South Australian Protective Security Framework

# GOVSEC 2

## SECURITY PLANNING

SOUTH AUSTRALIA

Government of South Australia

# Contents

Policy ..... 3
Purpose ..... 3
Core Requirement ..... 3
Supporting Requirements ..... 3
Guidance ..... 4
Security planning ..... 4
The security plan ..... 4
Supporting Security Plans ..... 5
Setting security goals and strategic objectives ..... 6
Security maturity ..... 6
SAPSF security roadmap ..... 7
Risk-based security practices ..... 7
Risk appetite ..... 7
Risk tolerance ..... 7
Identifying security risks ..... 8
Security risk assessments ..... 8
Threat assessments ..... 8
Vulnerability assessments ..... 8
Criticality assessments ..... 9
Analysing security risks ..... 9
Evaluating security risks ..... 9
Shared risks ..... 9
Planning and implementing risk treatments ..... 10
Treatment plans ..... 10
Risk, treatment strategies ..... 10
Implementing treatments ..... 11
Scalable measures ..... 11
Security alert levels ..... 12
Identifying risk managers ..... 13
Deviating from the security plan or SAPSF requirements ..... 13
Reviewing the security plan ..... 13
Document control ..... 15
Change Log ..... 15

# POLICY

## PURPOSE

1. Good security planning will assist agencies to identify and manage security risks while maintaining the continuous delivery of efficient and effective government services. This policy describes how agencies can effectively manage security risks through planning and embedding security into risk management practices and procedures.
2. Security planning through risk management processes enables agencies to prioritise the most critical risks, set protective security targets, adjust objectives based on changes to the risk environment, improve agency resilience to threats and overall protective security maturity.

## CORE REQUIREMENT

**Maintain a security plan[1] to manage security risks**

## SUPPORTING REQUIREMENTS

3. To establish a security plan that manages security risks, agencies[2] must:
    I. determine the agency's security goals and strategic objectives
    II. determine the risk tolerance for the agency
    III. identify the agency's security risks, including shared risks
    IV. plan and implement treatments to manage agency security risks
    V. identify a risk manager to be responsible for each security risk, or category of security risk
    VI. document any decisions to deviate from the security plan, including justifications and alternative treatments implemented
    VII. review the security plan (and any supporting security plans) at least every two years for:
        a. the adequacy of existing security arrangements and risk treatments
        b. significant changes to the risk environment or tolerance

[1] Where a single security plan is not practicable due to the agency's size or complexity of business, the accountable authority may approve a single, strategic-level overarching security plan that addresses the core requirements of the SAPSF, which is then supported by other more details plans (supporting security plans).

[2] 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 PLANNING

4. To be successful at managing security risks, an agency needs to know what the threats are, what resources need protecting and how they will be protected.
5. Security planning is using sound risk management processes to design, implement, monitor and review an agency's protective security arrangements to ensure efficient and effective delivery of government services. All security planning should be based upon achieving a cycle of continuous improvement.

## THE SECURITY PLAN

6. All agencies must develop a security plan which outlines the approach, responsibilities and resources applied to managing protective security risks in line with the core and supporting requirements of the SAPSF. A security plan enables agencies to review strategic and operational risks and implement the appropriate treatments that manage those risks to an acceptable level.
7. The agency's accountable authority is responsible for their agency's security plan, supported by the Agency Security Executive (ASE).
8. The security plan must take a risk-management approach to protective security and address threats, risks and vulnerabilities across all areas of security in the agency (governance, information, personnel and physical).
9. A risk-management approach means making informed decisions about how to implement the core and supporting requirements of the SAPSF, and includes:
    I. undertaking structured risk assessments to identify, analyse and prioritise security risks
    II. implementing risk treatments that are considered and coordinated and that involve the efficient and effective use of resources to mitigate security risks
10. Irrespective of an agency's function, size or risk environment, the foundation for managing security risks must be the principles of the SAPSF.
11. Every agency's security plan will, and should, be different. The plan must reflect the agency's protective security requirements in line with the risks that agency faces. As an agency of the South Australian Government, how risks are managed can have broader implications for other agencies or the government generally.
12. Security plans should be developed by a person(s) who has a sound understanding of the agency's strategic objectives and an appropriate level of security risk management knowledge and expertise.
13. Security plans should be made available across the agency as it helps to build security culture and awareness through common understanding, particularly for those with obligations or responsibilities outlined under the plan.
14. **Table 1 – Recommended structure and content coverage of a security plan** provides an overview of the recommended structure and content coverage of a security plan. Agencies should align their security plan to the core and supporting requirements of the SAPSF. An example template security plan is available in the Security SA MS Teams site.

