



Security Governance

GOVSEC-5: Security planning



Contents

About this document	3
Definitions and shortened terms	5
Context	9
Guidance	10
Introduction	10
Required action: Conduct a criticality assessment	10
Required action: Identify security risks	11
Required action: Consider site-specific security risk assessments	14
Required action: Determine the risk tolerance for your agency	15
Develop an agency security plan	16
Required action: Plan protective security measures and capture decisions	18
Required action: Review and evaluate the security plan	21
References and resources	37

Author: Resilience and Recovery Tasmania
Publisher: Department of Premier and Cabinet
Date: April 2023

© Crown in Right of the State of Tasmania April 2023

About this document

This document – GOVSEC-5: Security planning – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF is a whole-of-government approach to the protection of Tasmanian Government information, people and assets from compromise and harm. It establishes minimum protective security standards and makes clear that to continue ensuring the security of our people and assets, Tasmanian Government agencies need to:

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

The TAS-PSF sets out 14 core requirements – with each accompanied by supplementary requirements – that define what must be addressed in order to protect our information, people and assets.

The suite of policies and guidance, including those found in this document, ensures that the TAS-PSPF will be applied across Tasmanian Government agencies in a consistent way. It will also assist agencies to achieve the expected outcomes of the following protective security domains under the TAS-PSPF:

- security governance
- information security
- people security
- physical security.

OFFICIAL

The table below lists all 14 core requirements of the TAS-PSPF and their corresponding policies. The name of the policy and guidance provided in this document is [highlighted](#).

Protective security outcome	Core requirement	Relevant policies and guidance
Security governance	1	GOVSEC-1: Establish security governance
	2	GOVSEC-2: Security advice and responsibilities
	3	GOVSEC-3: Security awareness
	4	GOVSEC-4: Annual reporting
	5	GOVSEC-5: Security planning
	6	GOVSEC-6: Reporting incidents and security investigations
Information security	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
People security	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
Physical security	13	PHYSEC-1: Protecting assets
	14	PHYSEC-2: Agency facilities

Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/required/ responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/ recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the <i>State Service Act 2000</i>), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	The person nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's required protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of official information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted or obtained by an agency.
originator	The instigating individual (or agency) who generated or received the information and is responsible for classifying it.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF. 1. Security is a responsibility of government, its agencies and its people.

Term	What this means in the context of the TAS-PSPF
	<ol style="list-style-type: none"> 2. Each agency is accountable and owns its security risks. 3. Security will be guided by a risk management approach. 4. Strong governance ensures protective security is reflected in agency planning. 5. A positive security culture is critical.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
Responsible Executive	The person who oversees protective security matters within your agency, they may also be the Chief Security Officer (CSO).
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security classified	Information that holds a classification of PROTECTED, SECRET or TOP SECRET and must be protected against compromise. Access to the information must be controlled and accessed by appropriately security cleared people.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	<p>A security incident is:</p> <ul style="list-style-type: none"> • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.

Term	What this means in the context of the TAS-PSPF
security plan	Central document detailing how an agency plans to manage and address their security risks.
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not security-classified information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's required protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
zone	The physical locality, workspaces, and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Acronym/abbreviation	Meaning
ASA	Agency Security Advisor
ASIO	Australian Security Intelligence Organisation
BIL	business impact level
RE	Responsible Executive

Context

The **GOVSEC-5 Security planning** policy and guidance will assist agencies to achieve an effective protective security outcome within the security governance domain of the TAS-PSPF. They address core requirement 5 and its supplementary requirements.

Core requirement 5

The Accountable Authority will be responsible for adopting protective security planning and monitoring to manage security risks.

Supplementary requirements

To identify and manage security risks, the Accountable Authority will:

- a) conduct a criticality assessment to identify the agency's key functionality and assets
- b) identify agency-specific, and shared intergovernmental, security risks
- c) consider site-specific security risk assessments where necessary¹
- d) determine the risk tolerance for the agency, which is subject to measuring and monitoring
- e) plan and determine priority application of protective security measures to manage identified agency security risks and capture decisions which deviate from, or alter, the agency security plan
- f) review and evaluate the security plan as necessary or when risks or circumstances change.²

Adequate security planning and preparedness will support and enable business objectives while protecting vulnerabilities. The adoption of protective security planning will improve agency-specific resilience appropriate to risk appetite and tolerance.

¹ Such circumstances may include multi-site agencies or complex and varied agency sites. Where site-specific plans are actioned, there must still be an overarching agency security plan.

² For example, where the agency functions vary, certain functions are relocated, or new or evolving threats are identified.

Guidance

Introduction

To be successful at managing security risks, agencies need to understand the threats they face, what resources need protecting, and how to protect them.

The TAS-PSPF policy: Establish security governance (GOVSEC-1) requires agencies to develop a security plan. A security plan enables agencies to review strategic and operational risks and implement the appropriate treatments that manage those risks to an acceptable level.

Security planning uses 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.

Required action: Conduct a criticality assessment

Conducting assessments strengthens your familiarity with the environment in which your agency operates, promotes situational awareness, and supports sound decision-making.

