PSR | Protective Security Requirements

Moderation Framework 2025

Version date	01 October 2025
Version	2.0
Version description	Approved

Contents

Introduction

The purpose of this document is to provide supplemental guidance to the PSR Assurance Framework Guide.

This guide will help an organisation to provide effective assurance of the organisation's protective security capabilities and understand:

- Different types of evidence that could demonstrate key capabilities and measures for each mandatory requirement
- Best practices in PSR assurance
- How to independently verify or moderate their annual PSR self-assessment findings.

Evidence guide

Organisations need to provide the evidence to support their PSR self-assessment. Use the following evidence base and guides to review the organisation's security capability.

Evidence base

To demonstrate the required capability or measure, the organisation needs:

1) **Evidence of policy and process**
   a) Relevant policies, processes, procedures, materials, and plans are defined covering the security capabilities and measures defined in the PS-CMM and PSR policy frameworks.
   b) The relevant documentation has assigned ownership and management and has clear review cycles, revision history, and currency.
2) **Evidence of practice**
   a) There is evidence that the specific policies, processes, and procedures are actively and consistently applied across all people identified as in scope for adhering to them.
   b) There is evidence that the specific activities are undertaken to the standard set out at the identified PS-CMM level.

Example evidence

The PSR Policy Framework sets out protective security objectives. In this section, we have provided examples of the types of evidence you could use to demonstrate the achievement of some security objectives. PSR policy statements can be in the following format:

<Organisation /personnel> MUST/SHOULD/COULD **<policy word or phrase>** **<capability/activity/measure>** to address security risks.

The table below provides examples on the types of evidence that could be used to demonstrate how well the security objective is achieved based on the language used in the policy and question in the PSR Self-Assessment Tool.

Policy word/phrase	Example types of evidence
Enable Encourage Support Is responsible for Inform	• **Policy and procedures coverage**: the defined capabilities/measures/responsibilities are covered in relevant policies and procedures. • **Roles and responsibilities coverage**: the defined capabilities/responsibilities are covered in relevant role descriptions. • **Terms of reference coverage**: the defined capabilities/responsibilities are covered in a relevant group's terms of reference or mandate if applicable. • **Security awareness campaigns coverage**: security capabilities/responsibilities are covered in communications delivered, posters, training programmes, or other security awareness campaign activities.
Take responsibility for Consider Understand Evaluate Demonstrate behaviours Model culture norms Adhere to	• **Inventories and audits**: to identify and understand relevant people, information, and assets at risk • **Security threat and risk assessments**: identifies and assesses the relevant risks that the organisation is exposed to • **Security plans & design documentation:** details the selected security measures, design criteria, and how it will address requirements • **Training programme coverage**: the capabilities, expected behaviours, understanding, norms and beliefs are covered in training materials. • **Training course completion**: there is evidence that relevant training courses have been undertaken and completed by relevant parties. • **Training quiz results**: Where quizzes or tests are possible, there is evidence that relevant parties understand and can pass the quizzes presented. • **Culture survey coverage and results**: Where culture surveys are undertaken, the survey covers the relevant expected behaviours, practice, culture norms, etc
Ensure Assure Measure Review Resourced for	• **Security measure testing or certification and accreditation documentation**: there is evidence that measures meet its requirements. • **Contracted requirements:** Relevant requirements are stipulated, agreed, and tracked within agreements. • **Incident findings**: Security incidents are tracked, reviewed, and analysed identifying where relevant security capability/requirements are not achieved. • **Security risk review findings**: findings from relevant security risk reviews undertaken to confirm effectiveness of risk treatment plans. • **Compliance tracking**: outcomes from compliance spot checks undertaken on relevant policies, procedures, expected behaviours or practices to inform improvements including policy changes, additional security awareness programmes, or individual training. • **Performance metrics and reports**: relevant qualitative and quantitative measures historical tracking to assess the security capability performance identifying possible future improvements. • **Assurance activities/effectiveness audits**: findings from relevant assurance activities undertaken during the year.

Table 1 Example types of evidence based on specific policy language

Evidence guides

The following guides[1] demonstrate indicative types of evidence you may find to support the self-assessment findings. Evidence may exist as documents, intranet pages, electronic registers, logs, system databases, reports, meeting minutes, or interview records. Note that any data/ evidence provided for audit or moderation may need sanitisation to retain privacy and confidentiality. To ensure quality assurance, sample evidence, data, or records may be randomly selected for review by an independent assessor or moderator.