**Table 1 – Recommended structure and content coverage of a security plan**

| Section of the Plan | Recommended Content Coverage |
|---|---|
| **Security goals and strategic objectives** | The accountable authorities approach and commitment to effective security risk management of the agency, its security priorities, goals and objectives and the development and promotion of a positive security culture |
| **Security risk environment** | The agency's security risk environment in which it operates and the security risks to the agency. Understanding of what resources (people, information, assets) the agency needs to protect, what it needs to protect those resources from, and how those risks will be managed in the agency |
| **Risk tolerance** | The agency's level of risk tolerance determined by the level of potential damage to the agency or the South Australian Government |
| **Security capability and maturity** | What the level of security maturity in the agency is, and what capabilities it has in place to deliver against its security goals and objectives |
| **Security risk management and treatment strategies** | What the strategies are to manage risk and implement treatments in the agency, how these treatments keep risk within tolerances and how security risks are monitored, managed and reviewed. |
| **Supporting and evidentiary documents** | Agencies should consider if any evidentiary documents are needed to establish an effective and comprehensive security plan. Examples include:<br>• supporting security plans<br>• security risks assessment reports<br>• security alert levels<br>• threat assessments<br>• site security plans<br>• vulnerability assessments<br>• agency specific security procedures<br>• security risk register<br>• agency security maturity monitoring<br>• critical asset register<br>• security incident register/response procedure<br>• privacy impact assessments<br>• ICT system security plans (see SACSF)<br>• information asset register<br>• other agency operational or compliance plans |

.

## SUPPORTING SECURITY PLANS

15. Supporting security plans may be appropriate where an agency's size or complexity of business makes a single security plan impractical or inappropriate. In such circumstances, the accountable authority may determine that supporting security plans are needed to address the complexity of the agency's business, including where an agency operates over multiple locations or has multiple distinct functions which have unique or varying security risk profiles.

16. Supporting security plans should cover the same content and structure as security plans described in this policy.

## SETTING SECURITY GOALS AND STRATEGIC OBJECTIVES

17. The security arrangements of an agency must support and be reflective of the agency's strategic objectives by reflecting the risks that would impact upon those objectives being achieved.
18. The accountable authority, with support from the ASE, must establish clear security goals that support both the strategic objectives of the agency and the requirements of the SAPSF, and reflect those goals in the agency's security plan.

## SECURITY MATURITY

19. 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.
20. The security maturity of an agency can be measured by how it:
    I. understands, prioritises and manages its security risks
    II. responds to and learns from security incidents
    III. fosters a positive security culture
    IV. achieves security outcomes and core requirements while delivering business outcomes.
21. It is recommended that agencies consider and develop their security maturity monitoring plans as part of the agency's security plan to support SAPSF policy Security monitoring.
22. **Table 2 – SAPSF maturity** lists the four maturity levels under the SAPSF which agencies should use to help set security goals and inform risk management decisions. See Annex A for guidance on how to assess current security maturity levels to inform maturity targets for the future.