Criticality assessment

Addressing risk management requires you to identify your agency's most crucial assets – those that are essential to the ongoing operation of your agency. Identifying these assets and understanding your agency's operational risk environment will help you to apply prioritised risk treatment strategies that are proportionate to your agency's environment.

A criticality assessment will depend upon your agency's function, business objectives and risk environment. Performing this assessment allows you to make informed risk management decisions.

Typically, a criticality assessment includes:

- criticality ratings – a measure of the importance of the assets to your agency, e.g. numerical scale, importance value scale or business impact level (BIL). Applying a BIL³ is based on the assessed impact to your agency in the event of integrity or availability compromise to the asset.
- consequence of compromise – what could happen
- category – what part of the agency or business this would impact (e.g. people, information, property, reputation, finances, business operations or services).

Assets identified as being critical should have the greatest protections assigned to them, in priority order.

Threat assessment

A threat assessment identifies where the threats to your agency, or its assets, come from and considers the likelihood of the threat eventuating. 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 assessment

A vulnerability assessment identifies how likely your agency, or its assets, are to be impacted by the identified risks. Understanding your agency's vulnerability to risk informs the likelihood and consequence of those risks which, in turn, helps you to prioritise risks and develop treatments.

Required action: Identify security risks

Identifying security risks is imperative to effective security risk management. Developing good security risk management supports your agency's resilience and builds a positive risk culture. It enables your people to know your agency's risks, make coordinated and informed decisions in managing those risks, identify new opportunities, and learn from mistakes.

³ See TAS-PSPF policy: Protecting official information (INFOSEC-2) for advice relating to BILs when determining the consequences of compromise, or loss of agency information or assets, or harm to your people.



Agency-specific risks

A security risk can result in compromise, loss, unavailability or damage to your agency's resources, including causing harm to people. Security risk is measured in terms of the chance of the risk event occurring (likelihood) and the outcomes if the risk event occurs (consequence).

Identifying security risks generates a clear, comprehensive and concise list of potential sources of risks and threats which could impact the Tasmanian Government, your agency and its ability to deliver its core function for government.

You can develop this list by determining the importance of the agency assets (criticality of assets – as above) and mapping those against sources of the risk (threat assessment) and the manner in which these elements may facilitate or inhibit this interaction (vulnerability assessment).

When determining what risks, threats, vulnerabilities or criticalities could affect your agency or its assets, you should consider the following questions:

- what could happen? (potential event or incident)
- what is the likely outcome and impact if it does happen? (consequences)
- when could it happen? (frequency)
- where could it happen? (location and assets affected)
- what could make it happen? (sources, potential threats, triggers, catalysts)
- do we need more information to properly assess this risk?
- why could it happen? (vulnerabilities, gaps, inadequate arrangements)
- who could be affected? (individuals or groups, stakeholders, service providers)
- does mitigating this risk create other risks to clients or the public?

Manipulating risk assessment inputs (the consequence or likelihood of a risk event⁴) to achieve a lower result is not an appropriate method of risk management and bypasses the intent of risk tolerance. You should develop appropriate rating scales for likelihood and consequence in accordance with your agency's risk tolerances.

⁴ Event: as defined in ISO Guide 73: 2009 Risk Management – Vocabulary

Analysing security risks

Analysing your agency's security risks involves assessing the likelihood of the risk event occurring and potential consequence should the risk event occur. You should also determine if existing security controls or risk treatments are adequate in managing the identified risks.

The likelihood and consequence of an event are defined by considering:

Likelihood	The chance or probability of the event occurring.
Consequence	The outcome affecting objectives if the event occurs (consequences can be expressed qualitatively or quantitatively and can be certain or uncertain and have positive or negative effects on objectives). There may be a number of possible outcomes associated with an event.

Defining your risks in terms of likelihood and consequence allow you to produce a risk rating, which is then used to assist in prioritising the risks in descending order. It is recommended that you adopt a risk rating-matrix approach to determining the levels of risk which align to your agency's risk tolerances.

Evaluating security risks

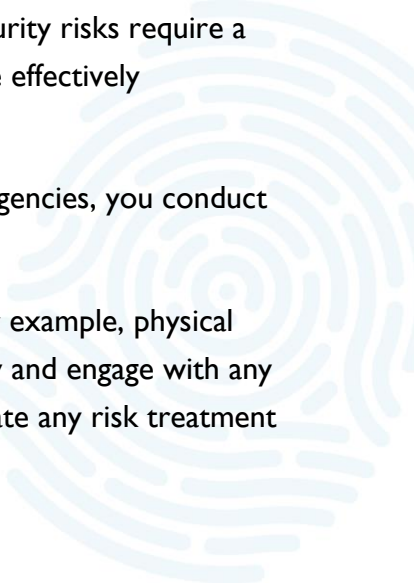
Following analysis, security risks must be evaluated to determine if those risks are acceptable (tolerable, within existing controls) or unacceptable (intolerable, in need of additional treatments or prohibited). Refer to the section on risk tolerance below for more information.

