Self-assessment report

Name of organisation

Due: 30April 2025 By email: to [psr@protectivesecurity.govt.nz](mailto:psr@protectivesecurity.govt.nz)

# Introduction

## Purpose

Cabinet has noted that good security practice and capability is the accountability of every Chief Executive and should be commensurate with the specific level of risk carried by the organisation.

This report is designed to assist Chief Executives to know if their security measures are appropriate, where improvements are needed, and help them plan for the future.

Reporting also provides assurance information to lead security agencies and helps the PSR team and the Security System Leads understand what further support is needed.

Your completion, and provision of this report to your Chief Executive and the PSR Team aligns with GOV8 - Assess your capability.

## 2024/25 Interim Self-Assessment

This template is for agencies not participating in the pilot of the new Assurance Framework. It includes minor changes from last year’s template that are outlined in the PSR Annual Self-Assessment Information Sheet

## The report has 2 sections:

* The Chief Security Officer’s (CSO) summary for the Chief Executive including summary of their capability maturity assessment.
* Report on compliance with PSR mandatory requirements.

## How your information will be used

Your organisation’s information will be consolidated into an aggregated summary report on system-wide progress in improving protective security.

Information may be shared with those responsible for building protective security capability ingovernment. These include the New Zealand Security Intelligence Service (NZSIS), the Government Communications Security Bureau (GCSB), the Department of the Prime Minister and Cabinet, Te Kawa Mataaho - Public Service Commission, the Department of Internal Affairs, the National Security Board (NSB) and the Minister responsible for the NZSIS and GCSB.

Any Official Information Act requests will be assessed on a case-by-case basis in consultation with organisations. The PSR team will transfer any requests for completed reports directly to the organisations concerned.

Please review the classification of your completed report and update protective marking as appropriate.

**Contact** the PSR team at [psr@protectivesecurity.govt.nz](mailto:psr@protectivesecurity.govt.nz) if you would like more guidance on the self-assessment reporting process.

# 

# Summary for the Chief Executive (for CSO to complete)

|  |  |
| --- | --- |
| Organisation: |  |
| Report as at 31 March 2025 | **(Note: to be delivered on or before 30 April 2025)** |

### Significant changes to our organisation’s security profile in the last 12 months (if any):

[In this section, summarise your current significant protective security risks and any changes to your organisation’s security profile. This should include direct or indirect security events such as major security incidents, organisational changes, or legislative changes that could impact your security profile. It should also summarise key improvements or actions taken this year to reduce your security risks.]

[In each section below, summarise the significant risks/changes across the four protective security domains.]

#### Governance (GOV1–GOV8)

* [Summary of key themes across Governance]

#### Personnel Security (PERSEC1–PERSEC 4)

* [Summary of key themes across PERSEC]

#### Information Security (INFOSEC1–INFOSEC4)

* [Summary of key themes across INFOSEC]

#### Physical Security (PHYSEC1–PHYSEC4)

* [Summary of key themes across PHYSEC]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Summary of our compliance with the 20 PSR Mandatory Requirements[[1]](#footnote-2)** | | | | | | | |
|  | **GOV1** | **GOV2** | **GOV3** | **GOV4** | **GOV5** |
| Status: |  |  |  |  |  |
|  | **GOV6** | **GOV7** | **GOV8** | **PERSEC1** | **PERSEC2** |
| Status: |  |  |  |  |  |
|  | **PERSEC3** | **PERSEC4** | **INFOSEC1** | **INFOSEC2** | **INFOSEC3** |
| Status: |  |  |  |  |  |
|  | **INFOSEC4** | **PHYSEC1** | **PHYSEC2** | **PHYSEC3** | **PHYSEC4** |
| Status: |  |  |  |  |  |

### Our protective security priorities for the next 12 months:

[Include in this section your plans for improving your organisation’s ability to comply with the mandatory requirements. Specify how these improvements will aid the organisation in achieving your protective security goals.

Identify any significant obstacles you face in achieving/maintaining your protective security goals and how these obstacles will be addressed.]

### PSR Unit support:

[Describe what PSR support or action you would like in the coming year]

**Summary of our organisation’s protective security capability maturity:**

Our organisation has completed the PSR Capability Maturity Assessment and the information provided in this report reflects the key findings and our plans for the next year.

### Summary of our organisation’s protective security capability maturity[[2]](#footnote-3):



#### Key findings from the CMM assessment

[In this section, summarise key CMM findings from your latest CMM assessment. Identify the CMM dimensions targeted this year and the improvements/achievements undertaken.]

#### Recommended actions for next 12 months

[In this section, summarise your recommended CMM capability focus areas and planned actions for the next year.]