**Table 2 – SAPSF maturity levels**

| Maturity levels | Definition | Target |
|---|---|---|
| **1 Informal** | Security is ad-hoc, unmanaged and unpredictable. Security success relies on individuals rather than effective processes. | Not recommended as a maturity target as it reflects a lack of capability maturity |
| **2 Basic** | Policies and processes are in place to meet the core and supporting requirements of the SAPSF, but security management is mainly reactive and inconsistent. | This level is reflective of developing capability maturity and may be appropriate as a stepping-stone to a higher maturity target |
| **3 Managed** | Security of the agency is risk-based, fit-for-purpose measure are in place, understood and consistently followed. Ongoing investment is required to sustain measures at this level. | Managed is considered the effective implementation of the SAPSF core and supporting requirements. |
| **4** | Security capability is adaptable to a dynamic, high-risk operating environment. | Target should be selected if risks identified require enhanced security measures. |

| | | |
|---|---|---|
| **Enhanced** | Security culture is embedded and security goals and objectives are consistently exceeded. | |

## SAPSF SECURITY ROADMAP

23. It is recommended that agencies use the SAPSF Security Roadmap (found in the Security SA MS Teams site) when assessing their security maturity. The roadmap enables agencies to consolidate all the relevant information into a single document that can then be used as the basis for completing the annual security attestation (see SAPSF policy Annual security attestation).

# RISK-BASED SECURITY PRACTICES

24. The existence of risk in and of itself is not an inhibitor to achieving the objectives of the agency or the government generally, but it must be managed. Agency security should follow a risk-based approach through identifying and understanding the highest areas of risk and taking the appropriate mitigation measures in accordance with the risk appetite and tolerance

25. The accountable authority is responsible for determining and managing their agency's security risks, which includes determining the agency's risk appetite and risk tolerances (see SAPSF policy Security governance).

## RISK APPETITE

26. In basic terms, *risk appetite* reflects an agency's attitude to risk, and how much risk the agency is willing to accept and is expressed in the form of high-level, qualitative statements, or similar. Risk appetite is established through careful consideration of an agency's function, objectives, resources, the risk environment and the accountable authority's approach to risk and security.

27. Correctly defined, approached and implemented, risk appetite should help to set the business and strategic objectives of an agency.

28. Establishing an agency's risk appetite **should** help build the agency's overall boundary for risk (risk capacity) and help to set expectations by informing agency staff, external stakeholders or parties of the risk posture of the agency. Without a defined risk appetite, an agency cannot determine its risk tolerances.

## RISK TOLERANCE

29. *Risk tolerance* is an informed decision to accept risk after risk treatments have been applied. Although agencies **must** endeavour to minimise their levels of risk as low as is reasonable, risk tolerance allows for the practical application of risk appetite and can lead to innovative business practices and positive business outcomes.

30. The agency's risk tolerance **must** include:

    I. the expectations for mitigating, accepting and pursuing specific types of risk

    II. boundaries and thresholds for acceptable risk taking (measurable operational limits)

    III. actions to be taken or consequences for exceeding approved tolerances.

31. The risk tolerance **should** take into account changes in the risk environment and changes to the accountable authority's or broader government's objectives or risk appetite. Risk tolerance is often specified for relevant risks, and can be expressed as

'acceptable', 'tolerable' or 'unacceptable' levels and is subject to measuring and monitoring.

# IDENTIFYING SECURITY RISKS

## SECURITY RISK ASSESSMENTS

32. People, information and assets (including ICT) require protections to ensure the ongoing operation of an agency and to protect state and national interests.

33. A security risk (including shared risk) can result in compromise, loss, unavailability or damage to an agency's resources, including causing harm to people. Security risk is the effect [3] of uncertainty on the agency's objectives and is measured in terms of the chance of the risk event occurring (likelihood) and the outcomes if the risk event occurs (consequence).

