PROTECTIVE SECURITY REQUIREMENTS

GUIDANCE ON EVIDENCE OF POLICY & PRACTICE and a SELF-ASSESSMENT MODERATION FRAMEWORK

UPDATED FOR 1 JULY 2022

SUMMARY OF EVIDENCE REQUIREMENTS

Agencies need to provide the underlying evidence to support their self-assessment. Use this evidence base to review your self-assessment …

EVIDENCE BASE

- Achieving "meets" in the mandatory areas and "managed" for the maturity levels requires:
  - Comprehensive global policy and process in place across the whole agency
  - Evidence that the policy is being comprehensively and consistently applied.
- The table to the right lists the typical policies that will need to be in place and how evidence of practice can be demonstrated. It is guidance only.

EVIDENCE OF POLICY

- Evidence of policy will generally consist of security related policies integrated into the wider agency policy and processes.
- Agencies may have summary sheets showing the current status of policy / process documents, last review, next review, etc.

EVIDENCE OF PRACTICE

- Evidence of practice will generally consist of registers and logs demonstrating that policy and process is in fact being applied. Verbal evidence provided in interviews can also be used.
- These documents will include dates of reviews, changes, as well as accountabilities.

AREA		EVIDENCE OF POLICY & PROCESS	EVIDENCE OF PRACTICE
OVERARCHING	RISK MANAGEMENT	• Enterprise risk management framework • Corporate risk register • Threat assessments	• Threat assessments register/log • Security risk register (including review log)
	SECURITY POLICY	• Security governance terms of reference • CSO terms of reference • CISO terms of reference • Security policy (including risk management) • Security operational processes and procedures (including reporting) • Security enhancement roadmap	• Security governance minutes • Security management regular reports • Security incident register and actions taken • Security enhancement plan review • Policy update cycle evidence • Annual security assessment • Independent assessment reviews and management responses • Environment scans
PERSEC	STAFF	• Health and Safety policy • Staff management procedures • Personnel on-boarding procedures / induction • Personnel appraisal and review procedures • Personnel termination procedures • Roles and responsibilities for security (including dedicated roles) • National security clearance holder policy • Personnel security review procedures • HR personnel security access policy • JD security requirements (including risk management) • Personnel training policy	• Security questionnaires and surveys • Personnel security access register (including approvals, briefing evidence, notification evidence, briefing, overseas travel intended) • Security roles appointment register/log (incl. CSO, CISO • Annual training plan • Annual training reports • Annual appraisals (incl security) • Exit interviews • Suspicious and unusual contact register/log • Signed confidentiality agreements • Register of people changes • Annual security clearance register/log • Clearance holder personal travel approvals register/log
	CONTRACTORS	• Standard contracts for external providers	• Contractor security access register (including approvals, briefing evidence, notification evidence, briefing, overseas travel intended) • Contractor issues register • External supplier security due diligence and reviews • Supplier briefings on incident reporting
	VISITORS	• Visitor security policy	• Visitor register
INFOSEC	SYSTEMS	• Development life cycle (including security by design) • System controls to prevent unauthorised access • Mobile device policies	• Certification & Accreditation reports • System security testing (including penetration tests)
	INFORMATION	• Information management strategy and policy • Information security framework and policy (including business linkages) • Information security operational procedures	• Clear desk evidence (e.g. review and breach registers) • Information security reviews and audits • Register of information assets and providers • Certification & Accreditation reports • Accountable documents register/log • Zone 5 security policies
	ARCHIVING	• Archiving and disposal policies	• Archive and disposal reviews
PHYSEC	PHYSICAL	• Physical security framework and policy • Physical security operational procedures • Physical security systems, controls, facilities, provisions • External asset security framework and policy • Threat level change plan	• Certification & Accreditation reports (physical access, adequacy of access controls and monitoring) • Physical security plan (shows implementation of policy in actual physical locations) • Register of devices held at reception • Emergency security plan test • Physical safety and security concern register/log
COMMS	COMMUNICATIONS	• Security communications plan • Security intranet • External supplier training requirements	• Information security awareness campaign • Access to policies and procedures by staff • Security information needs assessment (annual or bi-annual) • Security awareness campaigns (all aspects) • Security alerts • Security newsletters (integrated in other communications) • Staff newsletters (including security)
INCIDENT	BUSINESS CONT.	• Business continuity plan (incl. security)	• Business continuity plan test results
	INCIDENT MANAGEMENT	• Incident management procedures, escalation, and reporting processes	• Incident register/log • Incident reports • Incident review and root cause analysis • Incident drills