### Report verification

[In this section, describe how you have verified the self-assessment findings this year (e.g. internal audit / assurance processes, independent assurance process, or moderation undertaken by an external entity or person).]

### Report approval

|  |
| --- |
| **Chief Executive comments:** |
| I confirm I have reviewed this completed self-assessment for my organisation and approve for it to be submitted to the PSR.  **Chief Executive signature:** |
| **Dated:** |

# PSR mandatory requirements

For each requirement enter one of the following status values into the tables below.

|  |  |
| --- | --- |
| Status | Description |
| **Meets** | You currently meet the requirement. |
| **Mostly meets** | You have the structures, policies, processes and / or resources in place that are needed to meet the requirement, however these are not yet fully rolled out across your organisation. |
| **Partially meets** | You have delivered some of the elements needed to meet the requirement. Remaining work is underway and progressing as planned. |
| **Progress planned** | You have a programme of work in place that includes work to meet the requirement; and the plan is appropriately phased and resourced. |
| **Does not meet** | You have not yet defined or planned the work needed to meet the requirement. Alternatively you have started work but there are significant risks it cannot be completed. |

Please ensure that below each status value you enter, you provide evidence of policy and practice to support your assessment. A guidance on evidence of policy & practice can be found at [**www.protectivesecurity.govt.nz/self-assessment-and-reporting**](http://www.protectivesecurity.govt.nz/self-assessment-and-reporting)

Please note that this guidance is indicative only and your own evidence will likely extend beyond these examples or be demonstrated in wider agency policies. This list may identify any gaps in your current capability and is to be used as a guide only.

#### How To Guide

The PSR team has developed and provided a PSR-Self-Assessment-Reporting How To Guide to accompany this template. The purpose of the guide is to demonstrate what good evidence looks like to support the rating you have assessed for each mandatory requirement.

This includes a general summary, an audit of current policy and standard operating procedures, an outline of the specific practise and initiatives that are underway, and the specific actions that will be taken in the coming year to either uplift or maintain your agency’s rating.

Ensure you read the advice regarding not repeating content in the tables of policy and practice.

[**Link to PSR Self-Assessment Reporting How To Guide 2022/23**](https://protectivesecurity.govt.nz/assets/Governance/PSR-Self-Assessment-Reporting-How-to-Guide-2223.pdf)

**The supporting documentation excel spreadsheet** is available if you wish to collate evidence of policy and practice rather than within each mandatory requirement.

## Security governance

|  |  |  |
| --- | --- | --- |
| Requirement | | Status |
| **GOV1** | **Establish and maintain the right governance**  Establish and maintain a governance structure that ensures the successful leadership and oversight of protective security risk.  Appoint members of the senior team as:   * Chief Security Officer (CSO), responsible for your organisation’s overall protective security policy and oversight of protective security practices. * Chief Information Security Officer (CISO), responsible for your organisation’s information security.   …………………………………………………………………………………………………  **Self-assessment Prompt:**  Please identify the key members within your security governance structure. Please also describe any committees responsible for security across all four domains, and how their duties and responsibilities are defined and documented. In addition, please describe what security reports, including cyber, are provided to your agency’s executive leadership. |  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 1?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV2** | **Take a risk-based approach**  Adopt a risk-management approach that covers every area of protective security across your organisation, in accordance with the New Zealand standard *ISO 31000:2018 Risk management – guidelines.*  Develop and maintain security policies and plans that meet your organisation’s specific business needs. Make sure you address security requirements in all areas: governance, information, personnel, and physical.  ………………………………………………………………………………………..  **Self-assessment Prompt:**  Please evidence the security policies and standards, including cyber; describe how they align with your agency’s strategic outcome; and how staff are inducted or receive training on them. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 2?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV3** | **Prepare for business continuity**  Maintain a business continuity management programme, so that your organisation’s critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.  ………………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please evidence your business security plans, and describe your agency’s approach in identifying and prioritising its critical services, assets and information. This should include any information exchanges with other organisations or external parties. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 3?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV4** | **Build security awareness**  Provide regular information, security awareness training, and support for everyone in your organisation, so they can meet the Protective Security Requirements and uphold your organisation’s security policies.  ………………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please outline your agency’s approach/programmes relating to security awareness training, including guidance on the relevant sections of legislation covering the unauthorised disclosure of official information, and conditions attached to national security clearances. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 4?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV5** | **Manage risks when working with others**  Identify and manage the risks to your people, information, and assets before you begin working with others who may become part of your supply chain.  ………………………………………………………………………………………………………………………………...  **Self-assessment Prompt:**  Provide detail on processes to identify and assess supply chain risk (including national security risk under *New Zealand Government Procurement Rule 44: Reasons to exclude a supplier*), and select vendors; and include whether cyber security is considered. In addition, please elaborate on security requirements in your agency’s contract arrangements and whether there are policies and procedures for the ongoing management of third-parties. Please also indicate if third-parties are required to report security incidents. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 5?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV6** | **Manage security incidents**  Make sure every security incident is identified, reported, responded to, investigated, and recovered from as quickly as possible. Ensure any appropriate corrective action is taken.  ……………………………………………………………………………………………………………………………….  **Self-assessment Prompt:**  Please detail your agency’s approach to managing security incidents – this could include triage, categorisation, incident reviews, cause identification, response plans, testing and reporting requirements (i.e. to NCSC for cyber incidents). | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 6?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV7** | **Be able to respond to increased threat levels**  Develop plans and be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets.  ………………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please outline your plans for heightened security levels and how they integrate and coordinate with other emergency prevention and response plans (e.g. fire, power failure, civil defence emergency etc.). | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 7?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **GOV8** | **Assess your capability**  Use an annual evidence-based assessment process to provide assurance that your organisation’s security capability is fit for purpose. Provide an assurance report to Government through the Protective Security Requirements team if requested.  Review your policies and plans every two years, or sooner if changes in the threat or operating environment make it necessary.  ………………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please outline your agency’s approach or methods to monitoring, reporting, reviewing and auditing policies and procedures as part of the self-assessment process. What assurance do you have that your security policies and procedures are being followed? Is your agency aware of when information needs to be archived, destroyed, repurposed or disposed of securely? | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for GOV 8?**