For each security domain and mandatory requirement, these guides provide example types of:

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

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
GOV 1 Establish and maintain the right governance	• Chief executive accountabilities & delegations • Security governance terms of reference • CSO, CISO, and security management roles and responsibilities • Security governance reporting process and SOPs	• Security governance and management personnel register • Security governance minutes • Leadership meeting minutes where security is discussed • Conflict of interest register (security role related) • Historical security governance and management reports • Security role appointments register/log
GOV 2 Take a risk-based approach	• Risk management framework (ISO 31000) and SOPs covering security risks • Threat assessment plan and procedures (including vulnerabilities) • Security risk management plan / security plan(s) (for enterprise plus information security, personnel security, physical security) • Co-location security agreements (if applicable) • Security policies • Security operational processes and procedures • Security performance management and reporting framework • Security improvement programme plan / roadmap	• Security risk register (for enterprise, information security, personnel security, and physical security) • Threat assessment reports • Environment scans • Security risk reporting • Security risk review findings • Security vulnerability trend analysis (for each security domain) • Policy review updates (for each policy) • Historical security performance data / logs / reports • Security programme deliverables • Security improvement / action plan results

[1] Evidence guides are intended to show 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.

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
GOV 3 Prepare for business continuity	• Business continuity policy • Business continuity management programme/plan • Business continuity templates, procedures, and checklists • Business continuity training and awareness campaign materials • BCM review action plan	• Business impact analysis • Critical function risk assessments • Business continuity exercise results • Business continuity training and awareness campaign results • BCM review findings • BCM action plan deliverables / results
GOV 4 Build security awareness	• Policy on how security policy adherence will be assessed • Personnel security training policy • Security communication, awareness and training programme targets and plans • Security awareness training and campaign materials • Security briefing policies and procedures • Security culture assessment plan • Action plans from security awareness and culture assessments	• Security awareness and training needs analysis report • Access to security policies, procedures, and training by personnel • Security training register and reports • Security briefing register and results • Security communications (e.g., roadshows, alerts, and newsletters) and awareness campaign results / reports • Security culture assessment findings • Action plan deliverables / results
GOV 5 Manage risks when working with others **(for suppliers, supply chains, or co-tenancy, or cooperating organisations)**	• Supplier security risk management policy and procedures • Supplier risk management plans • Procurement policies, procedures, and templates (security and ICT assets related requirements) • Security related contract / clause templates • Supply chain security requirements (including training) • Policies and plans regarding the organisation's obligations as a supplier (to another organisation) • MOUs, contracts, agreements with security requirements specified and clauses applied • Action plans from security performance and assurance reports	• Procurement deliverables (including security requirements assessments/due diligence) • Supply chain analysis findings • Register of third-party briefings • Performance reports against security requirements • Security knowledge sharing and/or continuous improvement reports • Security assurance reports • Action plan deliverables / results
GOV 6 Manage security incidents	• Policies, procedures, and systems for security incident management (including raising, investigating, reporting, and reviewing) • Security incident detection, monitoring, and management plan • Security incident escalation policy and plan • Process / systems for reporting and raising security incidents • Security incident training • Action plans from security incident management activities	• Security incident records, register, and logs • Security incident reports (including investigation, reporting (internal and external), and review/root cause analysis) • Incident drill / exercise results • Action plan results • Security re-training statistics
GOV 7 Be able to respond to increased threat levels	• Threat alert response policy & criteria • Alert response plans • Alert response templates, procedures, checklists • Threat level change plan including (integration between BCM & heightened threat alerts) • Action plans from alert response exercises/drills and reviews	• Alert response reports • Alert response exercise / drill results • Action plan deliverables / results

