



# PSR Assurance Framework - Guidance

A guide on how to use the PSR Assurance Framework as part of GOV 8: Assess your protective security capability.

Version date	01 October 2025
Version	1.0
Version description	Approved

Contents

Introduction ..... 3

How to assess your capability ..... 5

    01 Set target maturity ..... 5

    02 Gather / review evidence ..... 7

    03. Complete PSR Self-Assessment Tool ..... 7

    04. Verify your self-assessment..... 11

    05. Secure executive signoff ..... 12

    06. Report to us ..... 14

    07. Prioritise and plan improvements ..... 15

Tips, tricks, and advice..... 16

    Use what you already have ..... 16

    Get familiar with the Framework ..... 16

    Plan and resource your PSR assurance process ..... 18

    Be pragmatic when setting maturity targets ..... 18

    Stocktake what you have in place ..... 19

    Assess applicability of gaps against PSR requirements ..... 19

    Assessing and reporting for multi-site organisations..... 20

# Introduction

This guide will help an organisation to meet their obligations under PSR GOV 8 Assess your capability and to use the PSR Assurance Framework to set capability targets and assure that the organisation has appropriate security capability to address their risks.

Each organisation is exposed to different security risks and requires different security measures to effectively address them. Using a risk-based approach allows an organisation to tailor a protective security programme to suit its operating context and risks.

The Protective Security Requirements (PSR) Assurance Framework (Framework) enables organisations to select appropriate levels of protective security capability to address their level of risk.

The Framework is first and foremost a tool for organisations to assess themselves against the PSR mandatory requirements and to understand their protective security capability and gaps so that they can address the gaps when it is important to do so.

The PSR Assurance Framework provides objective criteria to establish expectations for a protective security programme and select the appropriate security measures to treat the organisation's security risks. As risk increases in the organisation, so too should the target capability maturity.

Effective assurance requires organisations to undertake regular and ongoing assurance activities.

The recommended processes and activities in this guide are set out to help organisations establish an effective protective security assurance process. However, it is up to each organisation to determine their own processes and activities needed for their unique situation,

This document should be read alongside the following additional guidance documents:

[PSR Capability Maturity Model](#) and [PSR Moderation Framework](#).

# The PSR Assurance Framework – key steps for reporting agencies



## 01 Set target maturity

- PSR capability maturity model (PS-CMM) levels have been updated.
- Target the minimum baseline protective security maturity level (PS-CMM 2), or select a higher target, based on your risk assessment.

## 02 Gather / review evidence

- The reporting period is 1 January to 31 December.
- Identify what has changed since your last PSR self-assessment. Gather and review evidence. Evidence guides have been updated. More guidance has been provided.
- You can record your evidence in your PSR Self-Assessment Tool but this isn't mandatory.

## 03 Complete PSR Self-Assessment Tool

- Answer questions in the new PSR Self-Assessment Tool to confirm if the measures required by the PSR are in place. Possible answers are: Yes, Partial, No, N/A, or Alternate control.
- Add commentary to support your moderation activities and provide explanations for your answers including identifying gaps and plans for improvement.

## 04 Verify your self-assessment

- We recommend that you independently verify (aka moderate) your self-assessment to provide confidence in the results. You can undertake this internally or on occasion externally.
- Adjust your answers in the PSR Self-Assessment Tool where required.

## 05 Secure executive sign off

- Complete a PSR Assurance Report summarising the finding for your Chief Executive. Draw on the tables, graphs, and results from your completed PSR Self-Assessment Tool.
- Obtain Chief Executive approval and sign off.

## 06 Report to us

- Email a copy of your final PSR Self-Assessment Tool and PSR Assurance Report to the PSR Unit by 30 April.
- These reports inform system-level analysis on protective security capability.

## 07 Prioritise and plan improvements

- Prioritise identified security capability gaps, areas of risk exposure, and planned improvements and maintain a security improvement roadmap.

# How to assess your capability

*An organisation needs to understand its operating environment and risks before deciding on what security capability it needs.*

Before beginning this process, organisations should undertake security threat and risk assessments to understand the organisation's security risks and how they change over time.

This should be regular and ongoing throughout the year to reflect changes within the organisation or environment. Consider any new or changed security threats (increased or decreased) that the organisation may be exposed to.

Refer to the [PSR protective security threat and risk guidance](#) for more support on how to identify and manage security threats and risks.

Self-assessment involves:

01. Setting target capability maturity levels based on your risk assessment
02. Gathering and reviewing evidence of capability
03. Completing a self-assessment using the PSR Self-Assessment Tool
04. Verifying self-assessment results by undertaking an independent review
05. Securing executive approval of self-assessment results and signing off the report
06. Reporting self-assessment results to PSR
07. Prioritising and planning improvements to address your risks.

## 01 Set target maturity

The PSR Assurance Framework recognises that each organisation has a unique combination of:

- people, information, and assets it needs to protect
- types of security risks to manage
- risk appetite and exposure
- funding, resources, and capability allocated to address its risks.

One size does not fit all.

The organisation's capability maturity targets should be considered and informed by the organisation's security context, potential threats, and risk appetite. This approach might drive the organisation to select different maturity targets for different locations, business activities, or security dimensions.

