Annual self-assessment report

'How to' guide

Department of Premier and Cabinet

Tasmanian Government

Introduction

This document has been developed to guide agencies in the preparation of their TAS-PSPF annual report for 2024-25. It will aid in determining an appropriate maturity score and providing evidence in support of that score.

This 'How to' guide contains an example against at least one core requirement under each of the security domains. These examples are not taken from the inaugural annual reporting round, but they are a contextual, point-in-time reference to the current implementation status and maturity levels across the Tasmanian Government. The examples are designed to guide your thinking about how the agency has delivered against the core requirement. It does not provide complete solutions for your agency.

DPAC continues to acknowledge that the TAS-PSPF is a risk-based framework that will be adopted according to your agency's most critical assets and security risk assessment. Each agency will have different policies, procedures and practices that deliver against the requirements of the framework.

If you have any questions about completing your annual report, please contact the TAS-PSPF team via taspspf@dpac.tas.gov.au or phone 6232 7770.

Using this guide

The examples provided in this guide use the following formatting:

- [Instructional text is provided in square brackets]
- *Example responses are provided in italics.*

Examples

Security Governance

Requirement	
GOVSEC3	**Security awareness** The Accountable Authority will work to develop a protective security culture within their agency.
Self-assessment guidance prompt	[Provide evidence of the policies and procedures that the agency is currently actioning to ensure everyone understands their role in a positive security culture. What training is being delivered and how (what is the schedule, is it induction only)? Are there any awareness campaigns that support security culture?]
Current maturity	Choose an item.
	[Complete the next sections with evidence to support rating.]
Maturity target	Choose an item.
	[Identify the actions that will support the agency in achieving this.]

Summary:

[Summarise the actions supporting the agency self-assessment score – an overview of all evidence]

In 2024-2025 the agency has continued to roll out the TAS-PSPF Introduction to Protective Security training provided by DPAC, with a completion rate of 65% across the agency as at [date]. The training is included in induction for new employees and is a requirement for all staff annually.

The agency has also introduced the introduction to countering foreign interference training, made available by the Department of Home Affairs, and is meeting the requirements for hosting this training.

The agency has rolled out a range of awareness materials that support staff in knowing their role in a positive security culture and how to report matters of security concern. This includes displaying the security awareness behaviour posters provided by DPAC around all agency buildings, and distributing regular intranet stories. This has been successful with staff demonstrating they feel comfortable to challenge others when agency security policies and procedures are not followed.

Policy documentation:

[Use this table to demonstrate what policy and procedure documents the agency has in support of this core requirement]

Policy/procedure document name	Produced/last review	Next review	Authorised by
Security awareness strategy	*November 2023*	*November 2025*	*Responsible Executive*
Induction policy and procedure	*February 2024*	*February 2026*	*Accountable Authority*
Letter of exchange – DHA	*April 2024*	*April 2025*	*Accountable Authority*
Security incident reporting	*June 2024*	*June 2025*	*Accountable Authority*

Practices/procedures:

[This section is to provide details on current action, responses and assessments in support of the core requirement]

- *The security awareness strategy states our ASA will use the agency security plan to inform agency specific security awareness training. This year, this tailored training has been targeted towards our high-risk work areas and security clearance holders.*
- *Agency specific security awareness training is reviewed by the ASA every 2 years, per the security awareness policy. This allows us to address emerging trends and keep staff up-to-date with our expectations.*
- *The agency has developed a procedure for reporting security incidents (per GOVSEC-6), and awareness training in support of this is being rolled out across the agency.*

Actions:

[This section is to provide details on the actions your agency will undertake to meet, or maintain, the nominated maturity target]

- *The induction policy and procedure will be reviewed in February 2025. The induction policy does not currently differentiate requirements between appointed positions and is generic in nature. We will incorporate high-risk areas and those identified as requiring security clearances in the review, so that specific training can be issued during induction.*
- *A framework for travel briefings is being developed and will be submitted for approval to our Responsible Executive. This framework will formalise the procedure for security cleared staff to receive appropriate travel briefings and debriefings. The framework will include a travel notification process for all staff that will be communicated to staff through an intranet story and through targeted reminders to line managers.*

