South Australian Protective Security Framework

GOVSEC3 SECURITY MONITORING

SOUTH AUSTRALIA

Government of South Australia

CONTENTS

GOVSEC3: SECURITY MONITORING

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, agencies must:[1]

    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".

GUIDANCE

SECURITY MATURITY

5. 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 South Australian Protective Security Framework (SAPSF) implementation as well as areas requiring improvement.

6. 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

7. 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*'.

8. 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

9. 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.

10. 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.

11. 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

12. 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

13. 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.

14. 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: Chief Executive, Department of the Premier and Cabinet	Date of first approval: 20 April 2020
Revision number: 2.0	Date of review: 26 October 2022
Next review date: December 2024	Contact: sapsf@sa.gov.au

CHANGE LOG

Version	Date	Changes
1.0	20/04/2020	- First issue of policy
1.1	21/08/2020	- Definition of 'personnel' added
2.0	30/11/2022	- Policy reviewed, no change
2.1	19/07/2024	- Minor formatting updates

For more information:

National and Protective Security
Security, Emergency & Recovery Management
Social Policy and Intergovernmental Relations
Department of the Premier and Cabinet

E SAPSF@sa.gov.au

W security.sa.gov.au

SOUTH AUSTRALIA

Government of South Australia