### Understand the PSR Capability Maturity Model

The [PSR Capability Maturity Model](#) will help organisations to select capability maturity targets. It provides details on the capability levels and measures you should put in place to achieve your target across the 20 mandatory requirements.

An organisation can also use the [PSR Enterprise Risk CMM Calculator](#) to use a standard enterprise risk framework for setting its target maturity.

The optimal capability maturity level will be unique to the organisation which balances the level of risk it is willing to accept with the level of capability and security control it can afford.

<b>Capability</b>	<b>Practice description</b>
<b>PS-CMM 5</b> <i>Optimising</i>	Security capability adapts to a dynamic, high risk operating environment. Practices are generally recognised as world leading and have near real-time measurement and response mechanisms.
<b>PS-CMM 4</b> <i>Quantitatively controlled</i>	Security capability and performance is measured, monitored; and objectively and quantitatively controlled. Security measures are hardened in response to performance alerts. Security is a strategic focus for the organisation.
<b>PS-CMM 3</b> <i>Standardised</i>	Security capability is standardised, integrated, understood, and followed consistently across the enterprise. Security performance is well governed and managed at an enterprise level.
<b>PS-CMM 2</b> <i>Planned &amp; tracked</i>	Security capability is well formed in designated business units, The security policies, capabilities, controls, and practices are in place and repeatable. They are designed to meet the organisation's core security requirements. <b>PSR minimum baseline.</b>
<b>PS-CMM 1</b> <i>Informal</i>	Security capability may be ad-hoc, unmanaged, or unpredictable. Success may rely on individuals rather than institutional capability.

*Table 1 – Overview of capability and practices as capability maturity increases*

A minimum baseline of PS-CMM 2 is required for all organisations. This means that the organisation has in place all required measures (measures expressed as 'MUST' (or 'MUST NOT') in the PSR Policy Framework.

When the organisation's faces higher risks, PSR recommends additional measures detailed at PS-CMM 3 (measures expressed as 'SHOULD' (or 'SHOULD NOT'), and PS-CMM 4 or higher (measures expressed as 'COULD') to effectively address the risks faced.

An organisation may choose to target the minimum baseline or select a higher target if it deems necessary to adequately address its risks. For example, some organisations face ongoing and serious threats to people's safety. Their targets and security measures for physical security and incident management might need to be higher than for other dimensions.

As the organisation continually re-calibrates and responds to its risk environment, it should reassess its current capability maturity and establish new capability maturity targets to ensure they remain proportionate in an ever-changing threat and risk landscape.

Building your organisation's optimal capability maturity may take several years and require investment of significant resources. Organisations should establish an effective capability development plan (see [Step 7](#) for more information). Consider setting realistic and achievable next maturity targets based on your current plan while aiming for a longer-term optimal target.

#### **PSR Self-Assessment ToolTip**

Within the **PS-CMM Target** tab, for each of the Mandatory Requirements, set your next capability target: **Agency Target PS-CMM Level** and your long-term optimal target: **Agency Optimal PS-CMM Target**.

### Different targets for different locations or functions

Be mindful that broad and disproportionately strong measures can be expensive and may impede business functions. For example, different business units or locations might have different security needs, especially when the organisation's functions are diverse. Other scenarios that might give rise to differing security needs are operating across multiple locations or in higher threat environments. In such cases, the organisation might conduct several capability assessments (for example, by using separate PSR Self-Assessment Tools) and prepare separate capability development and improvement plans.

## 02 Gather / review evidence

An organisation's self-assessment needs to be supported by evidence that demonstrates that the capability and security measures are in place.

The [PSR Moderation Framework](#) provides guidance on the indicative types of evidence you may find to support your self-assessment. Refer to the Evidence guide section for example types of:

- policies, processes, and procedures that may exist and their coverage at different levels of maturity
- practices that demonstrate the capability and how you might evidence that the practices are working as expected.

The evidence guide is intended to demonstrate possible ways in which an organisation could support its findings in the assessment. They are not intended to suggest that the specific evidence defined would be appropriate to an organisation. All organisations are different and will have different plans, policies, and practices that comprise the organisation's security settings.

#### PSR Self-Assessment Tooltip

Optionally, within the **Evidence** tab, record or update any supporting evidential documentation (e.g., policies, SOPs, and other relevant materials to support the capability assessment). This is a useful approach that will enable you to use your collected information in future periods and have visibility of when policies and processes need to be scheduled for review.

## 03. Complete PSR Self-Assessment Tool

Complete the questionnaires within the [PSR Self-Assessment Tool](#) to assess the organisation's current capability across all PSR Mandatory Requirements.

You should also refer to the [PSR Capability Maturity Model](#) for example capability and measures expected and the [PSR Moderation Framework](#) for the type of evidence that demonstrates the capability.

#### PSR Self-Assessment Tooltip




See the **Instructions** tab for detailed instructions on how to use the PSR Self-Assessment Tool to conduct your self-assessment.

