Annual self-assessment report

[Name of Agency]

Contents

[1. Introduction 3](#_Toc170998630)

[1.1 Purpose 3](#_Toc170998631)

[1.2 Completing the report 3](#_Toc170998632)

[1.3 Use of supplied information 3](#_Toc170998633)

[2. Scoring 4](#_Toc170998634)

[2.2 Maturity assessment model 4](#_Toc170998635)

[3. Reporting 5](#_Toc170998636)

[3.1 Security Governance 5](#_Toc170998637)

[3.2 Information Security 15](#_Toc170998638)

[3.3 People Security 21](#_Toc170998639)

[3.4 Physical Security 27](#_Toc170998640)

[4. Security risk environment and capability 31](#_Toc170998641)

[4.1 Agency risk environment 31](#_Toc170998642)

[4.2 Security capability 31](#_Toc170998643)

[4.3 Exceptional circumstances 32](#_Toc170998644)

[5. Feedback 33](#_Toc170998645)

[5.1 How could support be improved? 33](#_Toc170998646)

[5.2 Can we help you further? 33](#_Toc170998647)

Author: A Marshall  
Publisher: Department of Premier and Cabinet  
Date: August 2022

© Crown in Right of the State of Tasmania December 2022

# Introduction

## 1.1 Purpose

The Tasmanian Government has a responsibility to protect its people, information and assets. In November 2022, Cabinet determined Tasmania’s Protective Security Policy Framework (TAS-PSPF) represents the minimum protective security standards required for the protection and resilience of Tasmanian Government resources.

The completion of this report will allow Accountable Authorities to assess their existing security measures, identify improvement opportunities and support necessary modifications commensurate with the agency risk profile.

Upon completion of this report, a copy must be forwarded to the Department of Premier and Cabinet (DPAC) in accordance with TAS-PSPF core requirement 4 – Annual Reporting.

Reporting provides assurance that Accountable Authorities are working towards a continuous cycle of improvement and provides opportunity for targeted support according to demonstrated need/s.

## 1.2 Completing the report

The report is designed to be completed by the Agency Security Advisor, who reports to the Chief Security Officer/Responsible Executive. The report should be reviewed by the CSO/RE, with final approval issued by the Accountable Authority as the responsible party to the TAS-PSPF.

The report is intended to provide clear and succinct assessment against TAS-PSPF core requirements, along with protective security capability and maturity indicators. Noting, [text in square brackets is instructional].

The report must be submitted to DPAC by no later than 30 March of each calendar year, reviewing the agency’s preceding 12-months protective security performance. The report should be submitted by the CSO/RE or their nominated delegate.

Please ensure the report is classified according to the information provided and update the protective marking as appropriate.

If you require further guidance or assistance to complete this report, please contact the TAS-PSPF team for support: [taspspf@dpac.tas.gov.au](mailto:taspspf@dpac.tas.gov.au)

## 1.3 Use of supplied information

The data provided in each annual report will be analysed and consolidated into an aggregated summary record demonstrating whole of government performance review and evaluation in the improvement of protective security. DPAC will provide a comprehensive review to Cabinet with the following purview:

* Whole-of-government security maturity
* Identification of consistent security themes/gaps
* Financial burdens and considerations
* Information sharing (as necessary)
* Lessons learned

# Scoring

## 2.2 Maturity assessment model

The TAS-PSPF requires agencies to demonstrate a continuous cycle of improvement, measured against the core requirements. In doing so, a maturity assessment is included in annual reporting. The scaled maturity model allows agencies to identify the most appropriate maturity level that accurately reflects their security posture and capability over the reporting period.

Evaluating maturity must be in accordance with the agency risk assessment, the agency’s current operating environment and security maturity targets. The TAS-PSPF requires agencies to evaluate their maturity on each of the core requirements, applying a final average of the aggregate maturity scores. This final score will represent an overall indicator of current security maturity in accordance with the agency’s risk profile.

