PSR | Protective Security Requirements

GUIDE TO EVIDENCING ASSESSMENTS IN THE PSR ANNUAL SELF-ASSESSMENT REPORT

PURPOSE

The purpose of the guide is to demonstrate how the 2022/2023 PSR Annual Self-Assessment Report template should be used to support the rating you have assessed for each mandatory requirement.

HOW TO USE THE UPDATED TEMPLATE

This guide includes examples intended to demonstrate the way in which the ratings for the mandatory requirements could be supported within the template. While these are real examples, although sanitised, they are not intended to suggest that the specific evidence defined would be appropriate for your agency. All agencies are different and will have different plans, policies and practices that comprise an agency's security profile and settings. The plans, policies and practices that are fit for purpose for your agency is what should be detailed in this assessment template.

The most important change to note in the template this year is the structure and guiding prompts. The changes to the template and this guide are aimed to assist you in understanding how to provide appropriate evidence to support your rating against the mandatory requirement.

Should you have any concerns with the use of the updated template, please contact the PSR team for information or advice.

GOV2: EXAMPLE OF EVIDENCE REQUIRED TO SUPPORT RATING

The below example is provided to demonstrate what is required to support the rating you have assessed for each mandatory requirement.

This includes a general summary, an overview/stocktake of current policy, practice and standard operating procedures, an outline of the specific practice and initiatives that are underway, and any specific actions that will be taken in the coming year to either uplift or maintain your agency's rating. The sections are provided in the accompanying PSR self-assessment template.

EXAMPLE ONE

Requirement		Status
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.	**MEETS**

Evidence of policy and practice to support status:

SUMMARY

[*This section is for you to summarise information detailed below as an overview of this mandatory requirement]*

The agency has a number of initiatives and policies designed to be a holistic approach to risk-management. There is a strong focus on staff education through initiatives such as Security Roadshows and the Staff-Safety information pack. The agency intends to support this further through training modules/internal programmes.

POLICY/DOCUMENTATION [with examples for GOV 2]

[*This table is to be filled out with the policies, SOPs and relevant documents that support this mandatory requirement. The Link/Doc ID box is intended to help your agency keep track of your security documentation for the self-assessment process*]

Document Name	Last Reviewed	Next Review	Link/Doc ID
Risk Management Policy- GOV 2 and GOV 6*	2022	2025	XX-1234
Information Security Policy	2021	2023	XX-1234
Security Risk Register	N/A	Ongoing	XX-1234
Agency A - Agency B Memorandum of Understanding	In development	N/A	XX-1234
Organisational Exposure to Insider threat	9/2022	N/A	XX-1234

***N.B if you have a document that is relevant for more than one mandatory requirement, you only need to evidence it once, but refer to the other mandatory requirement/s.

PRACTICE

[This section is intended for details on initiatives, governance group action, response to incidents, assessments completed etc]

- Security Roadshows focus on staff safety as the number one priority. Identifying different types of behaviour and understanding individual responses are key factors to risk identification and management discussions during Security Roadshows and workshops. Staff education in risk identification, management and tactical communication/situational awareness have been focus areas for the Security Team in the past year.

- The agency is finalising a Memorandum of Understanding (MoU) with Agency B to establish and promote a collaborative working partnership and formalise information sharing arrangements between Parties.

- The Security team has developed and regularly promoted a Staff–Safety Information Pack which includes a range of documents that provide advice and guidance to staff on managing difficult situations and keeping themselves safe.

- After several investigations into personnel security within the agency, both intentional and unintentional, the Security team submitted a Memo to senior leaders to highlight the potential for exposure to insider threat.

How will you achieve or maintain a 'Meets' rating?

[This section is intended for details on how your agency will achieve or maintain rating. If a 'meets' rating cannot be achieved, an explanation for why this is the case and how the risk of not meeting the requirement will be treated should be placed here.]

ACTIONS

- Maintain the Security Risk Register and raise relevant risks and issues through the Governance Group.

- Implement an additional PSR governance layer at senior executive level.

- If supported through Organisational Development, we would like to develop training modules and internal programmes for risk identification and management training.

- Understand the risks associated to insider threats and develop a systematic approach to enhancing controls and mitigating risks.

EXAMPLE TWO

Requirement		Status
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.	**MOSTLY MEETS**

Evidence of policy and practice to support status:

SUMMARY

While the agency has and embedded C&A process, resourcing issues have made it difficult to attend to legacy systems. There has been a reliance on third-party vendors to undertake C&A but the agency has recruitment plans to address these issues. This will likely be a medium term outcome so at this stage we assess that our current compliance would most accurately reflect a 'mostly meets' rating.