Protective Security Requirements [UNCLASSIFIED]

### PSR Self-Assessment Tool instructions

This tool provides an automated and simple checklist to help your organisation review and assess that its security capability and maturity is appropriate to its level of risk. Questions are based on the policy and security measure requirements of the PSR Framework and the NCSC Minimum Cyber Security Standards

Agency name	
Date completed	
Assessor(s)	
Quality Assured by	
Business unit / department (optional)	
Update Classification when complete (this will autopopulate across the workbook)	[UNCLASSIFIED]

#### Overview

Ongoing continuous improvement in protective security requires a cycle of assessing and managing your risks in an ever-changing environment.

The self-assessment tool enables you to:

- Identify gaps in your protective security posture
- Evaluate the effectiveness of your overall protective security measures
- Understand the focus areas in which to improve your protective security
- Report back to Government on current capability maturity, as well as improvement plans.

Please see the [PSR Assurance Framework Guidance](#) for full details on the PSR self-assessment process

**To conduct a self-assessment:**

- Involve others in the self-assessment representing different parts of your organisation, from executives to specialists and take them on the journey. It is a learning process for everyone and provides a good forum for balancing needs and priorities.
- Capability maturity is not necessarily static. There may be areas that show decrease or increase over time.
- Gather the evidence that supports your assessment. This may include review of documentation of processes and procedures, security programme deliverables, evidence of measures and controls, and evidence of assurance and assessment processes. It is for the evidence generated.

#### 3. Results

The assessment tool will automatically calculate your current capability score and illustrate this in the spider diagram and other graphs in the [PSR CMM Graphs](#), [PSR All Measures Charts](#) and [MCSS Results](#) tabs. This provides snapshots of your current security capability mapped against your goals across the dimensions of the protective security framework. The PSR model has five capability and maturity levels, and the NCSC model has four (with option for five in the future once fully embedded).

The Results page also calculates your organisation's risk levels and scores by domain and the enterprise overall. This will show you if your overall capability maturity is appropriate for its enterprise-wide risk.

For organisations new to the framework, your year one results may be very different to organisations who have been on the protective security journey for multiple years.

Next step – complete the accompanying [PSR Assurance Report Template](#), incorporating key themes, priorities and general information. **Note:** including the results of the Minimum Cyber Security Standards in the Assurance Report is **optional**.

Minimum Cyber Security Standards Self-Assessment Guide

Figure 1 Example PSR Self-Assessment Tool Instructions page

## Questions instructions

The tool provides a standardised list of questions by security domain aligned to the PS-CMM and PSR policies. These questions ask organisations to assess whether measures required by the PSR are in place. **You only need to answer questions up to your Agency PS-CMM Target.**

### PSR Self-Assessment Tooltip

The selectable answers are defined in the table below. An additional **Comments/Improvement Plans** field is available to provide additional information to support your internal assurance activities and to provide additional feedback for the PSR Unit if the field turns **Red**.

Answer	Description	Score
<b>Yes</b>	The measure/capability is fully in place	Full
<b>Partial</b>	The measure/capability is partially in place. Describe in commentary any plans in place for improvement.	Half
<b>Alternate control</b>	An alternative measure is in place to provide a realistic alternative to address the specific risk. Commentary describes the measure.	Full
<b>No</b>	The measure/capability is not in place and is a gap.	Zero
<b>N/A</b>	The control / measure is not applicable to the organisation. Commentary describes the reason.	Full

Table 2 – Definitions of the answer options used within the PSR self-assessment tool questionnaires

### PSR Self-Assessment Tooltip

If your organisation believes that a required PSR measure is not appropriate to effectively manage the risk, please answer “**N/A**” and describe why you believe this to be the case.



**Note:** Answers of **N/A** and **Alternate control** will be reviewed by the PSR Unit to assess for possible future policy improvements.

### Self-assessment tool scoring methodology

Generally, an organisation should aim to have all PS-CMM-2 measures in place before moving onto PS-CMM 3.

As a methodology, each CMM level builds on the previous CMM level. For example, within GOV 1.2 Ensure functional management and governance responsibility, each of the higher maturity capabilities and measures build upon the levels below:

PS-CMM 2	PS-CMM 3	PS-CMM 4
There is clear allocation of responsibility for personnel security, information security, and physical security management.  Protective security leadership and management responsibilities and reporting lines are reviewed when relevant organisation structure, people, or responsibilities change.	'Security Manager' roles and responsibilities are formalised for personnel security, information security, and physical security with a reporting line to the CSO for those responsibilities.  Protective security leadership and management responsibilities and reporting lines are reviewed regularly, at least every two years.	Security managers drive the use of research, environment scans, and long-term planning to ensure security priorities and resource levels remain proportionate.

*Table 3 – GOV 1.2 example of how capabilities and measures build on the level below*

#### PSR Self-Assessment Tooltip

The Tool's PS-CMM score will not progress to a higher CMM level until all measures within that CMM level are indicated as either "Yes", "Alternate control", or "N/A". This is still true even if you have other CMM-3, CMM-4, or CMM-5 capability in place.

If you believe that a measure you have implemented at a higher CMM level overrides your need for a measure at a lower CMM level, **select "Alternate control"** and describe which measures override its need in the Comment field.

#### PSR Self-Assessment Tooltip

Once you have completed the self-assessment questionnaires, go to the **PSR Results** tab to review the calculated **PS-CMM Score** and **Baseline Rating**. The PSR minimum baseline is PS-CMM 2.