Requirement	
GOVSEC5	**Security planning** The Accountable Authority will be responsible for adopting protective security planning and monitoring to manage security risks.
Self-assessment guidance prompt	[Provide evidence of the protective security measures that your agency has applied to its identified critical assets and how this has been determined. How did you identify your critical assets and key functions? Did you conduct security risk assessments to inform the protective security measures? Is there an established security plan that documents the agency risk tolerance?]
Current maturity	Choose an item.
	[Complete the next sections with evidence to support rating.]
Maturity target	Choose an item.
	[Identify the actions that will support the agency in achieving this.]

Summary:

[Summarise the actions supporting the agency self-assessment score – an overview of all evidence]

An agency with multiple sites and risk considerations:

During the last 12 months, we have completed an agency Security Risk Assessment (SRA) which formalises our risk tolerance. This has been accepted and endorsed by our Accountable Authority. The agency will develop site specific SRAs throughout 2025-2026, on an identified priority basis.

The agency has conducted criticality assessments across 5 locations. These assessments, in conjunction with SRA, will inform our priority application of protective security measures. Security plans for these 5 sites are now under development and will include minimum standards and requirements in accordance with the outcomes of the Criticality Assessment (CA), SRA and Business Impact Levels (BILs).

A smaller agency:

During the last 12 months, we have completed an agency Security Risk Assessment (SRA) which formalises our risk tolerance. This has been accepted and endorsed by our Accountable Authority. This SRA informs our approach to protective security measures across all our locations.

We have conducted an agency criticality assessment and in conjunction with the SRA and Business Impact Levels (BILs), have commenced identifying priority protective security measures across our agency.

Using our assessments, we have commenced development of an informed agency security plan that will be a living document, updated according to security needs and requirements. Non-sensitive elements of this plan have been shared with staff to support awareness of their responsibilities in protecting agency assets.

Policy documentation:

[Use this table to demonstrate what policy and procedure documents the agency has in support of this core requirement]

Policy/procedure document name	**Produced/last review**	**Next review**	**Authorised by**
Criticality assessment	*Commenced*	*N/A*	*N/A*
Security risk assessment	*Commenced*	*N/A*	*N/A*

Practices/procedures:

[This section is to provide details on current action, responses and assessments in support of the core requirement]

- *Criticality assessments were informed through workshop engagement with key stakeholders, using the CARVER method. This year our ASA completed this procedure across 5 sites and with our executive members. By doing this, the assessments are informed by those who have working knowledge of the relevant key functions of a business area/location.*
- *The security risk assessments were commenced using the following procedure to evaluate risk: Man-Made Threats (Attractiveness, Vulnerability, Impact) and Natural Hazards (Likelihood and Impact). This is part of our security risk assessment process and ensures a consistent approach to how we are evaluating our risks.*
- *Using these results and assessing our business impact against loss or compromise, we have commenced development of site-specific security plans. Our security plans will consider each security domain of the TAS-PSPF.*

Actions:

[This section is to provide details on the actions your agency will undertake to meet, or maintain, the nominated maturity target]

- *The agency will develop an internal protective security policy that will inform decision making and ensure security planning documentation is kept up-to-date.*
- *Some site security plans are underway, these will be finalised by June 2025. The remaining site security plans will be delivered by November 2025.*
- *As site security plans are developed, appropriate protective security measures to address identified unacceptable risks will be applied.*

Information Security

Requirement	
INFOSEC1	**Access to, and management of, official information** The Accountable Authority must adhere to whole-of-government protective security policies and procedures relating to the management of information security.
Self-assessment guidance prompt	[Provide evidence of how your agency is adopting any whole-of-government information management policies. How do you ensure the 'need to know' principle is applied in your agency? Does the agency have formal user registration and deregistration procedures for granting and cancelling access to information systems?]
Current maturity	Choose an item.
	[Complete the next sections with evidence to support rating.]
Maturity target	Choose an item.
	[Identify the actions that will support the agency in achieving this.]