34. Security risk assessments create a clear, comprehensive and concise list of potential sources of risks, threats, vulnerabilities or criticalities to the agency and its ability to deliver its core function for government. When determining what risks, threats, vulnerabilities or criticalities could affect the agency or resources, agencies should consider:

    I. what could happen? (potential event or incident and resulting outcomes or consequences)

    II. what is the likely outcome and impact if it does happen?

    III. how likely is it to happen? (frequency)

    IV. where could it happen? (location and assets affected)

    V. what could make it happen? (sources, potential threats, triggers, catalysts)

    VI. do we need more information to properly assess this risk?

    VII. why could it happen? (vulnerabilities, gaps, inadequate arrangements)

    VIII. who could be affected? (individuals or groups, stakeholders, service providers)

    IX. does mitigating this risk create other risks to clients or the public?

35. It is not consistent with this policy to intentionally lower the likelihood or consequence in order to produce a lower risk level.

## THREAT ASSESSMENTS

36. A threat assessment identifies where the threats to an agency, or its resources, come from, and considers the likelihood that threat will eventuate. The level of threat is a combination of the intent and capability to cause harm or damage. Threats can be either malicious or accidental.

## VULNERABILITY ASSESSMENTS

37. A vulnerability assessment identifies how likely an agency, or its resources, are to be impacted by the identified risks. Understanding the vulnerability of the agency to risk

[3] The effects of a security risk result in a deviation from what is expected, or planned, and can be either positive or negative.

informs the likelihood and consequence of those risks. Vulnerability **should** be used to help prioritise risks and develop treatments.

## CRITICALITY ASSESSMENTS

38. The criticality of a resource reflects how important that resource is to the agency's operations. The resources in an agency which are critical to its operation **should** have the greatest protections assigned to them.

39. A criticality assessment will depend upon the agency's function, business objectives and risk environment. Typically, a criticality assessment includes:

    - criticality ratings – a measure of the importance to the agency (e.g. numerical scale, importance value scale or business impact level (BIL))
    - consequence of compromise – what could happen
    - category – what part of the agency or business would this impact? (e.g. employees, financial)

## ANALYSING SECURITY RISKS

40. Once the agency's security risks have been identified, an assessment can be undertaken to determine if existing security controls or risk treatments are adequate.

41. Risks **should** be defined in terms of likelihood and consequence to produce a risk rating, which is then used to assist in prioritising the risks in descending order. It is **recommended** that agencies adopt a risk rating-matrix approach to determining the levels or risk which aligns to agency risk tolerances.

## EVALUATING SECURITY RISKS

42. Following analysis, security risks **must** be evaluated to work out if those risks are acceptable (tolerable, within existing controls) or unacceptable (intolerable, in need of additional treatments or prohibited). See paragraph 29. Risk tolerance for more information.

## SHARED RISKS

43. Shared security risks are those that emerge from a single source and extend across multiple agencies and/or their premises, the community, industry and international or interstate jurisdictions or partners. Shared security risks require a high-level of cooperation and communication between agency stakeholders to be effectively understood and managed.[4]

44. It is **recommended** that agencies with shared tenancies or facilities conduct risk assessments to evaluate the security risks for the co-tenancy and apply appropriate security treatments to address the combined risks.

45. If an agency assesses a security risk is, or needs to be shared due to its location (e.g. physical boundaries, shared public spaces, government precincts), it **should** identify and engage with any other agencies or entities it deems are affected by the security risk, and coordinate any risk treatment accordingly.

46. If no other party with whom the security risk can be shared can be reasonable identified, the agency **must** mitigate the security risk to the extent it is able to within its function and operations.

[4] For more information on managing shared risks, see the Commonwealth Risk Management Policy Understanding and managing shared risks information sheet.

47. With complex shared risks, flexible governance arrangements may need to be agreed. In such cases, agencies **should** agree a set of mutual and possibly distributed responsibilities to ensure mutual understanding, resourcing and assurance mechanisms are created from the outset.
48. If agencies with shared security risks have different tolerances for the risk, it is **recommended** that all parties identify the areas of difference and if additional treatments can be implemented to alleviate any concerns.
49. All roles and responsibilities for shared risks **must** be clearly defined to reduce the likelihood that a security risk is neglected or overlooked. It is **recommended** that agencies negotiate an appropriate risk manager for all shared risks.