The **Baseline Rating** values are:

- **Achieved:** The current **PS-CMM Score** is  $\geq 2.0$
- **Not achieved:** The current **PS-CMM Score** is  $< 2.0$

MANDATORY REQUIREMENT	DOMAIN	PS-CMM SCORE	BASELINE RATING	AGENCY TARGET PS-CMM LEVEL	AGENCY OPTIMAL PS-CMM TARGET
Establish and maintain the right governance	GOV 1	PS-CMM 3	Achieved	PS-CMM 3	PS-CMM 4
Take a risk-based approach	GOV 2	PS-CMM 3.25	Achieved	PS-CMM 3	PS-CMM 4
Prepare for business continuity	GOV 3	PS-CMM 2.5	Achieved	PS-CMM 4	PS-CMM 4
Build security awareness	GOV 4	PS-CMM 4	Achieved	PS-CMM 4	PS-CMM 4
Manage risks when working with others	GOV 5	PS-CMM 2.25	Achieved	PS-CMM 3	PS-CMM 4
Manage security incidents	GOV 6	PS-CMM 3	Achieved	PS-CMM 3	PS-CMM 4
Be able to respond to increased threat levels	GOV 7	PS-CMM 3	Achieved	PS-CMM 3	PS-CMM 3
Assess your capability	GOV 8	PS-CMM 2.75	Achieved	PS-CMM 3	PS-CMM 4

Figure 2 Example PSR Preliminary Results Table

The PSR Preliminary Results Table is automatically calculated based on the answers provided in each of the questionnaires and the scoring methodology described above. There is an additional table that shows the average targets and scores across each of the domains and enterprise - wide.

## Minimum Cyber Security Standards assessment

For convenience, assurance against the Minimum Cyber Security Standards (the Standards) has been integrated into the PSR Assurance Framework.

The NCSC has developed the Standards in line with the [Government Chief Information Security Officer \(GCISO\) mandate](#). For more information on the Standards see the [NCSC website](#).

The Standards establish minimum expectations for cyber security practices by GCISO-mandated organisations. Non-mandated organisations are also encouraged to adopt the Standards.

### PSR Self-Assessment Tooltip

The PSR Self-Assessment Tool includes a questionnaire on the Standards within a separate "MCSS" tab. Where applicable, the Standards questionnaire will inherit answers already provided within the PSR self-assessment questionnaire.

Answers provided in the "MCSS" tab do not affect the organisation's PSR self-assessment scores. Separate Standards capability results scores and graphs are provided in the "MCSS Results" tab.

Refer to [NCSC](#) for more information on the Standards or the Standards assurance questionnaire.

## 04. Verify your self-assessment

Independent verification (also known as moderation) provides organisational leaders with confidence in the self-assessment results. Moderation helps an organisation improve the accuracy of their self-assessment of their protective security capability.

Moderation is an optional assurance activity that takes a holistic view of the organisation's PSR assurance capability assessment. The purpose of moderation is to independently review the PSR self-assessment findings against the evidence to confirm the results and report on any observations and conclusions. This step can be undertaken internally; however, an organisation should consider use of an external third party to undertake independent moderation on occasion.

Refer to PSR assurance and moderation section of the [PSR Moderation Framework](#) for more information on the moderation process, approach, and best practices for assurance.

A guide and tool have been created for moderators to record and track their moderation activities and results: [PSR Self-Assessment CMM and Moderator Tool](#).

This tool details the PSR Self-Assessment Tool questions with its corresponding PS-CMM capability expected, and an area to track the original vs. moderated answers (if different) and add any moderation observations as appropriate.

### Self-assessment tool answers moderation

For answers in the Self-Assessment Tool in scope for moderation, the moderator will check each assertion against the documentary and other evidence provided by the organisation as defined in the table below. The moderator will note any observations and conclusions that should be included in the [PSR Assurance Report](#) (See [Step 5](#) for more information.)

Selected answer	Moderation instructions
<b>Yes</b>	There is sufficient evidence that the measure/capability is fully in place
<b>Partial</b>	There is sufficient evidence that the measure/capability is partially in place and the comments accurately describe the gaps and any plans to address the gaps.
<b>Alternate control</b>	Comments describe the alternative measure which will provide a realistic alternative to address the specific risk.  There is sufficient evidence that the alternative measure/capability is fully in place.
<b>No</b>	There is no evidence that the measure/capability is in place.
<b>N/A</b>	The control / measure is not applicable to the organisation and the comments accurately describe the reason for that

*Table 4 Guidance for moderators based on selected self-assessment answers*

## 05. Secure executive signoff

After assessing and moderating the PSR capability self-assessment, the CSO (or their delegate) should write the [PSR Assurance Report](#) that summarises the security risks faced by the organisation, outlines the findings from the PSR self-assessment and moderation activities, and identifies the priorities and plans for improvement to address the risks.

This report is for the Chief Executive and your organisation's security leadership and should focus on areas of key capability gaps where you need to secure executive commitment and obtain resources and/or funding to drive improvements to address your specific security risks. Be sure to address the specific risks, the capability gaps, and the possible implications if not addressed. Then detail how you recommend addressing the specific gaps within the next year and beyond.