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
GOV 8 Assess your capability	• Security performance management and reporting framework • Security risk management plan • Security improvement programme plan / roadmap • Security self-assessment and assurance framework • PSR assurance plans (including effectiveness audits and self-assessment moderation) • PSR assurance roles and responsibilities	• Security performance reports • Security incident reports • Security self-assessment results • PSR assurance reports • Independent assurance audits / reviews / moderation findings / reports • Security and/or risk governance minutes (PSR assurance discussions) • Security improvement deliverables
PERSEC 1 Recruit the right person	• Personnel security policy and procedures (covering pre-employment security check practices) • Role risk assessment procedures • Individual risk management plans • Personnel on-boarding procedures / induction	• Role risk assessments • High risk roles list • Pre-employment check records • On-boarding and induction deliverables
PERSEC 2 Ensure their ongoing suitability	• Personnel management procedures • Personnel appraisal and review procedures • Personnel security policy and procedures (covering ongoing suitability assessment practices) • Role descriptions (with security responsibilities) • Insider risk management plan • Personnel security review procedures • Personnel security access policy and procedures • Personnel role change policy and procedures • Contractor management policy and procedures • Contracts for contractors (with security responsibilities) • Personnel security improvement action plans	• Personnel appraisals (including security) • Ongoing suitability assessment records such as SOUP contacts, change of circumstance, security risk concerns, engagement surveys, police vetting, credit checks, conflict of interest register, practicing certificates) for new personnel, people changing roles, and contractors. • Individual risk management plan results • Role risk assessment review results • Insider risk management deliverables • Register of people changes • Contractor issues register • Action plan deliverables / results
PERSEC 3 Manage their departure	• Personnel departure policy and procedures • Security de-briefing policies and procedures	• Exit-debrief / interview register and results • Signed confidentiality agreements (when used)

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
PERSEC 4 Manage national security clearances	• National security clearance (NSC) holder policy and procedures • NSC holder briefing/on-boarding procedures • NSC holder training plans • NSC holder risk management plans • NSC holder overseas travel policy and procedures • NSC holder changes in personal circumstances policy and procedures • NSC holder social media policy and guidance • NSC change management procedures (renewals, transfers, sharing, upgrades, cancellations) • Emergency access policies and procedures • NSC holder exit and debrief policy and procedures • NSC holder post separation policy and procedures	• Role specific NSC requirement assessments • NSC individual eligibility and suitability assessments • NSC vetting applications / register (e.g., via Tiaki • NSC holder registers (briefings/de-briefings, overseas travel requests/approvals, changes in personal circumstances, SOUP contacts, security incidents) • NSC holder risk assessments and response plans • Review for cause findings • NSC lifecycle management records (including new, renewal, transfers, shares, upgrades, cancellations) • Emergency access, briefing, debriefing, acknowledgement records • NSC holder exit debrief / register and results • SCI debrief records • NSC holder signed acknowledgement of lifelong obligations • NSC holder post separation contact register
INFOSEC 1 Understand what you need to protect	• Information security business impact criteria • Policy/criteria covering aggregated information • Asset management policy and procedures • Information / data management policy and procedures	• Information asset and ICT system inventory / register (including asset/system owners) • Information security providers register • Asset tracking and auditing results • Information security business impact analysis • Business critical functions definition (including critical assets that support them)

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
INFOSEC 2 Design your information security	• Information security management framework and policy • Information security design policies (e.g., defence-in-depth, zero trust principles/enterprise architecture, security by design) • Information security management lifecycle integration with procurement, architecture, project management, change management, and information management • Information security operational procedures • Access control policies and procedures • Classification policies and procedures (including information secure handling/protection, information sharing, and declassification) – may be part of information management policy and procedures • Information sharing authority, roles and responsibilities • Information declassification programme plan • Information security and classification training plan & materials • Information security review plan • Information security and classification performance measurement plan • Information sharing agreements • Secure information/ICT destruction procedures • Working away from the office / information security procedures	• Information security framework review findings • Information security measures/deliverables as per risk plan (effectiveness audit results) • Classified document / accountable material register (CDR) • Information security registers (e.g., access control lists, personnel access rights, security access audit logs, security incidents, classified information receipting, transport or removal tracking, security audits/spot checks, N*EO exception waivers, classified information and equipment waste and destruction) • As built configuration / risk measures documentation (for each system) • Information security review reports (e.g., classification practices, information audit, vulnerability assessments, security incidents, security training, and security culture assessments, Audit / Ombudsman / inquiries) • Information security testing (including penetration tests) results & remediation • Information security and classification performance reports • Information sharing agreement deliverables • Declassified information programme deliverables
INFOSEC 3 Validate your security measures	• Commercial support agreements (e.g., information security and ICT asset management requirements) • Cloud services validation policy and procedures • Information security certification and accreditation processes and procedures (including reviews and renewals) • C&A status / residual risk acceptance procedures • Certification and accreditation plan (including remediation & recertification) • Certification documentation & Certificates (for each ICT system) • Accreditation documentation (for each ICT system)	• ICT system accreditation status register • Cloud services validation register • ICT certification and accreditation findings / reports • ICT accreditation authority to operate (for each ICT system) • ICT security residual risk acceptance reports
INFOSEC 4 Keep your security up to date	• Information security vulnerability monitoring, analysis and management process, plan, and procedures • Information security operational procedures (e.g., access control, ICT equipment security, system security patching and updates) • Disaster recovery plans and procedures • Information security incident response plans • Information archiving and disposal policy and procedures • Action plans from information security vulnerabilities	• Monitoring systems • Information security access audit and maintenance logs/results • Security patching, equipment and software updates, and maintenance logs / results • Information security events and alerts (logs) • Information security event/vulnerability analysis reports • Vulnerability action plan results • Disaster recovery / major incident exercise results • Information archive and disposal log • Action plan deliverable / results