Summary:

[Summarise the actions supporting the agency self-assessment score – an overview of all evidence]

During the last reporting period the agency performed tests on various elements of our information management and access controls, this included a focus on role based access control and authorisations. This demonstrated some variables requiring treatment, particularly where a person was acting in a role but did not have suitable pre-employment security screening to access the suite of information available to the role they were acting in.

The agency is working on an update to our authorisation procedure, to ensure acting arrangements do not provide automatic access to all information without verification of appropriate levels of screening.

The 'need to know' principle is understood across key staff working in high-risk and security specific areas of the agency. This has been facilitated through sessions with our ASA/domain lead. Further work on broader awareness will be incorporated in security awareness training.

Policy documentation:

[Use this table to demonstrate what policy and procedure documents the agency has in support of this core requirement]

Policy/procedure document name	Produced/last review	Next review	Authorised by
Access control policy	*January 2024*	*January 2026 (or upon security incident/breach)*	*Responsible Executive*
Authentication procedure	*January 2024*	*January 2026 (or upon security incident/breach)*	*Responsible Executive*
Authorisation procedure	*January 2024*	*January 2026 (or upon security incident/breach)*	*Responsible Executive*

Practices/procedures:

[This section is to provide details on current action, responses and assessments in support of the core requirement]

- *The access control policy determines the type of access control our agency applies to all information, it follows ISO27001 and is adopted on a risk basis according to the information asset. The agency policy allows us to be consistent in the application of access control measures.*
- *The authentication and authorisation procedures form part of the access control policy and provide clear actions for every type of user. The agency is reviewing these post testing over the previous reporting period, to ensure these are updated as security maturity increases.*

Actions:

[This section is to provide details on the actions your agency will undertake to meet, or maintain, the nominated maturity target]

- *The agency will incorporate the 'need to know' principle in the next review of the security awareness training.*
- *A priority piece of work is for the agency to review and enhance formal user registration and deregistration procedures for granting and cancelling access to information systems, limiting the risk of unauthorised access and/or disclosure.*

People Security

Requirement	
PESEC1	**Recruiting the right people** Accountable authorities must assess the initial suitability, and validate the identities, of people who have access to, or are seeking access to, Tasmanian Government assets.
Self-assessment guidance prompt	[Provide evidence of what your agency is doing to manage the risks associated with recruitment, ensuring suitability of those you engage. What pre-employment screening is currently conducted and when do you determine these measures? Do you know who in your agency holds a security clearance and why?]
Current maturity	Choose an item.
	[Complete the next sections with evidence to support rating.]
Maturity target	Choose an item.
	[Identify the actions that will support the agency in achieving this.]

Summary:

[Summarise the actions supporting the agency self-assessment score – an overview of all evidence]

In 2024-2025, the PESEC domain lead was a member of the relevant human resources committee responsible for reviewing statements of duties as they were submitted for advertising. This allowed a security overview to be applied to the proposed SoDs and relevant pre-employment screening to be nominated and included in the advertising.

A current review of all SoDs is underway, as a result of the Commission of Inquiry recommendations, which will incorporate updates stemming from Employment Direction reviews. This work is ongoing.

We have developed an identified positions register for all positions requiring a security clearance. This has highlighted a need for the agency to seek sponsorship of more security clearances due to the number of positions that have increased security risks and engagement with security classified information.