Obtain the Chief Executive's approval to sign off the PSR assurance findings.

### PSR Assurance Report tip

The Self-Assessment Tool is accompanied by a PSR assurance report template for use in writing your PSR assurance report for your Chief Executive to approve and sign off.

You can copy and paste any of the results tables, charts, or graphs provided in the PSR Self-Assessment Tool to support your report.

## Available information that may be included in the PSR Assurance Report

### CMM Table and Graph

ASSESSMENT DIMENSIONS	PS-CMM SCORE	BASELINE RATING	AGENCY TARGET	OPTIMAL TARGET
<b>GOVERNANCE (GOV)</b>				
GOV-1 Establish and maintain the right governance	1.75	Not Achieved	4.00	4.00
GOV-2 Take a risk-based approach	3.25	Achieved	3.00	4.00
GOV-3 Prepare for business continuity	2.50	Achieved	4.00	4.00
GOV-4 Build security awareness	4.00	Achieved	4.00	4.00
GOV-5 Manage risks when working with others	1.75	Not Achieved	3.00	4.00
GOV-6 Manage security incidents	3.00	Achieved	3.00	4.00
GOV-7 Be able to respond to increased threat levels	3.00	Achieved	3.00	3.00
GOV-8 Assess your capability	2.75	Achieved	3.00	4.00
<b>INFORMATION SECURITY (INFOSEC)</b>				
INFOSEC-1 Understand what you need to protect	2.50	Achieved	2.00	3.00
INFOSEC-2 Design your information security	2.50	Achieved	3.00	4.00
INFOSEC-3 Validate your security measures	2.00	Achieved	2.00	3.00
INFOSEC-4 Keep your security up to date	2.75	Achieved	3.00	3.00
<b>PERSONNEL SECURITY (PERSEC)</b>				
PERSEC-1 Recruit the right person	2.75	Achieved	3.00	4.00
PERSEC-2 Ensure their ongoing suitability	3.75	Achieved	4.00	5.00
PERSEC-3 Manage their departure	2.50	Achieved	2.00	3.00
PERSEC-4 Manage national security clearances	2.75	Achieved	3.00	4.00
<b>PHYSICAL SECURITY (PHYSEC)</b>				
PHYSEC-1 Understand what you need to protect	2.00	Achieved	2.00	2.00
PHYSEC-2 Design your physical security	2.75	Achieved	3.00	3.00
PHYSEC-3 Validate your security measures	2.00	Achieved	2.00	2.00
PHYSEC-4 Keep your security up to date	2.50	Achieved	3.00	4.00

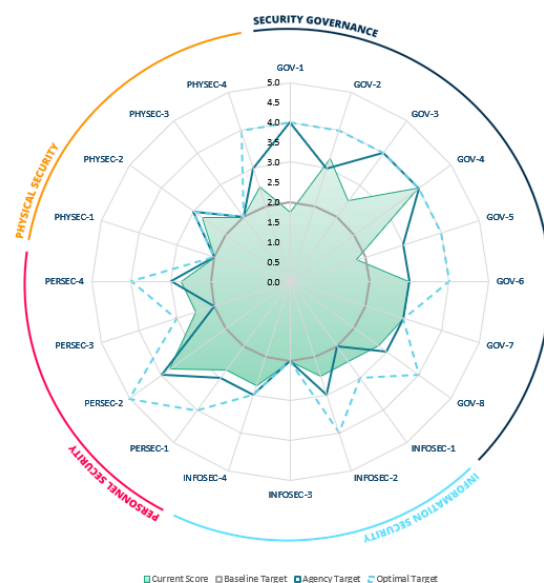


Figure 3 Example PSR Capability Maturity Table and Diagram

This is the core CMM results table and graph that provides the following information:

Information	Description
<b>PS-CMM Score</b>	The current calculated maturity score for the organisation. Note: Capability at each maturity level builds on the previous level. All required measures must be addressed at lower maturity levels before the score will move to a higher level.
<b>Baseline Rating</b>	Does the organisation meet the minimum baseline PSR requirements? Ratings values are: <ul style="list-style-type: none"> <li><i>Achieved</i> (PS-CMM Score is <math>\geq 2.0</math>),</li> <li><i>Not Achieved</i> (PS-CMM Score is <math>&lt; 2.0</math>)</li> </ul>
<b>Agency Target</b>	What is the organisation's next PS-CMM target? Targets: 2.0 (Planned and tracked / minimum), 3.0 (Standardised), 4.0 (Quantitatively controlled), 5.0 (Optimising)
<b>Optimal Target</b>	Based on the risk profile, what is the organisation's optimal (long-term) PS-CMM target? Targets: 2.0 (Planned and tracked / minimum), 3.0 (Standardised), 4.0 (Quantitatively controlled), 5.0 (Optimising)
<b>Radar diagram</b>	The goal is for the green pool to fill through the Baseline Target line (achieving the PSR baseline requirement) and through the Agency Target line. The Optimal Target line shows the long-term goal necessary to optimally address the organisation's identified risks.