* [Detail action on how to achieve or maintain rating]

## Personnel security

| Requirement | | Status |
| --- | --- | --- |
| **PERSEC1** | **Recruit the right person**  Ensure that all people working for your agency (employees, contractors, and temporary staff) who access New Zealand Government information and assets:   * have had their identity established * have the right to work in New Zealand * are suitable for having access * agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.   …………………………………………………………………………………………………………………………..  **Self-assessment Prompt:**  Outline your agency’s approach to pre-employment checks, and security expectations during staff and third-party induction. |  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PERSEC 1?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **PERSEC2** | **Ensure their ongoing suitability**  Ensure the ongoing suitability of all people working for your agency. This responsibility includes addressing any concerns that may affect the person’s suitability for continued access to government information and assets.  …………………………………………………………………………………………………………………………….  **Self-assessment Prompt:**  Please outline your agency’s approach to managing and assessing your people’s ongoing suitability to access information and assets. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PERSEC 2?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **PERSEC3** | **Manage their departure**  Manage people’s departure to limit any risk to people, information, and assets arising from people leaving your agency. This responsibility includes ensuring that any access rights, security passes, and assets are returned, and that people understand their ongoing obligations.  ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please discuss your agency’s approach to the off-boarding and departure of staff, and what, if any, risk assessments are conducted as part of this process. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PERSEC 3?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **PERSEC4** | **Manage national security clearances**  Ensure people have the appropriate level of national security clearance before they are granted access to CONFIDENTIAL, SECRET and TOP SECRET information, assets, or work locations.  Manage the ongoing suitability of all national security clearance holders to hold a clearance and notify NZSIS of any changes regarding their clearance.  ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Please outline your agency’s approach to managing national security clearance holders and their ongoing suitability to access information and assets. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PERSEC 4?**

* [Detail action on how to achieve or maintain rating]

## Information security

|  |  |  |
| --- | --- | --- |
| Requirement | | Status |
| **INFOSEC1** | **Understand what you need to protect**  Identify the information and ICT systems that your organisation manages. Assess the security risks (threats and vulnerabilities) and the business impact of any security breaches.  …………………………………………………………………………………………………………………………..  **Self-assessment Prompt:**  Discuss the information security measures your agency has in place to know what you have and how your agency would be affected by any loss or harm. |  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc]   **Additional INFOSEC1 questions from NCSC:**   1. **How does your agency manage the ownership of, and accountability for, your ICT assets?** 2. **How does your agency manage information security assets based on criticality and sensitivity?** | | |

**How will you achieve or maintain a ‘Meets’ for INFOSEC 1?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **INFOSEC2** | **Design your information security**  Consider information security early in the process of planning, selection, and design.  Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with:   * the *New Zealand Government Security Classification System* * the *New Zealand Information Security Manual* * any privacy, legal, and regulatory obligations you operate under.   Adopt an appropriate information security management framework that is appropriate to your risks.  ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  What tools have been developed for key information security domains to enable the deployment of service solutions? | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc]   **Additional INFOSEC2 questions from NCSC:**   1. **How well does your agency integrate security as a part of your procurement, design, and management of ICT assets?**    1. **What security considerations do you adopt for your security architecture? For example, zero trust.** 2. **What aspects of information technology does your organisation find challenging, taking into account people, processes and technology?** | | |
|  | | |