# Reporting

|  |  |  |
| --- | --- | --- |
| Icon  Description automatically generated | 3.1 Security Governance | |
| **Requirement** | | |
| GOVSEC1 | | **Establish security governance**  The Accountable Authority will establish and implement appropriate security governance for the agency, with specific consideration of the environment in which the agency operates. |
| Self-assessment guidance prompt | | [Provide evidence of the actions taken to ensure the agency has appropriate security governance.  What actions have been completed to understand the threat context and environment of the agency?  Has the agency documented the security risk tolerance that informs how decisions are made, particularly in the protection of your information, people and assets?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| GOVSEC2 | **Security advice and responsibilities**  The Accountable Authority will nominate an ASA. |
| Self-assessment guidance prompt | [Provide evidence of how your ASA is actioning security advice and responsibilities across your agency.  Is your ASA responsible for developing and delivering security measures, policies and procedures?  Does your ASA respond to, investigate and report security incidents?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| GOVSEC4 | **Annual reporting**  The Accountable Authority will submit an annual self-assessment report, including evaluation of maturity across the TAS-PSPF, using a template provided by DPAC. |
| Self-assessment guidance prompt | [Provide evidence of the processes used to assess and identify progress of TAS-PSPF implementation in your agency.  Does the agency have an agency security plan that TAS-PSPF implementation can be mapped against?  Does the agency conduct a thorough deep dive to understand the effectiveness of existing protective security measures?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| GOVSEC6 | **Reporting incidents and security investigations**  The Accountable Authority will develop, implement and review processes to support the reporting and investigation of security breaches and incidents. |
| Self-assessment guidance prompt | [Provide evidence of the work the agency is doing to ensure awareness of actions that constitute a security breach/incident.  Do you have an established reporting process that your staff are familiar with?  Does your ASA take a lead role in security investigations?  Do you address learnings from security investigations?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |  |
| --- | --- | --- |
| Icon  Description automatically generated | 3.2 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| INFOSEC2 | **Protecting official information**  Agencies will adopt the Commonwealth Protective Security Policy Framework and related documentation for the classification, protective marking, transfer, handling and storage requirements of information (in any format) relative to its value, importance and sensitivity. |
| Self-assessment guidance prompt | [Provide evidence your agency’s information protection practices.  Do your staff understand security classifications, even if not using them? And do they know what to do if they see information with a classification that was not intended for them?  Does your agency have sufficient physical security measures in place to protect your information assets i.e. physical zoning, specific storage locations and containers, and information registers?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| INFOSEC3 | **Robust technology and information systems**  The Accountable Authority must ensure the security of technology and information assets to safeguard data, information and privacy, and to ensure continuous delivery of government business during all stages of the asset lifecycle. |
| Self-assessment guidance prompt | [Provide evidence of what your agency is doing to apply the Tasmanian Government cyber security principles and relevant aligning standards.  Do your ICT systems have documented business risk owner/s (system owners)?  Do you have clear procedures authorising ICT systems to a level appropriate to the highest assessed sensitive or security classified information and data it will process, store or communicate?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |  |
| --- | --- | --- |
| Icon  Description automatically generated | 3.3 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| PESEC2 | **Ongoing suitability assessment**  The Accountable Authority must ensure the ongoing suitability of their people to access official information and assets, while ensuring compliance with the TAS-PSPF. |
| Self-assessment guidance prompt | [Provide evidence of the procedures your agency has established to regularly assess the ongoing suitability of the people you engage.  Do you have standard operating procedures to determine intervals of suitability assessments and how they are conducted?  Do your managers and staff know when to report behaviours of concern and what those behaviours might be?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| PESEC3 | **Managing separating people**  The Accountable Authority must ensure adequate secure management of all separating people. |
| Self-assessment guidance note | [Provide evidence of the policies and procedures that your agency has in place to support secure management of separating people.  Do you conduct exit interviews, debriefs and formal separation procedures when a person is identified as separating?  Are managers aware of policies and procedures and are they prompt in notifying relevant security staff?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |  |
| --- | --- | --- |
| Icon  Description automatically generated | 3.4 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

|  |  |
| --- | --- |
| **Requirement** | |
| PHYSEC2 | **Agency facilities**  The Accountable Authority must consider physical security measures and ensure they are adopted and integrated in any proposed facility design, selection, development or modification. |
| Self-assessment guidance prompt | [Provide evidence of the policies and procedures that ensure physical security is appropriately adopted and integrated in your facilities.  Is physical security integrated at the concept and design stage?  Does your ASA conduct regular reviews of the agency physical security measures, confirming they remain fit for purpose?] |
| 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]

### 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** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### Practices/procedures

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

### Actions

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

# Security risk environment and capability

## 4.1 Agency risk environment

The Accountable Authority is required to provide details on the agency’s risk environment, to support the protective security measures and treatments outlined in this report. The agency’s risk environment includes the agency’s operating environment and the associated threats, risks and vulnerabilities impacting the agency’s ability to protect their critical information, people and assets.

Points for inclusion include:

* What the agency needs to protect – the identified information, people and assets which are critical to the agency’s ongoing key business functions
* What the agency needs to protect against
* How the risk is managed within the agency.

Points for consideration include:

* The aggregate value of the information holdings and classification of your agency’s IT networks
* The type of people in your agency (employees and contractors, security clearance holders or uncleared staff)
* The assets held by your agency
* Any physical security zones defined and held within your agency’s facilities.

|  |
| --- |
| Please provide your response to the Agency risk environment here: |

## 4.2 Security capability

The Accountable Authority is required to provide details on the maturity of the agency’s security capability. The security maturity component assesses the agency’s position in relation to their security environment (as discussed above) and risk tolerances.

Points for consideration include:

* How you are implementing and managing the TAS-PSPF core and supplementary requirements
* Your efforts to minimise harm to the Tasmanian Government’s assets
* The security culture you are embedding
* The agency’s ability to respond to and learn from security incidents
* The ability to achieve security outcomes while continuing to deliver your core business functions.

|  |
| --- |
| Please provide your response to the Agency security capability here: |

## 4.3 Exceptional circumstances

In accordance with the TAS-PSPF, the Accountable Authority is required to record and justify any exceptional circumstances which caused the agency to deviate from the core requirements, please see GOVSEC-4 policy for more information on exceptional circumstances.

Examples may include:

* Circumstances beyond the control of the agency
* The cost of implementation is so prohibitive it prevents the agency’s ability to perform and deliver its core business function
* Instances where alternate arrangements have been implemented to achieve equivalent or enhanced security outcomes than those applied by the minimum standard of the TAS-PSPF
* Legislative requirements that dictate your agency must address protective security differently to that outlined in the TAS-PSPF.

|  |
| --- |
| Please provide your response to any exceptional circumstances here: |

# Feedback

DPAC have provided guidance tools and education to assist with implantation of the TAS-PSPF. To improve overall performance, DPAC values your suggestions and feedback on the TAS-PSPF. Please add suggestions which you feel may aid progression and continuous improvement in the protective security landscape.

## 5.1 How could support be improved?

|  |
| --- |
| Please provide your response here: |

## 5.2 Can we help you further?

|  |
| --- |
| Please provide your response here: |