Table 5 Description of the key information in Figure 2 PSR Capability Maturity Table and Diagram

## PSR Measures Charts

SECURITY GOVERNANCE (GOV)				Percentage Achieved			
	Mandatory requirement	Agency PS-CMM Target	PS-CMM Score	PS-CMM 2 (Baseline)	PS-CMM 3	PS-CMM 4	PS-CMM 5
GOV-1	Establish and maintain the right governance	PS-CMM 3	PS-CMM 2.5	100%	69%	0%	N/A
GOV-2	Take a risk-based approach	PS-CMM 3	PS-CMM 1.75	96%	63%	44%	50%
GOV-3	Prepare for business continuity	PS-CMM 4	PS-CMM 1.75	88%	50%	33%	N/A
GOV-4	Build security awareness	PS-CMM 3	PS-CMM 4	100%	100%	100%	N/A
GOV-5	Manage risks when working with others	PS-CMM 3	PS-CMM 1.75	83%	75%	75%	50%
GOV-6	Manage security incidents	PS-CMM 2	PS-CMM 3.75	100%	100%	75%	0%
GOV-7	Be able to respond to increased threat levels	PS-CMM 2	PS-CMM 1.75	86%	92%	N/A	N/A
GOV-8	Assess your capability	PS-CMM 2	PS-CMM 1.75	90%	67%	39%	0%

Figure 4 Example PSR Security Governance Measures Table

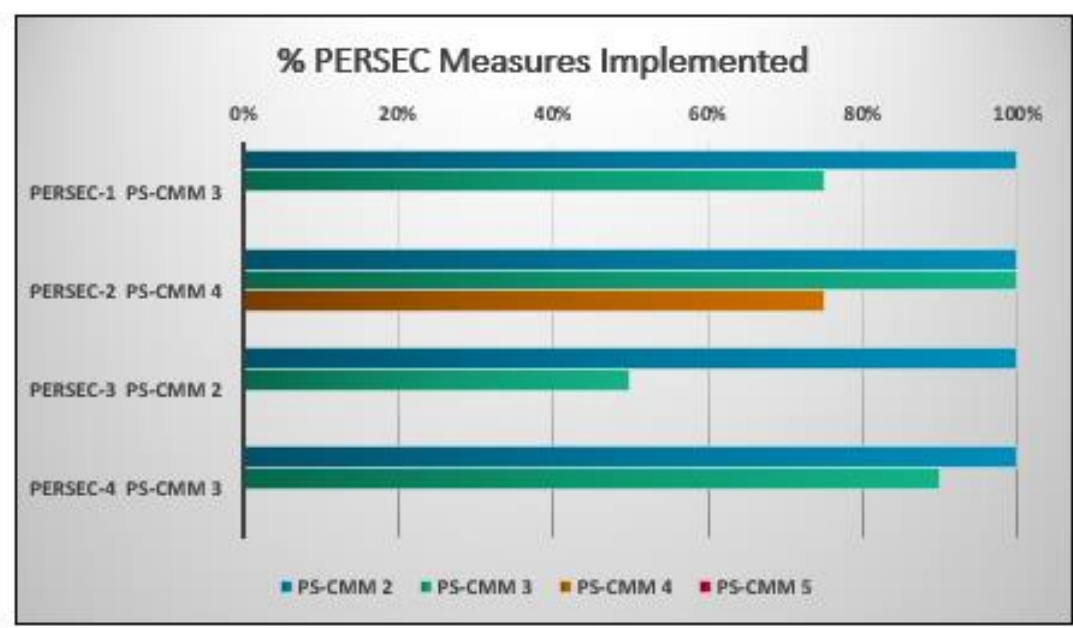


Figure 5 Example PSR Personnel Security Measures Graph

These are additional information charts and graphs that provides the following information:

Information	Description
Percentage Achieved	<p>This shows the total percentage of measures / capabilities where the answer = “Yes” or “Alternate Control” for the different maturity levels and mandatory requirements.</p> <p>This is useful to show how close an organisation is to achieving a certain capability maturity level and where they may want to focus development effort to raise their capability to address specific risks.</p> <p>It can also help identify where the organisation may have over invested in capabilities or measures at higher maturity levels than where they are currently targeting.</p>

Table 6 Description of the key information in Figure 4 and 5 Security Measures Charts

## 06. Report to us

Where mandated to do so, you should provide the PSR Unit with a copy of your completed [PSR Self-Assessment Tool](#) and [PSR Assurance Report](#). Other public sector organisations are also encouraged to report voluntarily.

If you completed multiple PSR Self-Assessment Tools for different parts of the organisation with different risk levels, you should present one PSR Self-Assessment Tool and PSR Assurance Report that represents the overall organisation. You should describe in the PSR Assurance Report the areas of the organisation that have different risk levels and how they are being managed differently.

PSR will analyse the results providing system-level insights and adjusting the PSR work programme to support agencies to lift capability to address their risks.

PSR will report to the Government Protective Security Lead (GPSL), Government Chief Information Security Officer (GCISO), and Government to inform plans for system-level national security risks.

## 07. Prioritise and plan improvements

An organisation needs to review and prioritise identified security capability gaps and improvements. This step should be undertaken at least annually to ensure that the organisation is investing in the most important security measures to address its risks.