# PLANNING AND IMPLEMENTING RISK TREATMENTS

50. Risk treatments are the controls or mitigations put in place to reduce or manage the security risks an agency has identified to within the agency risk tolerance levels. Risk treatments can be applied separately or in combination with other treatments to achieve a desired result.
51. Agencies **should** balance the cost and effort of implementing treatments against the expected benefits to ensure that the treatment is proportional to the risk rating (see 40. Analysing security risks). It **may not** be possible or cost-effective to implement all possible risk treatments, however, agencies **must** prioritise and implement the most appropriate or effective treatments.
52. The Australian Standards HB 167: Security Risk Management provides a six-step process for treating risks that entails:
    I. prioritising intolerable risks
    II. establishing treatment options
    III. identifying and developing treatment options
    IV. evaluating treatment options
    V. detailing the design and review of chosen options, including management of residual risks
    VI. communicating and implementing the selected treatments

## TREATMENT PLANS

53. Treatment plans **should** be used to assist agencies in selecting, implementing, monitoring and reviewing risk treatments to ensure their effectiveness and appropriateness. Effective treatment plans:
    I. prioritise the risks to be treated
    II. monitor the risk after treatments have been applied
    III. identify gaps and residual risks that **may** require further treatments
    IV. record decisions about treatments and actions taken
    V. determine and monitor timeframes for implementation of treatments
    VI. identify resources and responsibilities required to achieve treatment outcomes

## RISK, TREATMENT STRATEGIES

54. Table 3 provides some examples for agencies to consider using when assessing whether risk treatments will be effective in reducing security risks:

**Table 3 - Risk treatment strategies**

| Strategy | Reason/cause/action |
|---|---|
| **Accept risk** | • the risk is considered tolerable (before or after treatment) based on an informed decision<br>• there is no other option but to accept the risk and monitor it until circumstances change and action can be taken<br>• the benefits of accepting a higher level of risk outweigh the consequences<br>• the risk is considered intolerable but capability, resources or exceptional circumstances give cause to accept the higher risk |
| **Avoid risk** | • do not start or undertake actions or take decisions that give rise to the risk<br>• remove or reduce the activities or personnel that are causing, or creating exposure to, the risk |
| **Exploit risk** | • take or increase the level of risk in order to realise the benefit an opportunity presents by ensuring the event occurs |
| **Reduce risk** | Change the likelihood and/or consequence by:<br>• implementing new treatments or controls to reduce, deter, delay or detect the threat or event<br>• improving business processes, training or practices<br>• establishing or improving audit and compliance arrangements, contractual agreements, communication channels etc. |
| **Share risk** | • the risk has no single owner and/or other agencies or entities are exposed to the same or similar risks (such as shared tenancies, shared services, partnerships or joint ventures)<br>• the risk has no apparent owner |

## IMPLEMENTING TREATMENTS

55. Implementation is the process of deciding on the resources required and who is responsible for applying the risk treatments. It **should** also include the details of what ongoing resources are needed to maintain the treatment to the required level.

## SCALABLE MEASURES

56. In planning and implementing treatments for security risks, agencies **must** consider how treatments can be scaled to account for increases and decreases to the threat level. [5]

57. Scalable measures **may** need to consider:

    I. how the threat level is identified and monitored for change

    II. determining who in the agency needs to be informed of changes to the threat level

    III. determining who is responsible for implementing change to the risk treatments

    IV. ensuring business continuity planning can account for increases to heightened threat levels

[5] Including changes to the National Terrorism Threat Level

V. what additional resources **may** be needed if the threat level increases

## SECURITY ALERT LEVELS

58. Agencies **may** consider implementing internal security alert levels as a way of informing or educating employees of the security measures in place or that **may** be required, as well as their own security responsibilities under different security threat levels.

59. Security risks can be categorised into three areas:

    I. **Event** – an event is an incident impacting the agency's ability to function (e.g. extreme weather event, fire etc.)