Shared risks

Shared security risks 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 all stakeholders to be effectively understood and managed.

It is recommended that, where you share tenancies or facilities with other agencies, you conduct risk assessments to evaluate the security risks for the co-tenancy.

If your agency assesses a security risk to be shared due to your location (for example, physical boundaries, shared public spaces, government precincts), you should identify and engage with any other agencies or entities that are affected by the security risk, and coordinate any risk treatment accordingly.



If no other party with whom the security risk can be shared can be reasonably identified, you must mitigate the combined security risk to the extent you are able to within your agency's function and operations.

Where there are shared security risks, but each party has a different tolerance for the risk, it is recommended that all parties identify the areas of difference and determine whether additional treatments can be implemented to alleviate any concerns.

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 parties negotiate an appropriate risk manager for all shared risks.

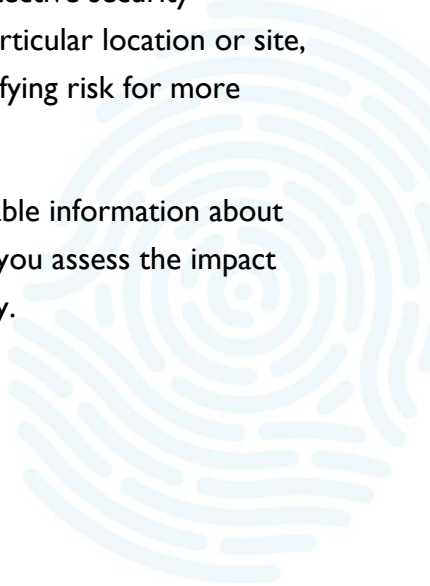
Required action: Consider site-specific security risk assessments

If your agency operates over multiple locations or with complex and varied sites, you should consider if site-specific security risk assessments are necessary to establish an effective and comprehensive security plan. This includes any new sites or facilities under construction or major refurbishment.

Conducting site-specific security risk assessments can help you to prepare site security plans and identify security requirements that should be included within existing or future site development plans, design briefs, requests for tender and contracts. Please note, though, that you are still required to have an overarching agency security plan.

The process of developing a site security plan is the same as for the development of your agency's overall security plan (described below). A site-specific plan documents protective security measures to counter risks to your agency's functions and resources at a particular location or site, identified through the risk assessment (refer to the section above on identifying risk for more information about how to do this).

Site security plans, like your overarching agency security plan, contain valuable information about your agency's security and operations. For this reason, it is important that you assess the impact of any loss or harm to each plan and apply a protective marking if necessary.



Required action: Determine the risk tolerance for your agency

Your Accountable Authority is responsible for determining and managing your agency's security risks, which includes determining your agency's risk appetite and risk tolerance.

Risk appetite reflects an agency's attitude to risk, and how much risk the agency or Accountable Authority is willing to accept.

Risk tolerance is the level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk. It is an informed decision to accept risk.

Although you must try to minimise your agency's level of risk to as low as is reasonable, risk tolerance allows for the practical application of risk appetite and can lead to innovative business practices, positive business outcomes and a positive risk environment.

Risk tolerance includes:

- expectations for mitigating, accepting and pursuing specific types of risk
- boundaries and thresholds for acceptable risk-taking (measurable operational limits)
- actions to be taken or consequences for exceeding approved tolerances.

Risk tolerance is often specified for relevant identified risks and can be expressed as acceptable/tolerable or unacceptable/intolerable and are subject to measuring and monitoring. The risk tolerance for your agency can be affected by modifications in evaluation criteria and your appetite for risk. It can vary depending on:

- prevailing political and community sensitivities and expectations
- the nature of a security incident (e.g. terrorist act, hacking)
- existing or emerging security incidents (trusted insider, cyber-attacks)
- strategic or business priorities
- vigilance, resilience and adaptability of your people and how effective they are at applying security awareness principles
- resource availability for treatment
- the ability of the government, agency or an individual to absorb losses.

In most cases, determining risk tolerance and levels of risk appetite can be understood as a gradient scale, where the appetite for the risk becomes progressively less tolerable as the risk level increases.

Required action: Develop an agency security plan

An agency's Accountable Authority is responsible for the agency's security plan, supported by the Responsible Executive (RE) and Agency Security Advisor (ASA). It is important to note that every agency's security plan will, and should, be different. Your security plan must reflect your agency's protective security requirements in line with the risks that your agency faces.

As an agency of the Tasmanian Government, the way you manage the risks in your agency can have broader impact across other agencies and the Tasmanian Government. For this reason, you must consider the aggregate risk-based decisions you make.

Your agency security plan should be developed by a person/s who has in-depth knowledge and understanding of the agency's strategic objectives and an appropriate level of security risk management knowledge and experience.

A less specific version of your security plan (that does not disclose complete criticalities, threats and vulnerabilities) should be shared and made available across the agency, as it assists to build security awareness and culture. Sharing your security plan provides common understanding of the protective security obligations and responsibilities across your agency.