Mandatory Requirement	Indicative evidence of policy and process	Indicative evidence of practice
PHYSEC 1 Understand what you need to protect	• Physical security business impact criteria • Site suitability criteria • Site risk assessment process and procedures • Site security survey / building plan	• Physical security site and asset register • Physical security business impact assessments • Site security survey results • Site specific threat and risk assessments
PHYSEC 2 Design your physical security	• Physical security management framework • Physical security design policies and procedures (e.g., security in depth; deter, detect, delay, respond, recover; Crime prevention through environmental design, other standards) • Security zones policy and procedures • Security product installation verification procedures • Physical security operational procedures (including emergency response) • Visitor security policy and procedures • Site security plans • Refurbishment plans • Construction security plans, design briefs, requests for tender, contracts • Physical security performance measurement plan • Co-location /co-tenancy agreements / contracts • Working away from the office / physical security procedures	• Physical security management framework review findings • Physical security measures/deliverables as per site security plans (effectiveness audit results) • Physical security design audit results • Physical security registers (e.g., visitor, zones, security products usage, physical access control lists, personnel physical access rights, security incidents, security audits/spot checks) • Physical security review reports (e.g., vulnerability assessments, security incidents, security training, emergency response exercises) • Physical security testing (e.g., security product, penetration) results • Product installation verification results • Physical security performance reports • Co-location / co-tenancy agreement deliverables • Construction security plan deliverables
PHYSEC 3 Validate your security controls	• Physical security certification and accreditation policy, process, and procedures • Certification and accreditation plan • Certification documentation (for each site or zone) • Accreditation documentation (for each site or zone)	• Site accreditation status register • Site certification audit reports • Site certification and accreditation deliverables • Site accreditation authority to operate • Site security residual risk acceptance reports
PHYSEC 4 Keep your security up to date	• Physical security vulnerability monitoring, analysis and management plan and procedures • Physical security operational procedures (e.g., physical access control mechanisms, physical site, zone, and equipment security) • Emergency response plans and procedures • Physical security incident response plans • Action plans from physical security vulnerabilities and issues	• Physical security vulnerabilities register • Physical security events and alerts logs • Vulnerability assessment reports • Emergency response exercise results • Action plan deliverables / results

Table 2 PSR Evidence guides

PSR assurance and moderation

PSR assurance best practices

Organisations need to conduct assurance of its security capability to provide organisational leaders' with:

- Confidence in the organisation's security capability and self-assessment findings
- Clarity on the capability gaps and possible areas for improvement and investment
- An understanding of the residual risks that the organisation faces to inform improvement plans.

One of the key assurance activities recommended by the PSR is to undertake independent verification (also known as moderation) of the organisation's security capability and self-assessment findings.

Three Lines Model for risk assurance

To ensure good governance of security risk and provide assurance to leaders of their current capability and residual risks, it is recommended that organisations follow the Institute of Internal Auditors (IIA) "Three Lines model' when establishing roles and responsibilities for PSR assurance.

The New Zealand Controller and Auditor General's office supports the use of this model for facilitating audit committees to ensure good governance and risk management.

