
shared risk	security risks that extend across multiple agencies and/or their premises, that impact the community, industry and international or interstate jurisdictions or partners

Term	Definition
threat	a declared intent to inflict harm on personnel or property
vulnerability	the degree of susceptibility and resilience of an agency to risks and threats

Acronyms

Acronym	Words
SAPSF	South Australian Protective Security Framework

SOUTH AUSTRALIAN PROTECTIVE SECURITY FRAMEWORK

Guidance

Security maturity

4. Security maturity is measure of an agency's capability to identify, assess and treat security risks specific to its risk environment and risk tolerances. Effective security maturity assessments identify the success of SAPSF implementation as well as areas requiring improvement.
5. Security maturity is a reflection of how an agency:
    a. implements and meets the SAPSF core and supporting requirements
    b. minimises harm to its people and assets
    c. fosters a positive security culture
    d. responds to and learns from security incidents
    e. understands and manages security risks
    f. achieves security outcomes while delivering business objectives.

Security culture

6. A positive security culture is an effective measure of an agency's security maturity. It is reflective of the behaviours, attitudes and understanding of security by an agency's employees and underpins the agency's ability to identify, manage and treat security risks effectively. The importance of security culture is reflected in SAPSF principle 5 *'a positive security culture empowers personal accountability, promotes ownership and management of risk and supports continuous improvement'.*
7. It **should** be an objective of all agencies to develop a security culture where leadership and employees:
    a. comprehensively understand the agency's security risks
    b. understand their collective and individual security responsibilities
    c. proactively manage the security risks relevant to their work environment
    d. embed good security practices in their day-to-day activities
    e. use risk management to inform decision that might affect the agency's security
    f. promote good security practices both internally and externally of the agency.

Monitoring security maturity

Gathering evidence of security maturity

8. Security maturity can be highly subjective and difficult to compare across business units, let alone agencies of varied size and function, so what information is required to assist in assessing an agency's maturity may not be obvious or evident. Therefore, when setting security goals and maturity targets, agencies **must** seek, identify and document evidence which supports the agency's present security maturity assessment.
9. This information can then be utilised to inform ongoing assessments and contribute to identifying new sources of information to further enhance and enrich maturity assessments.
10. Information which can contribute to security maturity assessments and monitoring **may** include:
    a. engagement with, and decisions on, security risk and risk tolerances
    b. risk mitigation strategies
    c. frequency and/or response to security incidents (including learnings)
    d. employee security behaviours (including security incidents)

e. security training programs
f. systematic and routine audits of security practices/procedures (including access controls)
g. security issues reported (internally or externally)
h. internal focus groups or security questionnaires
i. horizon scanning for emerging or evolving threats, risks and vulnerabilities
j. provision of security advice or services (for Lead Security Agencies)

Assessing progress to security goals and maturity targets

11. The information collected can then be used to validate the maturity level of the agency and determine progress toward the maturity targets identified in the security plan. Agencies **should** use the maturity level indicators described in SAPSF policy Security planning (see **Annex A**) to guide planning and assessment of maturity.

Amending the security plan

12. Security plans are only **required to** be reviewed every two years, however, changes in the risks, threats, vulnerabilities or capabilities of an agency **may** mean the security plan, or parts of the security plan, are no longer accurate or fit for purpose.

13. Agencies **must** consider amendments to their security plan where:

a. new or changing risks, threats, vulnerabilities or capabilities are identified (including shared risks)
b. significant discrepancies are identified between assessed and actual security maturity
c. the agency's risk tolerance changes
d. the agency's function changes significantly (e.g. machinery of government changes).

Document control

Approved by: Jim McDowell	Title: Chief Executive, Department of the Premier and Cabinet
Contact person: James Doherty	Telephone: 0447 180 915
Division: Security and Emergency Management, Intergovernmental and Diplomatic Relations	Date of approval: 20 April 2020
Revision number: 1.1	Date of review: 21 August 2020
Next review date: December 2021	

Change log

1.0	20/04/2020		First issue of policy
1.1	21/08/2020	-	Definition of 'personnel' added.