

MINIMUM CYBER SECURITY STANDARDS GUIDANCE

2025



Te Tira Tiaki
Government Communications
Security Bureau

www.ncsc.govt.nz

Contents

Ngā kaupapa

Purpose of this Guidance	3
The Standards	3
Cyber Security Capability Maturity Model (CS-CMM)	4
PSR Self-Assessment Tool	9

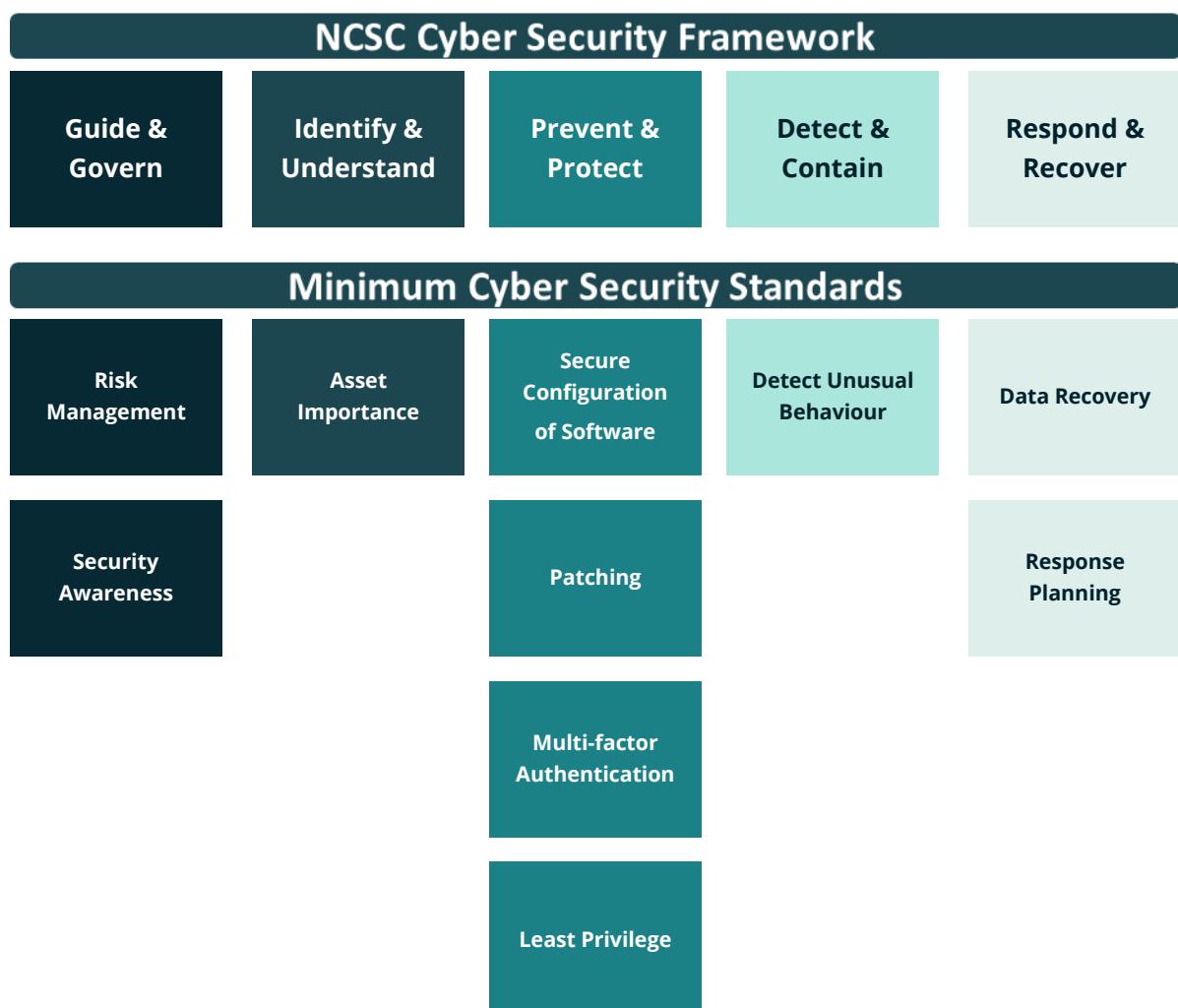
Purpose of this Guidance

This guidance is intended for GCISO agencies who will be required to implement the Standards. The information provided is specially tailored to help agencies determine the appropriate capability maturity levels as well as how to complete the PSR self-assessment process as part of the [PSR Assurance Framework](#). Agencies should acquaint themselves with the supporting information provided within each of the Standards, as they lay out the steps to implement, track and measure progress against the maturity requirements.

Non-mandated agencies wishing to adopt this guidance are welcome to do so.