POLICY/DOCUMENTATION

Document name	Last Reviewed	Next Review	Link/Doc ID
C&A Activities Register	N/A	N/A	XX-1234
C&A SOP	2021	2024	XX-1234

PRACTICE

- Whilst new systems are generally fully compliant, existing (legacy) systems continue to operate without having been fully certified or accredited. This is in part due to resourcing constraints. The agency is looking to recruit new staff to assist with the C&A programme.
- While we continue to address these it is expected to take some years before the agency is fully compliant.
- An Audit and Pen-test programme is yet to be formally implemented. It is anticipated that future budget bids will ring-fence funding for this purpose.

In addition, please answer the following questions:

- **Describe the way your agency conducts C&A on new systems. Is it mandatory for all new systems?**

C&A is an embedded requirement for ICT projects delivered by the Information Management team. Information Security Advisors follow the agencies Certification and Accreditation (C&A) standard operating procedure to identify and assess risks. The framework follows GCDO guidelines, NZISM standards, and supports the PSR.

New systems or services must be approved to operate. Where the system/service meets the security standard it is referred to as an 'approved' system. A System Security Certificate is issued to the signing authority summarizing the risk assessment activities completed, remediation activities to be completed, and residual risk. Based on the residual risk, the signing authority approves the system/service for use.

- **What process does your agency have in place for tracking and monitoring the C&A lifespan, so systems undertake C&A renewal?**

C&A activities are recorded in a register – see document table. Reaccreditation is planned at 2-3 yearly intervals to identify new/emerging ICT risks to the Department's activities.

Total Systems and Services C&A planned 1 July 2021-30 March 2022 - 100

Completed – 40

In progress – 15

Backlog (not started) – 37

Requiring reaccreditation - 8

- **What is your process for managing C&A? Is it followed consistently, and is the risk acceptance signed off at an appropriate level?**

C&A of a new service is outsourced to a third-party vendor if our advisors are at capacity. Over the past 12 months we have outsourced 12 services for accreditation. Workshops are completed with key system/information users and business owners to identify the information security risks and the impact should the system, application, or network be compromised. Business owners receive a report advising them of risks and recommendations for mitigations. Workshops are completed with system Business Owners to enable a business impact assessment should the system be lost through negligence, natural event, or cyber-attack, and to define the maximum time the system could be unavailable, i.e. maximum allowable down-time.

The following members of staff can accept the risk and sign off a system - [NAME] [Job Title]

- **Does your agency have a process in place for managing the C&A of legacy systems? If not, why not?**

The agency currently has some legacy systems that have not undergone C&A. This is due to a lack of staff resourcing available. However, the agency plans to review the C&A framework to ensure it is fit-for-purpose and meets government standards. The agency will continue to use third-party vendors when required, and will include the legacy systems in the C&A process this year.

How will you achieve or maintain a 'Meets' for INFOSEC 3?

- Continue review of C&A framework to ensure it is fit-for-purpose and meets government standards.
- Enhance and where necessary develop new remediation practices that will enable us to reduce remediation activities and speed up the delivery of approved software to meet business demand.
- Develop security controls to specifically reduce risks associated with the use of cloud services.
- Continue reviewing existing commercial support agreements and adding information security requirements.

ADDITIONAL EXAMPLES OF PRACTICE EVIDENCE REQUIRED TO SUPPORT A RATING

The following are examples only and as stated earlier may not be fit-for-purpose for your particular agency. They are included to demonstrate the level of detail and the insight that may be required to support your self-assessed rating.

- **GOV 1** – The PSR Governance Group was established in 20XX and meets bi-monthly. Membership is currently being managed by the Chief Security Officer. The Group accepts that the agency has chosen not to appoint a formal CISO, and that some of the functions of this role may be included in the Position Description of an Information Security Manager. A formalised CISO role is an expectation of the PSR, therefore our rating remains at 'Mostly Meets'.

- **GOV 6** – The security team has developed Security Incident Reporting processes for internal staff and external contractors. This simple process has been distributed to operational staff that have had issues in the past with concerning behaviour or may be confronted by difficult members of the public.

- **GOV 8** – The Information Team have conducted an audit of the information management system to ensure documents are appropriately classified. The identified around 200 documents classified as 'R*STRICTED'. These documents have been reviewed with the document owner/originator to understand whether they are classified at the correct level. Many of these documents have been reclassified to a lower level.

- **PERSEC 2** – The National Security Clearance policy and SOP clearly outline the expectation for clearance holders to notify the Vetting Officer of significant changes in personal circumstances (e.g. new relationship, separation, change in address etc.)

- **INFOSEC 3** – The agency's C&A programme is well established. However, the pace of change within the technology environment and information domain continues to challenge the ability to ensure full compliance.

- **PHYSEC 4** – The Site Risk Assessment SOP outlines the end-to-end process for physical security upgrades at agency sites. The SOP states that following completion of upgrade works, the Security Team will engage with site lead(s) to determine:

    - Training on newly installed security systems has been delivered to a sufficient standard;
    - Site staff are aware of help desk points of contact for the security contractor and monitoring company, and are aware of processes for requesting assistance.