    II. **Threat** – a threat is a declared intent to inflict harm on personnel or property

    III. **Activity** – an activity is an action by one or more people that leads to a negative impact on physical security (e.g. protests, filming of personnel or premises)

60. In line with the BILs. **Table 4** provides examples of security alert levels.

**Table 4 - Example security alert levels**

| Security alert levels | Likelihood of threat | Security measures required |
|---|---|---|
| **Low** | Applies when only general concerns exist regarding an event, threat or activity | Existing security measures are sufficient |
| **Medium** | Applied when an event, threat or activity will possibly occur (feasible) | Security measures are maintainable indefinitely, with minimal impact on the agency's operations |
| **High** | Applies when an event, threat or activity is likely (expected) to occur | Security measures are sustainable for lengthy periods without causing undue hardship to employees, affecting operational capability or aggravating relationships with the local or broader community |
| **Extreme** | Applies when an event, threat or activity is imminent or has occurred | Security measures will not be sustainable over the long-term without creating hardship and affecting the agency's operations and employees |
| **Catastrophic** | Applies when a severe event, threat or activity is imminent or has occurred | Advice from other agencies, Lead Security Agencies (LSA), or the National Security Hotline is required for additional security measures |

61. In determining the security alert level, it is **recommended** that agencies monitor:

    I. National Terrorism Threat Level Advisory System and advice

    II. police and emergency management advice

    III. Bureau of Meteorology advice

    IV. agency security incident reports

    V. media reports

## IDENTIFYING RISK MANAGERS

62. Agencies **must** appoint a risk manager to be responsible for each security risk, or category of security risk, that the agency identifies.
63. A risk manager **should** be a person, or group of people, capable of monitoring, managing and reviewing risks, including any treatments that are applied, and for any changes to the risk, threat, vulnerability or criticality of the agency's resources.
64. Agencies with shared risks **must** determine an appropriate risk manager between all affected parties.

## DEVIATING FROM THE SECURITY PLAN OR SAPSF REQUIREMENTS

65. Agencies are **responsible for** managing their own risks and implementing appropriate treatments in line with the core and supporting requirements of the SAPSF and their security plan. However, it is **recommended** that agencies treat their security plan as a 'living document' that can be adjusted as needed to address new or changing risks.
66. If circumstances in an agency, such as an increase in risk, threat vulnerability or criticality, the agency **must** document any decisions made to deviate from or alter the security plan, including any justifications and alternative risk treatments implemented.
67. If an agency is unable to implement a core or supporting requirement, the risk management approach of the SAPSF agencies **may** implement an alternative risk treatment where it achieves an equivalent or better level of protection afforded by the SAPSF requirement.
68. As above, the accountable authority or ASE of the agency **must** document the decision and, if required, adjust the agency's security plan and maturity level. See section **Implementing core and supporting requirements of the SAPSF** in SAPSF policy Security governance for more detail.

## REVIEWING THE SECURITY PLAN

69. Security plans **must** be reviewed at least every two years to ensure the adequacy of existing protective security arrangements and risks treatments, while also monitoring for significant changes to the agency's risk environment or tolerance levels.
70. Where changes to the risk environment or tolerance is identified, it is **recommended** agencies review their security plans at this time.
71. Agencies **must** determine how their security plan (and any supporting security plans) will be reviewed. Agencies' plans **may** be reviewed by the ASE or appropriate security adviser, through a security governance or protective security committee, or via an external security consultant.
72. When reviewing the security plan, it is **recommended** that agencies seek advice and technical assistance from specialist agencies or entities, such as:
    - The Australian Security Intelligence Organisation (ASIO) for threat assessments
    - ASIO-T4 Protective Security for physical security advice or technical assistance
    - Protective Security Services Branch for physical security advice
    - South Australia Police for state criminal threat information

- The Australian Government Security Vetting Agency for security vetting procedural advice
- other subject matter experts

# 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' updated |
| 2.0 | 26/10/2022 | Definition of ‘shared risk’ updated<br>Guidance on ‘risk appetite’ updated (para 28)<br>Guidance on Shared Risk updated (para 43) |



Government
of South Australia