The Standards

The NCSC's Cyber Security Framework provides a basis for the development of the Standards. The below diagram illustrates how the 10 Standards align with the five functions of the NCSC Cyber Security Framework.



The Standards were selected based on our assessment of the most likely vectors for attack, as well as actual incidents that have occurred, and discussions held with government agencies during the scoping stage.

Although the 10 Standards do not cover the entire cyber security spectrum, they are an important standalone tool that provides alignment between policy requirements as established in the Protective Security Requirements, the NCSC's Cyber Security framework, and the technical controls within the NZISM.

The guidance contained in this document is intended to provide organisations with sufficient information to enable them to establish current capability maturity levels and determine whether this is appropriate for their environment. This document also provides guidance on completing the self-assessment questionnaire contained in the PSR Self-Assessment Tool.

Scope

The Standards apply to all business-critical and externally facing systems, where applicable. These are defined as follows:

Business-critical: systems and applications that must function for an organisation to conduct normal business operations, which includes internal and external systems.

Externally facing: systems and applications that are outside of the authorisation boundary established by the organisation and fall under the business-critical definition or has connectivity to a business-critical system(s).

Cyber Security Capability Maturity Model (CS-CMM)

A maturity model helps organisations to evaluate their maturity against the security requirements set out in the Standards. The model is aligned with the PSR Capability Maturity Model (PS-CMM). The PSR model has five levels; however, for the purpose of the Minimum Cyber Security Standards, four levels will be used at present (CS-CMM 1 to 4). In the future we will review the levels to determine whether a fifth level is required.

The CS-CMM levels are described below:

CS-CMM 5 Optimising	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.
CS-CMM 4 Quantitatively controlled	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.
CS-CMM 3 Standardised	Security capability is standardised, integrated, understood, and followed consistently across the enterprise. Security is well-governed and managed at an enterprise level.
CS-CMM 2 Planned & Tracked	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.
CS-CMM 1 Informal	Security capability may be ad-hoc, unmanaged, or unpredictable. Success may rely on individuals rather than institutional capability.

Minimum maturity level – CS-CMM 2

The minimum maturity level set for the Standards is *CS-CMM 2 – Planned and Tracked*. This level is appropriate since its intended outcomes focus primarily on organisational core security requirements. As stated, the intent of the Standards is to focus on security requirements impacting critical systems. To ensure there are adequate security settings to safeguard these assets, organisations need to have in place established policies, controls, and capabilities to maintain a satisfactory risk posture.

Over time, the minimum capability maturity level will be reviewed to ensure they adequately address the current security and threat environment. Results from the next PSR assurance round using the new PSR Self-Assessment Tool will be significant in helping us make this determination. Consideration will be given to the following factors:

- Whether the current minimum maturity level CS-CMM 2 is appropriate or should be elevated, and
- Whether different CS-CMM levels should be set for different standards or whether one level across all 10 Standards is appropriate.

Agencies should undertake a risk assessment to determine whether CS-CMM 2 is the appropriate level for their organisation. For some, the maturity level may need to be at a higher level, either for all the Standards or for a selection. Factors to consider include:

- The value of information the agency stores, transmits, or processes, either in isolation or in aggregate.
- Previous security breaches (and their severity), incidents, or near-misses.
- The results of risk assessments or threat intelligence received.
- An expansion or reduction in business operations, and the corresponding changes in the number of business-critical and/or externally facing systems, or provisioning of critical services.
- Changes in the existing architecture or operating model (for example, cloud adoption).

The intent of the minimum capability maturity level is to:

1. set minimum safeguards across the mandated agencies so that a baseline exists, and
2. facilitate the uplift of cyber resilience in the 10 areas.

The capability maturity levels are designed to assist in achieving these goals by providing a pathway for increasing maturity over time.

Although the minimum capability maturity level has been set at CS-CMM 2, we suggest that agencies adopt or work towards meeting the CS-CMM 3 'Standardised' capability maturity level. Since CS-CMM 3 requirements cover the entirety of an agency, they will help to ensure that security settings include the breadth and depth of business operations.

The differences between the two levels are shown in the diagram below:



How requirements for capability maturity levels are structured

Each Standard contains an intent statement. The purpose of these is to define and summarise the Standard. The intent statement also outlines the security risk(s) the standard is addressing.

Organisations have also told us that a more prescriptive set of measures and requirements would assist them with understanding and implementing the Standards. Where applicable, the requirements have been designed to incorporate preventive, compensatory, and detective measures. The requirements have also been designed to enable organisations to retain a level of flexibility in the solutions currently in existence or in development (for example, products, business processes, and delivery channels).