You should align your security plan with the core and supplementary requirements of the TAS-PSPF.

The following table provides an overview of the recommended structure and content to cover in your security plan.

Section of the plan	Recommended content coverage
Security goals and strategic objectives	Your approach and commitment to effective security risk management of your agency, its security priorities, goals and objectives and the development and promotion of a positive security culture.
Security risk environment	The security risk environment in which your agency operates and the security risks to your agency. Understanding what resources (information, people and assets) you need to protect, what you need to protect those resources from, and how those risks will be managed in your agency.
Risk tolerance	Your agency's level of risk tolerance determined by the level of potential damage to the agency or the Tasmanian Government.
Security capability and maturity	What the level of security maturity in your agency is, and what capabilities your agency 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 your agency, how these treatments keep risk within tolerance and how security risks are monitored, managed and reviewed.
Supporting and evidentiary documents	<p>Whether evidentiary documents are needed to establish an effective and comprehensive security plan. Examples include:</p> <ul style="list-style-type: none"> security risk assessment reports threat assessments site security plans vulnerability assessments agency-specific security procedures security risk register agency security maturity monitoring critical asset register security incident register/response procedure privacy impact assessments information asset register other agency operational or compliance plans.

Table I – Recommended structure and content of a security plan

Setting security goals and objectives

You must set security arrangements for your agency which support and reflect your agency's strategic objectives by reflecting the risks that would impact upon those objectives being achieved. Your Accountable Authority must establish clear security goals for your agency that support both the strategic objectives of the agency and the requirements of the TAS-PSPF, while also reflecting those goals in the agency security plan.

Security maturity

Security maturity is a meaningful way of measuring the agency's overall capability in line with the risk environment and the agency's risk tolerance. Maturity recognises the inherent differences between agencies, functions, risk environments and security risks. It acknowledges the journey each agency is taking to achieve their security goals and objectives, while helping to identify areas for improvement.

The security maturity of your agency can be measured by how you:

- understand, prioritise and manage your agency's security risks
- respond to and learn from security incidents
- foster a positive security culture
- achieve security outcomes and core requirements while delivering business outcomes.

It is recommended that you consider and develop a security maturity monitoring plan as part of your agency's security plan.

Required action: Plan protective security measures and capture decisions

Priority application of risk treatments

Using the steps outlined in this policy (GOVSEC-5), you must develop a security plan for your agency. The security plan must outline the approach, responsibilities and resources that will be applied to manage the protective security risks in line with the core and supplementary requirements of the TAS-PSPF. Your security plan will enable you to review strategic and operational risks and implement the appropriate treatments to manage those risks to an acceptable level.

Your agency security plan should take a risk-management approach to protective security and address threats, risks and vulnerabilities across all areas of security in your agency (security governance, information security, people security and physical security).

A risk-management approach means making informed decisions about how to implement the core and supplementary requirements of the TAS-PSPF, and includes:

- identifying your most critical assets to ensure the ongoing operation of your agency
- undertaking structured risk assessments to identify, analyse and prioritise security risks
- implementing risk treatments that are considered and coordinated and that involve the efficient and effective use of resources to mitigate security risks.

Risk treatments are the controls or mitigations put in place to reduce or manage the security risks you have identified - to within your agency's risk tolerance levels. You can apply risk treatments separately or in combination with other treatments to achieve a desired outcome.

In planning and implementing treatments for security risks, you must consider how treatments can be scaled to account for risk increases and decreases according to your operating environment and threat levels.⁵

Scalable measures should consider:

- how the threat level is identified and monitored for change
- who needs to be informed of changes to the threat level
- who is responsible for implementing changes to the risk treatment/s
- ensuring business continuity planning can account for the heightened threat level
- what additional resources may be needed if the threat level increases.

Risk treatments can be applied separately or in combination. It is recommended that you balance the cost and effort of implementing treatments against the expected benefits to ensure that the treatment is proportional to the risk rating. It may not be possible or cost-effective to implement all possible risk treatments; however, you must prioritise and implement the most appropriate or effective treatments.

The Australian Standards HB 167: 2006 Security Risk Management (chapter 7) provides a 6-step process for treating risks that entails:

- prioritising intolerable risks
- establishing treatment options
- identifying and developing treatment options
- evaluating treatment options
- detailing the design and review of chosen options, including management of residual risks
- communicating and implementing the selected treatments.

Developing treatment plans will assist you to select, implement, monitor and review risk treatments to ensure their effectiveness and appropriateness. Effective treatment plans:

- prioritise the risks to be treated
- monitor the risks after treatments have been applied

⁵ Including changes to Australia's national terrorism threat level; refer to www.nationalsecurity.gov.au/national-threat-level/current-national-terrorism-threat-level.

- identify gaps and residual risks that may require further treatments
- record decisions about treatments and actions taken
- determine and monitor time frames for implementation of treatments
- identify resources and responsibilities required to achieve treatment outcomes
- establish monitoring and reviewing processes.

The following table provides some examples for you to consider using when assessing whether risk treatments will be effective in reducing security risks.