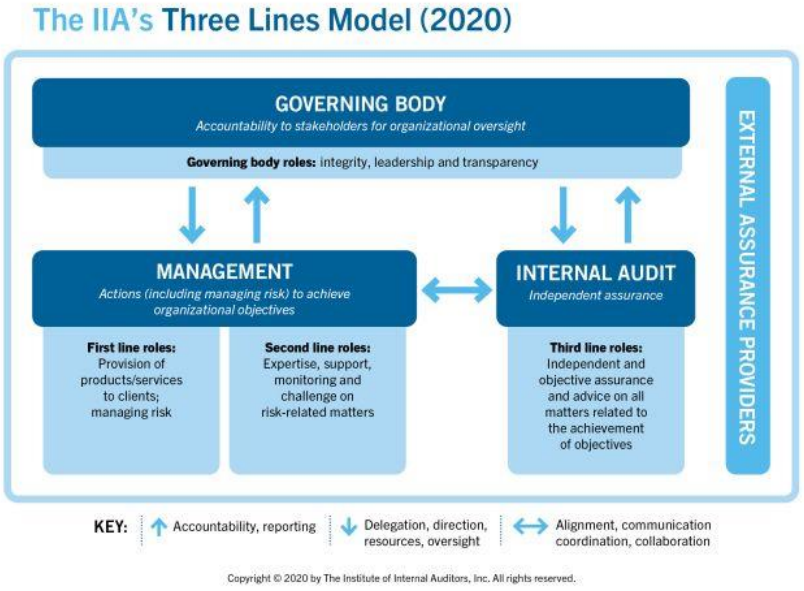

Figure 1 - Three Lines Model of Risk Governance

Example assurance roles and responsibilities

Line	Definition / risk governance	PSR assurance responsibility (examples)
First line: Security teams	The functions that own and manage the risks who are responsible for directing, assessing, and controlling the risk on a day-to-day basis.	• Determine security threats and risks • Set targets and implements security measures to address risks • Monitor security practices • **Gather / review evidence** • **Complete self-assessment** • **Facilitates audit/moderation** • Prioritise and plan improvements • Secure executive sign-off
Second line: Risk and assurance teams	The functions that oversee or specialises in risk management and compliance – responsible for monitoring and facilitating the effectiveness of risk management practices.	• Determining risk and assurance approach and plan • Facilitates security threat and risk assessments • **Commissioning assurance activities (third line) based on approach and plan** • Confirming assurance activity results and residual risks • Facilitating security risk governance discussions / risk acceptance.
Third line: Internal audit or external moderators	The functions that provide independent assurance, such as internal audit or other security certification and audit functions – responsible for determining how effectively the organisation assesses and manages its risks.	• **Undertakes assurance activities** • **Provides assurance report with findings and recommendations** • **Reviews findings with first and second line. If required, reviews and agrees changes to the annual report.**

Table 3 Three Lines Model lines definitions integrated with proposed PSR assurance responsibilities

Assurance activities

Each year, the organisation should decide on the assurance approach (e.g., assurance activities to be undertaken, assurance processes and timeframe), scope (e.g., which security domains/requirements are to be covered for each activity), and assurance roles and responsibilities.

This may include assurance activities such as undertaking effectiveness audits and/or moderation. Ensure that the PSR annual capability assessment includes any outcomes from the assurance activities undertaken throughout the year.

To be as efficient and effective as possible, the person undertaking assurance activities should have relevant expertise and sufficient background knowledge of the organisation and its risk profile.

Regularly, it should also provide risk assurance reports to its risk and assurance governance body.

Security measures effectiveness audits

An effectiveness audit will evaluate the operating effectiveness of a security control or measure and identify any gaps or improvements needed. An effectiveness audit should test that:

- the measure is operating as designed and within expected operating parameters
- the measure complies with PSR and organisation's policies
- if applicable, a person performing the measure has the necessary authority and competence to perform the measure
- the measure delivers the intended risk treatment
- security events (non-compliance / breaches) are detected and tracked.

Not every control or measure requires an effectiveness audit. An organisation will plan which security controls or measures may require an effectiveness audit depending on the degree of risk experienced and when it was last audited.

Monitoring security practices

An organisation should monitor and evaluate the effectiveness of its security measures. An organisation should adopt a layered approach which may include:

- root cause analysis on security incidents
- security risk reviews
- spot-check compliance with security policies and procedures
- security policy and procedure reviews.