Assessing your current capability maturity level

This section provides guidance for organisations on how to assess their current capability maturity level against the Standards.

As a self-assessment for the Standards has not previously been a requirement for organisations, establishing a baseline—and being able to demonstrate its requirements are being met—will assist in planning for ongoing cyber resilience uplifts.

While each organisation is best-placed to determine their own methodology for measuring their current capability maturity level, the following process is one option that may be adopted or modified when completing the self-assessment process. The intent is to ensure that the process is as efficient as possible. Figure 1 shows the recommended steps to complete the self-assessment.

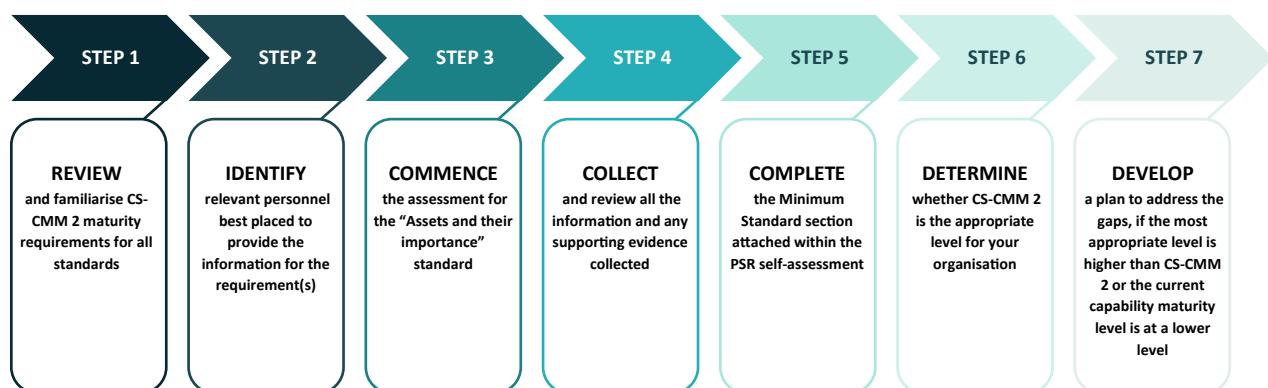


Figure 2 provides additional supporting information to complete the steps in the self-assessment:



Figure 2

PSR Self-Assessment Tool

The PSR Self-Assessment Tool includes a questionnaire on the Standards in the MCSS tab. Where applicable, the Standards questions will inherit answers already provided within the tool.

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.

Self-assessment questions

This section focuses on how organisations should answer the self-assessment questionnaire for maturity requirements. Each question contains a drop-down box with three options to choose from. Below are the options with explanations:

Option	Explanation
Yes	A <i>yes</i> response should be selected if all conditions for the maturity requirements are currently in place.
No	A <i>no</i> response should be selected if none of the conditions for the maturity requirements is currently in place.
Partial	A <i>partial</i> response should be selected if only some of the requirements are in place, or the requirements are not being met, but future work is planned.

Each question has the option to provide commentary in a free-text field. Using this field is not compulsory, but organisations are encouraged to complete this if the additional information will provide greater clarity or context. Organisations may wish to provide the following information:

- Reason(s) for the current maturity state.
- Planned investment in the future.
- Assurance measure(s) in place around the maturity requirements.
- Whether there has been an increase or decrease in maturity for the requirement.

PSR and MCSS reporting periods

To reduce the reporting burden for agencies, self-assessment for the Standards is integrated into the PSR Self-Assessment Tool. The tool centralises the PSR and Minimum Standards self-assessment in one location, for completion at the same time. The reporting period for Minimum Standards will run from 1 November 2025 to 30 April 2026 coinciding with the PSR assurance round. The PSR reporting period is the calendar year (1 January to 31 December). The NCSC will be aligning with the PSR reporting period from November 2026 after the Standards have been embedded.

The tool takes inputted self-assessment scores and provides the results diagrammatically. The results are in the MCSS Results worksheet. The radar diagram (or 'spider') provides a visual representation of an organisation's maturity levels for the Standards.

Note: The results will only be available to mandated agencies with access to the self-reporting tool.

Figures 3 and 4 are examples of the MCSS results outputted from the PSR Self-assessment tool.