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

Table 2 – Risk treatment strategies

Capture decisions which deviate from, or alter, the security plan

You are responsible for managing your agency's own risks and implementing appropriate treatments in line with the core and supplementary requirements of the TAS-PSPF and your security plan. Applying a risk-based approach to the TAS-PSPF is about making informed decisions on how to implement the core and supplementary requirements. You will implement the requirements of the TAS-PSPF based on your agency's size, operations, and risk environment.

It is recommended that you treat your agency security plan as a 'living document' to be adjusted as needed to address new or changing risks. For example, if circumstances in your agency change – such as an increase in risk, threat vulnerability or criticality – you may update the security plan. In these circumstances, you must document any decisions which led to deviation from or altering of the security plan, including any justifications and alternative risk treatments implemented.

It may be that you are unable to implement a requirement of the TAS-PSPF using the risk management approach taken by the TAS-PSPF. If this is the case, you may implement an alternative risk treatment if doing so will achieve an equivalent or better level of protection than if you had met the TAS-PSPF requirement.

As above, you must document your decision and, if required, adjust your agency's security plan and maturity level for the related TAS-PSPF requirement.

Required action: Review and evaluate the security plan

You must review your agency security plan at least every 2 years to ensure the adequacy of existing protective security arrangements and risk treatments, while also monitoring for significant changes to your agency's risk environment or tolerance levels.

You must consider amendments to your agency security plan where:

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

You must determine how your agency security plan and any supporting documents or additional site security plans will be reviewed. It is recommended that your agency security plan is reviewed by your ASA, or by an external security consultant.

When you review the security plan, it is recommended that you seek advice and technical assistance from specialist agencies or entities such as:

- the Australian Security Intelligence Organisation (ASIO) for threat assessments⁶
- ASIO-T4 Protective Security for physical security advice or technical assistance⁷
- Tasmania Police for state criminal threat information
- the Australian Government Security Vetting Agency⁸ for security vetting procedural advice
- other subject matter experts, as necessary.

⁶ Contact ASIO via their Outreach team on (02) 6234 1668.

⁷ Available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

⁸ For more information, refer to the agency's website at www.defence.gov.au/security/clearances.

Useful resource 1: TAS-PSPF maturity level indicators

Maturity level	Indicators
1	<p>Partial or basic TAS-PSPF implementation.</p> <p>Success is reliant upon individuals, not processes.</p> <p>Protective security is not well understood across the agency.</p> <p>Security resources are assigned reactively and based on who is available rather than competency or role responsibilities.</p> <p>Security information is siloed, duplicated and inconsistent.</p>
2	<p>Foundational practices with substantial implementation of the TAS-PSPF.</p> <p>Protective security requirements are not fully implemented into business practices, though the agency is meeting most security outcomes.</p> <p>The importance of security is recognised, and key leadership responsibilities are assigned and understood.</p> <p>Known security risks are understood and sometimes reviewed, including effectiveness of treatments.</p> <p>Required security policies are in place, but awareness and application is sporadic and not procedurally driven.</p> <p>Tools and technologies to assist security management meet basic needs but are not centrally organised or well-integrated.</p>
3	<p>Complete and effective risk-based security measures are implemented.</p> <p>Protective security requirements are integrated into business practices.</p> <p>The agency is meeting security outcomes.</p> <p>Effective security governance has been established. The agency's leadership supports and demonstrates a high level of security awareness and practice.</p> <p>Security is factored into the strategic objectives and all agency outputs.</p> <p>Agency leadership is empowered to make decisions to support good security.</p> <p>Risks are routinely identified, monitored and reviewed – new risks are quickly identified and addressed.</p> <p>Tools and technologies to assist security management are effective, well managed and integrated effectively.</p> <p>Strategic objectives and maturity targets are achieved or sustained.</p> <p>Investment in security is ongoing to sustain measures at this level.</p>

4	<p>Comprehensive and adaptive operating environment with effective TAS-PSPF implementation.</p> <p>Protective security requirements are proactively integrated into business practices and exceeding security outcomes.</p> <p>The agency is excelling at implementing better-practice protective security.</p> <p>Security culture is embedded and ubiquitous.</p> <p>Employees undertake regular security refreshers or training to ensure skills are current and relevant to the agency's needs.</p> <p>Security is maintained through role successions.</p> <p>Processes are in place to identify and test security improvement.</p> <p>The agency has achieved a cycle of continuous improvement.</p> <p>Tools and technologies to assist security management enable collaboration across the agency and improve process efficiency.</p> <p>Security planning integrates short, medium and long-term objectives effectively and seamlessly and adapts quickly to sudden changes.</p> <p>Security management information is captured, analysed and circulated in real time when needed.</p>
---	---