Moderation framework summary

	COLLATE EVIDENCE FOR MODERATION	MODERATE SELF ASSESSMENT	RESPOND TO MODERATION	CONFIRM FINAL MODERATION	CONFIRM NEXT STEPS
SUMMARY	First-line / security team collates the evidence supporting the self-assessment to enable moderation to occur	Third-line / moderator reviews the self-assessment and the supporting evidence and provides moderation report and any suggested rating changes back to first- and second-line representatives	First- and second-line representatives review moderation and accepts or rejects the changes	All party representatives agree the final assessment and any dissenting areas	Second-line confirms next steps
KEY STEPS	**All parties** • Meet to discuss the process, scope, and respond to any questions **First-line / security team** • Collates underlying evidence required to support the self-assessment **All parties** • Moderator and organisation meet to hand over evidence and discuss any gaps	**Third-line / moderator** • Review of self-assessment tool answers and commentary • Reviews evidence and forms view as to the accuracy of the answers and commentary • Additional data may be gathered through interviews with staff, especially when large document sets may need to viewed (e.g. certification & accreditation for large numbers of systems) • Uses PSR Self-Assessment Moderation Tool if desired to capture moderation findings • Advises organisation of initial moderation results and recommendations	**First- and second-line** • Reviews the initial moderation results **All parties** • Confirms any questions or issues • Focus will be on discussing the dissenting areas **First- line / security team** • Adjusts levels where there is agreement • Documents evidence where there is a dissenting view	**Third-line / moderator** • Reviews feedback • Provides final moderation output, highlighting any dissenting areas	**Second-line / risk & assurance** • CSO signs off any changes and dissenting views • Updates security plan as a result of any changes
TOOLS	• Example evidence needed to typically support a self-assessment • Agreed evidence checklist • Completed PSR Self-Assessment Tool	• PSR supporting resources – policy documents, appendices, guidance, Capability Maturity Model • This document – PSR Moderation Framework • PSR Self-Assessment CMM Guide / Moderator Tool	• Completed PSR Moderator Tool	• Final moderation outputs which may include final PSR Moderator Tool	

Table 4 Moderation framework summary

Moderation process

PHASE	TASK	ACTIVITIES	COMMENTS
A. INITIATION	**Meet to agree scope & requirements**	• Moderator meets with CSO and staff who will gather evidence and respond to questions • All parties agree the scope of moderation and type of evidence required to assess • Moderator arranges for evidence gathering	• Moderator to send indicative evidence checklist and framework to organisation before meeting
	Ensure evidence gathered	• Moderator meets with security team to confirm the evidence will meet the required scope for moderation	• Use the checklist to note where evidence may not be sufficient and identify how this can be addressed
B. MODERATION	**Moderation self-assessment against the evidence**	• Moderator reviews self-assessment against requirements and evidence provided, going through in scope mandatory requirements in the Self-Assessment Tool • Use Moderator Tool to note observations and conclusions highlighting dissenting views • Look at the evidence pack in totality again to get a sense for how it fits together • Review your moderation comments considering the whole assessment and the evidence pack • Provide initial moderation findings to representatives and confirm initial moderation review meeting	• See next page for moderation approach guidance • Discuss any issues with first- and second-line to enable further evidence to be shared if necessary
C. FEEDBACK	**All parties to meet to discuss initial moderation**	• Meet with CSO and representatives to discuss initial moderation • Review dissenting areas especially	• Focus on dissenting areas • Moderator should have examples of what evidence is missing to support organisation self-assessment
	Provides additional evidence	• Security team provides additional evidence regarding dissenting requirements	• If there are dissents, additional evidence will need to be provided
D. FINALISATION	**Review additional evidence and update moderation**	• Examine additional evidence to see if moderation should change	• Time will depend on the amount of additional evidence
	Finalise moderation and provide to organisation and Protective Security	• Finalise moderation to ensure consistent and provide to organisation and to Protective Security Requirements • Advise organisation that all documents provided have been deleted	• Tidy-up and e-mail

Table 5 Moderation process

Moderation approach guidance

The moderator will manage the assignment with the requesting party according to the moderation requirements and time / budget assigned. Optimal duration for moderation is two to three weeks but will depend upon the scope, scale, turnaround time, and availability by all parties to undertake the moderation activities.

Self-assessment tool answers moderation

For answers in the Self-Assessment Tool, the moderator should check each assertion against the documentary evidence provided. Record the moderation in terms of "observations" regarding the evidence.

Selected answer	Moderation instructions
Yes	There is sufficient evidence that the measure/capability is fully in place
Partial	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.
Alternate control	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.
No	There is no evidence that the measure/capability is in place.
N/A	The control / measure is not applicable to the organisation and the comments accurately describe the reason for that

Table 6 Guidance for moderators based on selected self-assessment answers

Calculated capability maturity scores and ratings

The moderator should review the capability maturity scores and ratings calculated by the Self-assessment tool to confirm if the scores and ratings accurately reflect the overall capability for each mandatory requirement as discovered through the moderation process. For any capability maturity scores or ratings that seem incorrect, the moderator should review the answers to confirm if the capability has been incorrectly represented (either too high or too low).

Record any "conclusions" regarding the capability maturity scores and rating for each mandatory requirement.

Moderation guide and tool

A tool has been created for moderators to record and track their moderation activities and results. You can download the tool via the PSR Portal link below if you have a PSR Portal account. Contact the PSR team if you do not already have access to the PSR Portal.

PSR Self-Assessment CMM Guide and Moderator Tool [XLSX]

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