MINIMUM CYBER SECURITY STANDARDS		Percentage Achieved			BASELINE RATING (CS-CMM 2)	
ASSESSMENT DIMENSIONS		CS-CMM SCORE	CS-CMM 2	CS-CMM 3	CS-CMM 4	
MS-1	Cyber Risk Management	3.25	100%	100%	25%	Achieved
MS-2	Security Awareness	3.75	100%	100%	83%	Achieved
MS-3	Identifying Assets & Understanding their Importance	2.75	100%	88%	50%	Achieved
MS-4	Secure Configuration for Software and Applications	4.00	100%	100%	100%	Achieved
MS-5	Guidance for Patching	2.75	100%	75%	100%	Achieved
MS-6	Multi-Factor Authentication Measures	2.75	100%	75%	25%	Achieved
MS-7	Detect Unusual Behaviour	2.75	100%	92%	63%	Achieved
MS-8	Least Privilege	3.75	100%	100%	75%	Achieved
MS-9	Data Recovery	1.75	90%	100%	38%	Not Achieved
MS-10	Response Planning	1.75	88%	100%	83%	Not Achieved

ASSESSMENT AVERAGES	Average Score	Average CS-CMM 2	Average CS-CMM 3	Average CS-CMM 4	Average Baseline Rating
	CS-CMM 3	98%	93%	64%	Achieved

Figure 3

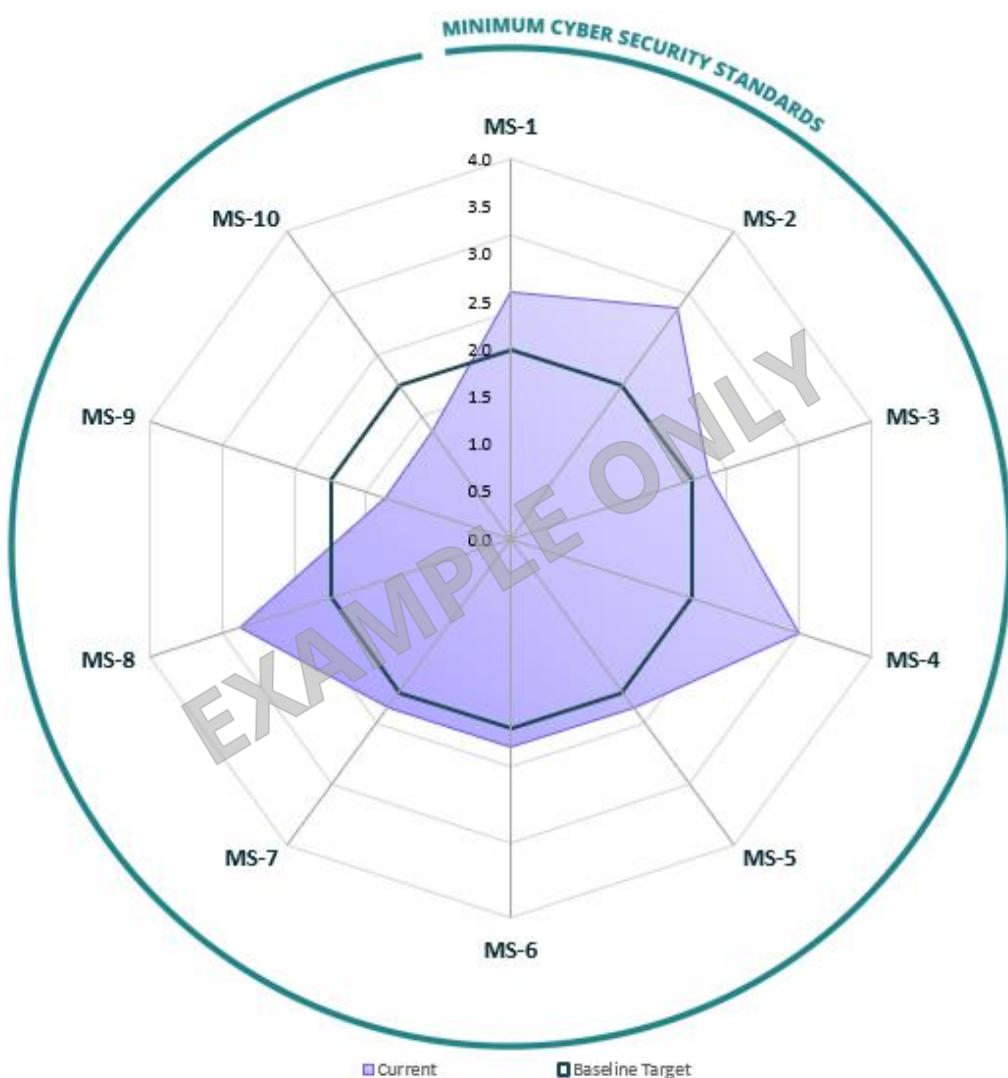


Figure 4

At the conclusion of the self-assessment exercise, please return the completed Excel file to the PSR team at psr@protectitvesecurity.govt.nz.

Glossary

A glossary including commonly used terminology and acronyms is included to complement the Standards. Due to the interchangeability of some terms, the glossary was developed to reduce the risk around varying interpretations and ambiguity.