**How will you achieve or maintain a ‘Meets’ for INFOSEC 2?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **INFOSEC3** | **Validate your security controls**  Confirm that your information security measures have been correctly implemented and are fit for purpose.  Complete the certification and accreditation process to ensure your ICT systems have approval to operate.  ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Describe how your agency validates its security measures and whether they will reduce risks to an acceptable level. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc]   **Additional INFOSEC3 questions from NCSC:**   1. **Do you conduct C&A audits during system lifecycle to review and validate your information security measures?**    * **If yes – can you please describe your process for undertaking C&A audits?**    * **If no – please describe your process.** 2. **What information security support, tools and advice do you need?** | | |

**How will you achieve or maintain a ‘Meets’ for INFOSEC 3?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **INFOSEC4** | **Keep your security up to date**  Ensure that your information security remains fit for purpose by:   * monitoring for security events and responding to them * keeping up to date with evolving threats and vulnerabilities * maintaining appropriate access to your information.   ………………………………………………………………………………………………………  **Self-assessment Prompt:**  Describe how your agency keeps information security up to date and in line with evolving threats and vulnerabilities. Detail how your agency responds to information security incidents. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc]   **Additional INFOSEC4 questions from NCSC:**   1. **How does your agency identify, keep itself up-to-date with and manage new threats and vulnerabilities?** 2. **Does your agency have a criteria to help determine the frequency at which threats and vulnerabilities need to be identified and actioned? What mechanism will they use to take action?** | | |

**How will you achieve or maintain a ‘Meets’ for INFOSEC 4?**

* [Detail action on how to achieve or maintain rating]

## Physical security

| Requirement | | Status |
| --- | --- | --- |
| **PHYSEC1** | **Understand what you need to protect**  Identify the people, information, and assets that your organisation needs to protect, and where they are. Assess the security risks (threats and vulnerabilities) and the business impact of loss or harm to people, information, or assets. Use your understanding to:   * protect your people from threats of violence, and support them if they experience a harmful event * protect members of the public who interact with your organisation * put physical security measures in place to minimise or remove risks to your information assets.   ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  Outline your agency’s approach to assessing physical security vulnerabilities and the level of risk they pose. |  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PHYSEC 1?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **PHYSEC2** | **Design your physical security**  Consider physical security early in the process of planning, selecting, designing, and modifying facilities.  Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with relevant health and safety obligations.  …………………………………………………………………………………………………………………………….  **Self-assessment Prompt:**  Assess how your agency evaluates risks and prepares plans; complies with security zone requirements; applies good practice in physical security design; implements physical security measures; includes physical security in business dealings; and manages planning and building processes | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PHYSEC 2?**

* [Detail action on how to achieve or maintain rating]

|  |  |  |
| --- | --- | --- |
| **PHYSEC3** | **Validate your security controls**  Confirm that your physical security measures have been correctly implemented and are fit for purpose.  Complete the certification and accreditation process to ensure that security zones have approval to operate.  ……………………………………………………………………………………………………………………………  **Self-assessment Prompt:**  How does your agency decide if physical security measures have been well-managed and allow governance responsibilities to be met, and risks have been properly identified? | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PHYSEC 3?**

* [Detail action on how to achieve or maintain rating

|  |  |  |
| --- | --- | --- |
| **PHYSEC4** | **Keep your security up to date**  Ensure that you keep up to date with evolving threats and vulnerabilities, and respond appropriately.  Ensure that your physical security measures are maintained effectively so they remain fit for purpose.  …………………………………………………………………………………………………………………………..  **Self-assessment Prompt:**  Describe how your agency keeps physical security up to date and in line with evolving threats and vulnerabilities. Detail how your agency responds to physical security incidents. | **STATUS** |
|  |
| ***Evidence of policy and practice to support status:***  **SUMMARY**  [Summarise information below here]  **POLICY/DOCUMENTATION** \*Complete below or in new separate excel spreadsheet   |  |  |  |  | | --- | --- | --- | --- | | Document name | Last Reviewed | Next Review | Link/Doc ID | | [NAME] [POLICY/SOP] | [DATE] | [DATE] | XX-1234 | |  |  |  |  | |  |  |  |  | |  |  |  |  |   **PRACTICE**   * [Detail initiative, governance group action, response to incidents, assessments completed etc] | | |

**How will you achieve or maintain a ‘Meets’ for PHYSEC 4?**

* [Detail action on how to achieve or maintain rating]

1. Manually enter into this chart your status level *(Meets/ Mostly Meets/ Partially Meets/ Progress Planned/ Does not Meet*) for each requirement. [↑](#footnote-ref-2)
2. Insert a copy of your organisation’s CMM table and spider diagram. [↑](#footnote-ref-3)