Be sure to use the organisation's previous PSR capability assessment to identify areas of risk exposure and capability gaps for improvement.

An organisation should maintain a [PSR security roadmap](#) to record and track the security measures and actions your organisation has put in place or plans to put in place to lift or maintain the organisation's protective security capability.

# Tips, tricks, and advice

This section provides useful tips, tricks, and advice learned from organisations who applied the Framework during the 2024/25 pilot.

## Use what you already have

Initially, the Framework may feel overwhelming due the sheer volume of new resources released and question sets presented in the Tool. If your organisation has already been on the PSR assurance journey for several years, you are not starting from scratch. If you are new to reporting, the approach is very straightforward.

Use what you already have – the organisation’s existing security risk assessments, policies, procedures, treatments/measures, and existing evidence all still apply.

The PSR mandatory requirements and policies have not changed, only clarified and consolidated into PSR policy framework documents. The updated resources and new Tool provide organisations with more information on what the PSR requires and makes that transparent. The new Framework is a more quantitative assessment which makes it easier to complete.

The results may look different using this more objective approach but, in most cases, your underlying security capability is unlikely to have significantly decreased. Note though that the new Framework is a re-baselining of capability maturity using a different scale.

***You cannot compare the results using the new Framework to previous years’ results.***

## Get familiar with the Framework

Get familiar with the core resources of the PSR Assurance Framework and then refer to the rest of the background policy reference material when it’s needed.

### Core PSR Assurance Framework resources

Document Name	Description
<b>PSR Assurance Framework Guide [PDF]</b>	[This guide]. A guide on how to use the PSR Assurance Framework. This is where organisations should start to understand the PSR Assurance Framework. It takes you through the 7 key steps defined in the PSR Assurance Framework Summary.
<a href="#">PSR Self-Assessment Tool template [MS Excel]</a>	A mandatory standardised questionnaire tool used to assess capability maturity against PSR mandatory requirements and required and recommended measures. This is a core tool that you will use to undertake the self-assessment.
<a href="#">PSR Capability Maturity Model [PDF]</a>	An updated PSR Capability Maturity Model (PS-CMM) with an overview to help organisations select capability maturity targets and tables showing specific measures expected for each security domain at each capability maturity level.



Document Name	Description
<a href="#">PSR Assurance Report template Portrait [MS Word]</a> <a href="#">PSR Assurance Report template Landscape [MS Word]</a>	<p>A mandatory reporting template used to summarise the results for the Chief Executive from the PSR assurance round for the year.</p> <p>2 templates provided with different formats for the graphics pages – landscape &amp; portrait.</p>
<a href="#">PSR Moderation Framework [PDF]</a>	An updated guide to support organisations when gathering evidence and undertaking moderation of the PSR self-assessment.
<a href="#">PSR Self-Assessment CMM and Moderator Tool [MS Excel]</a>	A tool for use by moderators and auditors when verifying an organisation's PSR self-assessment. The tool outlines the questions in the PSR Self-Assessment Tool, showing the relevant requirement in the PSR Capability Maturity Model (PS-CMM) and provides a moderation area to track the original answer provided and a moderated answer (if different) and provide any moderation commentary as appropriate.
<a href="#">PSR Enterprise Risk CMM Calculator</a>	A tool to help organisations to assess their inherent enterprise security risk levels for each PSR security domain and specific mandatory requirements against a standard enterprise risk framework. This calculator will recommend a target Protective Security Capability Maturity Model (PS-CMM) level for each mandatory requirement based on criterion scores.
<a href="#">PSR Security Roadmap [MS Excel]</a>	An optional PSR roadmap template to track the security measures and practices in place, are putting in place, and are planning to put in place to protect its people, information, and assets.

## PSR Policy Reference Material

Document Name	Description
<a href="#">PSR Policy Framework Overview [PDF]</a>	Overview of the PSR mandatory requirements and sub-requirements to manage security effectively.
<b>Security Governance</b> <ol style="list-style-type: none"> <li><a href="#">PSR Policy - GOV [PDF]</a></li> <li><a href="#">PSR Appendices - GOV [PDF]</a></li> </ol>	<ol style="list-style-type: none"> <li>A core PSR policy on security governance. It details the required and recommended security measures to address risks.</li> <li>Additional security governance guidance and materials referred to within the PSR Policy – GOV document.</li> </ol>
<b>Personnel Security</b> <ol style="list-style-type: none"> <li><a href="#">PSR Policy - PERSEC [PDF]</a></li> <li><a href="#">PSR Appendices - PERSEC [PDF]</a></li> </ol>	<ol style="list-style-type: none"> <li>A core PSR policy on personnel security. It details the required and recommended security measures to address risks.</li> <li>Additional personnel security guidance and materials referred to within the PSR Policy – PERSEC document.</li> </ol>
<b>Information Security</b> <ol style="list-style-type: none"> <li><a href="#">PSR Policy - INFOSEC [PDF]</a></li> <li><a href="#">PSR Appendices - INFOSEC [PDF]</a></li> </ol>	<ol style="list-style-type: none"> <li>A core PSR policy on information security. It details the required and recommended security measures to address risks.</li> <li>Additional information security guidance and materials referred to within the PSR Policy – INFOSEC document.</li> </ol>

Document Name	Description
<b>Physical Security</b> 1. <a href="#">PSR Policy - PHYSEC [PDF]</a> 2. <a href="#">PSR Appendices - PHYSEC [PDF]</a>	1. A core PSR policy on physical security. It details the required and recommended security measures to address risks. 2. Additional physical security guidance and materials referred to within the PSR Policy – PHYSEC document.
<a href="#">PSR Glossary [PDF]</a>	An updated Glossary of Terms.