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
GOVSEC-1: Establish security governance	<p>Your Accountable Authority is partially aware of protective security requirements across your agency.</p> <p>Partial understanding, assessment and management of security risks to your agency's people, information and assets. Security is not dealt with in a consistent manner.</p>	<p>Your Accountable Authority substantially applies protective security requirements across your agency.</p> <p>Most security risks and risk tolerances are identified and managed, monitored or reassessed on a regular basis.</p> <p>Security risk decisions and shared risks that affect other agencies are substantially managed and communicated to affected agencies.</p>	<p>Your Accountable Authority consistently applies protective security requirements across your agency, determines the agency's tolerance for security risks, promotes sound risk management processes and ensures appropriate governance arrangements are in place to protect your agency's people, information and assets.</p> <p>Security risk decisions and shared risks that affect other agencies are understood and communicated in a timely manner.</p>	<p>Your Accountable Authority has an integrated, continuous-improvement approach to security management across your agency.</p> <p>Security risk management is a significant priority for your agency, is embedded in your agency's operations and practices and is aligned to business objectives.</p> <p>Your agency identifies and operates within agreed and defensible risk tolerances, and leverages better practice to drive business and security decisions.</p> <p>Formal risk management processes and initiatives to connect security risk management and operations are in place.</p> <p>Your agency promotes inter-agency collaboration to</p>





OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
				improve management of security risk decisions and shared risks that affect other agencies. Where appropriate, your agency provides better practice advice, beyond TAS-PSPF requirements, to other agencies in its area of expertise.
GOVSEC-2: Security advice and responsibilities	Your agency nominates an Agency Security Advisor (ASA) who has partial capacity to conduct their responsibilities under the core and supplementary requirements of the TAS-PSPF.	Your agency nominates an ASA who is substantially supported and able to conduct their responsibilities under the core and supplementary requirements of the TAS-PSPF.	Your ASA is supported to complete their responsibilities consistently. They fully understand your agency's risk tolerance and operating environment and make sound protective security decisions accordingly. Your ASA regularly briefs the Responsible Executive (RE) and is empowered to make necessary protective security decisions which support the TAS-PSPF.	In addition to those items in Maturity level 3: Your ASA proactively engages across your agency in relation to protective security, enhancing awareness and assisting everyone to understand their responsibilities under the TAS-PSPF. Your ASA consistently monitors your agency's compliance with the TAS-PSPF and identifies



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
				opportunities to improve or exceed performance. Your ASA engages with other agencies to build better practice and share learnings.
GOVSEC-3: Security awareness	Your agency partially develops a positive security culture by ensuring staff complete any mandatory whole-of-government protective security training.	Your agency has created substantial security awareness where your people collectively foster a positive security culture.	Your people are provided with security awareness training relevant to your agency and/or their roles (where required). Your agency provides contemporary and tailored training according to changes in your security environment. Your agency provides role-specific training for people in emergency, safety or security-specific roles.	In addition to those items in Maturity level 3: The security culture of your agency is embedded in every aspect. You provide regular refresher training to agency people. Post-incident learnings are incorporated into policies, processes and/or procedures. Your agency has established effective communication and information-sharing channels.
GOVSEC-4: Annual reporting	Your agency partially monitors the security maturity performance of its security capability and risk culture against the goals and	Performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.	Consistent and defined approach to monitoring your agency's security performance, which is	Your agency proactively engages in ongoing monitoring and continuous improvement of security capability and culture through

OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
	strategic objectives identified in your agency's security plan.	Your agency's achievement against the security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and assets and mitigation strategies to manage identified risks is substantially captured in your annual security report.	tailored to its risk environment. Your agency meets these obligations through effective reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the agency.	long-term planning to predict and prepare for security challenges. Your agency exceeds reporting obligations and uses annual reporting to drive improvements, strengthen security culture and inform future planning, in line with better practice.
GOVSEC-5: Security planning	Security planning is conducted in a manner that is basic and not consistent. The security plan is partially developed and implemented but may not be current or comprehensive.	A security plan is endorsed by your Accountable Authority and captures most of your agency's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies.	A security plan is endorsed by your Accountable Authority and captures your agency's goals and strategic objectives, key threats, risks, vulnerabilities and details of security risk tolerances and risk mitigation strategies. The plan is regularly reviewed and informs	The security plan is comprehensive in identifying goals, strategic objectives, key threats, risks, vulnerabilities, risk tolerances and risk mitigations. The security plan influences executive management decision-making and planning. Your agency proactively and continuously adapts the



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
		The plan is consistently applied across your agency in the majority of instances.	decision-making within your agency. The plan is used to determine security objectives and clearly supports broader business goals. The security plan is communicated and accessible across your agency.	security plan in response to emerging or changing risks and threat levels.
GOVSEC-6: Reporting incidents and security investigations	Your agency has partially established internal security reporting requirements and understands any external reporting requirements (where necessary). Investigation of security breaches and incidents is not consistent.	Your agency has substantially established and pursues internal security reporting requirements. Your agency coordinates and reports to external organisations where necessary. Your people understand what constitutes a reportable incident and are comfortable to report.	Your agency has established and pursues internal and external security reporting requirements. Incidents are actively investigated, with learnings shared across the agency. Any identified corrections are addressed.	Your agency has an exemplary security culture with proactive security leadership. Your people trust the reporting process and incidents are few. Learnings from those incidents are used to define better practice.
INFOSEC-1: Access to, and management of, official information	Some information access controls and security procedures are in place.	Processes are substantially in place to enable appropriate sharing of information with	Information holdings are accessed and shared with appropriately	Your agency proactively refines and reinforces information management





OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
	Supporting requirements on information sharing, access to sensitive and security-classified information and controlling access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings are partially applied.	relevant stakeholders who have a 'need to know' and are appropriately security cleared. Access controls are substantially implemented to limit unauthorised access to supporting ICT systems, networks, infrastructure, devices, applications and data holdings in accordance with the information access control supporting requirements.	security-cleared personnel who have a 'need to know'. Access controls support the integrity of ICT systems, networks, infrastructure, devices, applications and data holdings.	processes and access controls to ensure superior protection of information and currency of systems to protect against emerging threats and issues. Information is shared with appropriately security-cleared personnel who have a 'need to know'. Systems are in place to detect, monitor and respond to irregular access to information or ICT systems, networks, infrastructure, devices and applications in real time.
INFOSEC-2: Protecting official information	Your agency has a partial understanding of its information holdings. Procedures and operational controls to protect official information proportional to their value, importance and	Your agency knows the value of its information holdings and has substantially established operational controls to ensure official information is managed in accordance with minimum protections identified in TAS-PSPF policy: Protecting	Your agency clearly understands the value of its information holdings and operational controls are in place to ensure official information holdings are consistently handled in accordance with minimum protections identified in the	Your agency culture proactively supports the consistent and appropriate handling of official government information asset holdings, exceeding minimum protections identified in TAS-PSPF policy:



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
	sensitivity are basic and not consistent.	official information (INFOSEC-2). Your agency monitors and controls classified information holdings in the context of its risk environment.	TAS-PSPF policy: Protecting official information (INFOSEC-2), proportional to their value, importance and sensitivity.	Protecting official information (INFOSEC-2). In a heightened risk environment, your agency closely monitors and controls classified information holdings.
INFOSEC-3: Robust technology and information systems	Partial security measures are in place for ICT system development. Management of ICT systems certification and accreditation (or assessment and authorisation) is basic and not consistently implemented.	Security measures are substantially in place for ICT system development. Certification and accreditation (or assessment and authorisation) of ICT systems is consistent and in accordance with TAS-PSPF policy: Robust technology and information systems (INFOSEC-3).	Security measures are applied during all stages of ICT system development. ICT systems are certified and accredited (or assessed and authorised) in accordance with TAS-PSPF policy: Robust technology and information systems (INFOSEC-3).	ICT security measures, including ICT systems certification and accreditation (or assessment and authorisation) exceed expected standards. Your agency excels in proactively exploring opportunities to further improve ICT security protections in response to ICT security threats.
PESEC-1: Recruiting the right people	Your agency has partially implemented procedures and systems to ensure people are eligible and suitable to access	Your agency has developed the majority of its procedures and systems to ensure that people are eligible and suitable to access	Procedures and systems are in place to ensure that all of your people are eligible and suitable to access Tasmanian Government resources.	Your agency excels in implementing efficient and timely processes to ensure the eligibility and suitability of

OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
	<p>Tasmanian Government resources.</p> <p>Pre-employment screening is not consistent and security vetting requirements (where relevant) are partially followed.</p> <p>Some risks associated with eligibility and suitability of people are managed.</p>	<p>Tasmanian Government resources.</p> <p>Pre-employment screening practices are substantially in place and security vetting requirements (where relevant) are mostly followed.</p> <p>Your agency manages the majority of risks associated with eligibility and suitability of people.</p>	<p>All pre-employment screening and security vetting (where relevant) requirements are followed.</p> <p>These procedures and systems mitigate risks identified in your agency's people security risk assessment.</p>	<p>people to access Tasmanian Government resources.</p> <p>All requirements are followed and your agency has comprehensive practices in place to proactively manage risks identified in its people security risk assessment.</p>
PESEC-2: Ongoing suitability assessment	<p>Your agency partially assesses and manages the ongoing suitability of its people.</p> <p>Information of security concern for the ongoing suitability of people is not consistently assessed and shared with relevant stakeholders.</p> <p>Some security clearance maintenance requirements (where relevant) are met.</p>	<p>Your agency has substantially developed its procedures and systems to assess and manage the ongoing suitability of its people.</p> <p>In the majority of cases, information of security concern for the ongoing suitability of people is assessed and shared by your agency with relevant stakeholders.</p>	<p>Procedures and systems are in place to ensure that the ongoing suitability of people is assessed and managed in accordance with your agency's people security risk assessment.</p> <p>Your agency has established lines of communication and processes to ensure information of security concern is shared with stakeholders as appropriate.</p>	<p>Your agency is proactive in assessing and managing the suitability of people, including security clearance maintenance requirements (where relevant), to ensure integrity of the agency's core business.</p> <p>Your agency has well-established lines of communication and robust processes to ensure information of security</p>

OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
		Procedures are mostly in place to ensure compliance with security clearance maintenance requirements (where relevant).	Your agency has procedures in place to ensure compliance with all security clearance maintenance requirements (where relevant).	concern for ongoing suitability of people is shared with stakeholders in a timely manner.
PESEC-3: Managing separating people	Your agency has partially implemented processes to ensure that separating people have their access to Tasmanian Government resources withdrawn and are informed of their ongoing security obligations.	<p>Separating people, in the majority of cases, understand their ongoing security obligations and have their access to Tasmanian Government resources withdrawn.</p> <p>Systems and processes are substantially developed to verify consistency of separating people practices across your agency.</p>	<p>Your agency has in place systems and processes to ensure that all separating people understand their ongoing security obligations, particularly where they have had access to sensitive and security-classified information and resources during their employment.</p> <p>Separating people have their access to Tasmanian Government resources withdrawn within an appropriate time frame.</p>	<p>Your agency has proactively implemented systems and processes that are reviewed regularly for separating people. Access to Tasmanian Government resources is withdrawn from people on separation.</p> <p>Your agency ensures separating people are debriefed and provided with a comprehensive understanding of their ongoing security obligations.</p> <p>Information of security concern about separating people is shared with relevant stakeholders, including internally, where appropriate.</p>



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
				Risk assessments are undertaken, where appropriate.
PHYSEC-1: Protecting assets	Your agency partially applies physical security requirements. Partial application increases the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation.	Your agency substantially has in place physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation. The majority of physical security measures are implemented according to the requirements.	Your agency applies physical security measures that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation in accordance with requirements. Risks to the compromise of resources are mitigated to a level consistent with agency risk tolerance levels, in accordance with your agency's security plan.	Your agency applies physical security measures and better practice guidance that minimise or remove the risk of resources being made inoperable, inaccessible, accessed or removed without proper authorisation, which improves the delivery of business. These measures are proportionate to the level of risk and are scalable to changes in the threat environment.
PHYSEC-2: Agency facilities	Your agency partially considers physical security in the early stages of planning, selecting, designing and modifying facilities. Where required, facility certification, accreditation,	In the majority of cases, your agency considers physical security when planning, selecting, designing and modifying facilities, substantially integrating physical security	Physical security requirements are integrated into all stages of planning and modifying facilities. Where required, your agency facilities are certified and accredited systematically,	Physical security requirements are a key driver for selection, design or modification of your agency facilities. Where required, your agency proactively ensures



OFFICIAL

TAS-PSPF policy	Maturity 1	Maturity 2	Maturity 3	Maturity 4
	documentation and review are partially in accordance with the TAS-PSPF and applicable ASIO Technical Notes.	requirements into all facilities. Where required, certification, accreditation, documentation and periodic review of the majority of facilities are in accordance with the TAS-PSPF and applicable ASIO Technical Notes.	with appropriate documentation, and in accordance with the TAS-PSPF and applicable ASIO Technical Notes.	systematic certification and accreditation, with appropriate documentation, of its facilities in accordance with the TAS-PSPF and applicable ASIO Technical Notes. Required physical security upgrades of facilities are implemented as a priority.

Useful resource 2: Risk register examples

Item	Description
Description	Describe the risk (consider the questions listed in the section on agency-specific risks above).
Category	People, information, property, reputation, finances, business operations.
Event	Occurrence or change of a particular set of circumstances.
Source	Threat or hazard that is the source of the risk.
Cause	Why the threat or hazard is a risk.
Consequences	Level of impact the risk will have on your agency.
Risk criteria	Determined tolerability against consequence and likelihood tables.
Priority	Comparing the level of risk (magnitude of risk = consequence + likelihood) with the risk criteria.
Controls	Adequacy of existing controls in place, or the known controls for the risk.
Current risk rating	The current risk rating status.
Risk decision	Whether the risk needs treatment.
Treatments	What action needs to be taken, by whom, with what resources and when.
Residual risk rating	Once treatments have been implemented, what the residual risk rating will be.
Stakeholders	Who else is impacted by the risk (e.g. other agencies, contractors, service providers).
Previous risk information	Information about any previous risk, threat or vulnerability assessments.

Version control and change log

First publication	April 2023	
Revision	February 2024	
Next review date	December 2024	
Change Log	Policy issued	V1.0 April 2023
	Definition: 'core requirement' updated	V2.0 February 2024
	Definition: 'originator' updated	
	Definition: 'protected information' removed and replaced with 'security classified'	
	Definition: 'Responsible Executive' added	
	Definition: 'supplementary requirement' updated	

References and resources

Australian Government, Protective Security Policy Framework, at www.protectivesecurity.gov.au/publications-library/policy-3-security-planning-and-risk-management
AS/NZS ISO 31000: 2018 – Risk management – Guidelines
ISO Guide 73:2009 – Risk management – Vocabulary
SA Government, security governance, at www.security.sa.gov.au/protective-security-framework/governance
Standards Australia HBI67: 2006 Security Risk Management

OFFICIAL



Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au

OFFICIAL