GOVSEC-4

Annual reporting

What to know

This summary sheet outlines key points from **GOVSEC-4: Annual reporting** – a policy under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF supports Tasmanian Government agencies to protect their people, information and assets from compromise and harm.

To read the TAS-PSPF or to find other summaries, policies and resources, go to **www.security.tas.gov.au**

To ensure we are all working towards a cycle of continuous improvement, every agency is required to monitor and review their protective security arrangements.

The requirement to report how we are tracking against the TAS-PSPF also makes it possible for the Tasmanian Government to maintain a solid understanding of how well the framework is protecting the security of information, people and assets across all of its agencies delivering business to the Tasmanian community.

Policy GOVSEC-4 addresses how your agency must produce an annual report about how it is meeting the requirements of the TAS-PSPF.

Assess and identify progress against the security plan

The TAS-PSPF requires regular monitoring and assessment of your agency's security capability and risk culture. This is done by considering progress against the goals and strategic objectives identified in your agency's security plan.

In meeting the requirements of the TAS PSPF, your Agency Security Advisor must put in place protective security arrangements for your agency that implement the core and supplementary requirements of the TAS PSPF, unless relevant circumstances prevent this from occurring. If this is the case, the annual self-assessment report should include justification/s for any decision to deviate from the TAS-PSPF core and supplementary requirements. It should also identify any challenges, themes and barriers which have impacted compliance.

Sharing these challenges and barriers to effective protective security can serve as a useful source of information for broader improvements to the TAS-PSPF. It also enables useful solutions or risk treatments to be identified from across government.

Where challenges or barriers are identified, the annual report should indicate how your agency will address any shortfall in the effectiveness of current protective security measures. In addition, it should identify strategies to overcome those challenges or barriers in the future.

Tasmanian Government

Assess security maturity

Security maturity is a meaningful way to demonstrate progress towards achieving or exceeding the minimum standards of the TAS-PSPF while factoring in the specific risk environment and risk tolerance of your agency.

Security maturity considers how holistically and effectively your agency:

- understands, prioritises and manages its security risks
- responds to and learns from security incidents
- fosters a positive security culture
- achieves security outcomes and core requirements while delivering business outcomes.

When you are setting security goals and maturity targets, you must seek, identify and document the best available evidence to support your agency's security maturity assessment. Information collected through security maturity monitoring can be used to inform your agency's annual self-assessment report. You can also use the information collected to validate the maturity level of your agency and determine progress toward the maturity targets identified in your agency's security plan.

Identify current vulnerabilities and key security risks

Your agency's annual self-assessment report includes consideration of current vulnerabilities and key security risks to your agency's information, people and assets.

Your agency's security risks and vulnerabilities may be influenced or changed by factors such as the risk environment, operational priorities, and security incidents. The priority of risks across your agency may change year on year as a result.

Your agency's security risk environment is determined after considering the threats, risks and vulnerabilities affecting the protection of your agency's information, people and assets, including:

- what you need to protect (via your risk assessment), this being the information, people and assets assessed as critical to your agency's ongoing key business functions
- what you need to protect against (via your threat assessment), for example, face-to-face contact with the public, shared facilities)
- how the risk will be managed within your agency.