## Plan and resource your PSR assurance process

Establish a high-level plan and timeframe for the organisation's assurance process with milestones for when key steps need to be completed. Sometimes it is easiest to work backwards to get through your governance processes and Chief Executive sign off.

The first time the organisation goes through the process, it will take more time and resources as you get familiar with the concepts and understand what resources are required given the organisation's usual assessment approach.

Allow more time than you would normally allow for each step and be pragmatic about what the scope of the work may entail. Be sure that everyone involved in the assurance process is provided with information on the new Framework, process, and resources and given time and training to enable them to undertake their part of the process successfully.

**Tip:** Smaller organisations undertaking the Framework for the first time asked for and received targeted support from the PSR Unit to help them successfully design their approach at the outset. Reach out to the PSR Unit if you want targeted support.

**Tip:** Some organisations found it useful to share the new Tool and CMM resources with the people involved in self-assessment ahead of group CMM workshops so that they were able to become familiar with the self-assessment questions and PSR requirements.

**Tip:** Get started on using the tool early; give it a go and you will find things get rolling far easier. Unanimously we heard that this was most useful for agencies.

## Be pragmatic when setting maturity targets

Be realistic when choosing the organisation's next maturity target based on the available resources and improvement programmes already underway.

Use the new [PSR Capability Maturity Model](#) to help people understand the changes to the CMM levels and to set new targets. The CMM levels have changed in the new Framework and may require a reset of the organisation's current maturity targets. Also you can use the [PSR Enterprise Risk CMM Calculator](#) to set capability targets based on a standard enterprise risk framework.

The organisation only needs to answer questions in the Tool up to their target CMM level. The minimum baseline is now PS-CMM 2 which covers all MUST policy requirements within the PSR.

The organisation may have capability in place at higher CMM levels but should ensure that all capability and measures at CMM2 are addressed first as they are the core capability that higher capability builds upon.

It may be appropriate in the first year on the new Framework to target the minimum baseline to ensure that the core capability is in place before looking to target higher capability maturity.

See [Step 01 Set target maturity](#) for more information.

## Stocktake what you have in place

Have a go with using the [PSR Self-Assessment Tool](#) to understand how it works and what may need to change in the organisation's current self-assessment process.

Rather than overthinking it, many organisations have found value in just getting started answering questions and collecting evidence. Once you get going you will get a good feel for how the tool works.

Undertake a stock take of current capability and measures against what is already in place as demonstrated in the existing evidence. See [Step 02 Gather / review evidence](#) for more information.

Two key resources to help the organisation answer questions in the Tool is the [PSR Capability Maturity Model](#) and the [PSR Self-Assessment CMM and Moderator Tool](#). Also refer to the relevant section in the [PSR Policy Reference Material](#) for more information.

See [Step 03 Complete PSR Self-Assessment Tool](#) for more information.

## Assess applicability of gaps against PSR requirements

The Framework has been updated to enable it to respond to organisations' unique risk settings while also informing possible future PSR Framework policies, guidance, and tools.

It does this by allowing organisations to select "N/A" and "Alternate Control" when appropriate. Commentary must be provided when these are selected as it will help inform possible future PSR Framework updates.

### Alternate control

For those areas where there may be gaps against the PSR requirements, an alternative measure may be in place to provide a realistic alternative to address the specific risk. This may include different risk treatments or measures already implemented at higher PS-CMM levels.

For example, the measure may not be covered in policy documentation (CMM 2); however, an automated system enforces the measure across your enterprise (CMM 3).

Based on the organisation's risk assessments and treatments, assess how important the required PSR measure is to address your specific risks. If there is disagreement with the policy requirement, use "Alternate control" and describe why this is the case.

### Not applicable (N/A)

Some of the measures required by the PSR may not be applicable to the organisation if the risk does not exist. If this is the case, answer "N/A" on the question and describe why it does not apply. E.g., The organisation does not have clearance holders that it is responsible for managing the clearance for. Therefore, it does not require measures for managing clearance holders.

## Assessing and reporting for multi-site organisations

The **PSR Self-Assessment Tool** does not currently cater for collating and summarising information from multiple sites into a single standard report. Organisations with multiple sites will need to continue to do whatever they do today to assess and understand the risks and capabilities in the multi-site environment.

For example, an organisation may decide to conduct different self-assessments for sites with different risk-profiles using a separate PSR Self-Assessment Tool for each risk-profile grouping. In this situation, the organisation should submit to the PSR Unit, the one PSR Self-Assessment Tool that represents most of the organisation and within the **PSR Assurance Report** to the Chief Executive, summarise and reflect on the findings within the other risk-profile self-assessments undertaken.