Policy documentation:

[Use this table to demonstrate what policy and procedure documents the agency has in support of this core requirement]

Policy/procedure document name	Produced/last review	Next review	Authorised by
Security clearance policy	*July 2024*	*July 2026*	*Accountable Authority*
Identified positions register	*October 2024*	*October 2025*	*Accountable Authority*
Recruitment review working group ToR	*August 2024*	*August 2025*	*Director – HR*

Practices/procedures:

[This section is to provide details on current action, responses and assessments in support of the core requirement]

- *The agency is currently reviewing all SoDs in line with the Commission of Inquiry recommendations. In this process, we are incorporating a review for any security clearance requirements and ensuring they are captured as required.*
- *The security clearance policy requires the ASA to monitor the identified positions register continuously, ensuring that security clearances are only held by those in 'identified positions'.*
- *The security clearance policy has clear procedures outlined, including:*
    - *Clearance holders must report changes in circumstances to AGSVA via the portal and notify our ASA;*
    - *Clearance holders must notify the ASA of travel and extended leave arrangements;*
    - *The ASA must communicate any security clearance holder matters to DPAC (the sponsoring agency)*
    - *Staff movements are reported to the ASA.*

Actions:

[This section is to provide details on the actions your agency will undertake to meet, or maintain, the nominated maturity target]

- *The agency is working through the identified positions register to ensure those in identified roles apply for security clearances. The agency aims for half the required security clearances to be applied for in the next 12mths (approx. 25).*
- *The security clearance policy will be further implemented, as more security clearances are issued.*
- *The recruitment working group will continue reviewing SoDs, with the aim for all to be reviewed across the next reporting period.*
- *All positions identified as requiring a security clearance will be bulk submitted for approval by the HoSS, under the requirements of Employment Direction 7.*

Physical Security

Requirement	
PHYSEC1	**Protecting assets** The Accountable Authority must identify and implement appropriate physical security measures to mitigate the risk of harm or compromise to its information, people and assets.
Self-assessment guidance prompt	[Provide evidence of what physical security measures your agency has implemented to mitigate the risk of compromise and harm to your information, people and assets. What steps have been taken to identify critical assets requiring protection? Do you have physical security measures that address the principles of Deter, Detect, Delay and Respond?]
Current maturity	Choose an item.
	[Complete the next sections with evidence to support rating.]
Maturity target	Choose an item.
	[Identify the actions that will support the agency in achieving this.]

Summary:

[Summarise the actions supporting the agency self-assessment score – an overview of all evidence]

Per GOVSEC5, over the last reporting period the agency has conducted a criticality assessment across 5 sites. This has provided a clear priority list of assets requiring protection at these locations.

Physical security protections have been adopted at our highest risk location, which include enhancing crime prevention through environmental design with greater delineation of public access points and secure areas, and the removal of vegetation that was identified to be providing concealment opportunities. We have installed additional electronic access control measures.

The agency will use the criticality assessments, SRA and BILs to inform implementation of physical security measures across the next reporting period, but this work will take time.

Policy documentation:

[Use this table to demonstrate what policy and procedure documents the agency has in support of this core requirement]

Policy/document name	Produced/last review	Next review	Authorised by
Criticality assessment	*Commenced*	*N/A*	
Site security risk assessment	*Commenced*	*N/A*	
Accommodation strategy	*To be commenced*	*N/A*	
Standard Operating Procedure	*To be commenced*	*N/A*	

Practices/procedures:

[This section is to provide details on current action, responses and assessments in support of the core requirement]

- *The agency will continue to perform criticality assessments, security risk assessments and the application of business impact levels to determine the security risks posed to our information, people and assets.*
- *These procedures are established and will assist in the application of priority and proportionate physical security measures. The work is ongoing.*

Actions:

[This section is to provide details on the actions your agency will undertake to meet, or maintain, the nominated maturity target]

- *The ASA is working to complete an agency SRA which will inform the development of an agency accommodation strategy. The agency accommodation strategy will incorporate minimum physical security requirements according to the SRA.*
- *The agency will produce a Standard Operating Procedure for physical security which will provide clear process for upgrades at sites. This work will then be led by the site lead, with guidance from the ASA.*
- *Our implemented physical security measures will be exercised over the next reporting period, to understand how they perform and will be modified to as necessary, to meet the requirement.*

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:
(03) 6232 7770

Email:
taspspf@dpac.tas.gov.au