EVIDENCE FOR MANDATORY REQUIREMENTS

Agencies need to provide the underlying evidence that support their self-assessment for the mandatory requirements. While it will vary between agencies, it will typically comprise the following …

	SECURITY GOVERNANCE	PERSONNEL SECURITY	INFORMATION SECURITY	PHYSICAL SECURITY
EVIDENCE OF POLICY & PROCESS “What evidence is there that the required policies and procedures are in place?”	• Security governance terms of reference • CSO terms of reference • CISO terms of reference • Security policy • Security operational processes and procedures (including reporting) • Business continuity plan (including security) • Security review and enhancement plan	• Personnel on-boarding procedures / induction • Personnel appraisal and review procedures • Personnel termination procedures • Personnel security review procedures • HR personnel security access policy • JD security requirements • Personnel training policy • Contracts for external providers • Visitor policy	• Information security framework and policy (including business linkages) • Information security operational procedures	• Physical security framework and policy • Physical security operational procedures • Security escalation plan • Visitor security policy
EVIDENCE OF PRACTICE “What evidence is there that the policies and procedures are being consistently followed?”	• Security awareness campaigns • Security risk register • Policy update cycle evidence • Security governance minutes • Annual security assessment • Business continuity plan test results	• Personnel and contractor security access register (including approvals, briefing evidence, notification evidence, briefing, overseas travel intended, etc) • Annual training plan • Annual training reports • Annual appraisals (incl. security) • Exit interviews • Suspicious and unusual contact register • Signed confidentiality agreements • Contractor issues register	• Information security awareness campaign • System controls to prevent unauthorised access • Clear desk evidence (e.g. review registers, breach log) • Reviews • Certification & Accreditation reports	• Physical security review report (physical access, adequacy of access controls and monitoring) • Register of devices held at reception • Emergency security plan test • Visitor register • Certification & Accreditation reports

This evidence may exist as documents, intranet pages, electronic registers, logs, systems databases, etc. These documents are listed to provide an indicative list of what evidence there might be to support an agency’s PSR self-assessment.

EVIDENCE FOR LEADERSHIP AND CULTURE

Agencies need to provide the underlying evidence that support their self-assessment for their capability maturity. While it will vary between agencies, it will typically comprise the following for leadership and culture …

	EXECUTIVE COMMITMENT & OVERSIGHT	MANAGEMENT STRUCTURE, ROLES, & RESPONSIBILITIES	MONITORING & ASSURANCE	CULTURE & BEHAVIOUR	EDUCATION & COMMUNICATIONS
EVIDENCE OF POLICY & PROCESS "What evidence is there that the required policies and procedures are in place?"	• Security governance terms of reference • Security policy • Security operational processes and procedures (including reporting) • Business continuity plan (including security) • Security review and enhancement plan *Update (July 2022)* • Classification and Declassification Policy that reflects the updated PSR Guidance 2022	• CSO terms of reference • CISO terms of reference • Roles and responsibilities for security (including dedicated roles) *Update (July 2022)* • Roles defined and assigned for your declassification programme	• Security reporting policy • Contracts for external providers • Visitor policy	• Personnel on-boarding procedures / induction • Personnel appraisal and review procedures • Personnel termination procedures • Personnel security review procedures • HR personnel security access policy • JD security requirements	• Security communications plan • Security intranet • External supplier training requirements *Update (July 2022)* • Education and training materials on the classification system
EVIDENCE OF PRACTICE "What evidence is there that the policies and procedures are being consistently followed?"	• Security governance minutes • Security management reports • Security roles appointment register/log (incl. CSO, CISO) • Security risk register • Policy update cycle evidence *Update (July 2022)* • Classification and Declassification management reports	• Security awareness campaigns • Incident drills • Accreditation authority register for Infosec and Physec *Update (July 2022)* • Update of JDs to reflect declassification, information collection, classification, and information sharing responsibilities	• Annual security assessment • Business continuity plan test results • Security performance and incident reports • Independent reviews and management responses • External supplier security due diligence *Update (July 2022)* • Reporting in outcomes of audit and review of classification • Evidence of business change based on classification audit and review • Process for monitoring classification, declassification, information sharing • Audit and review of classification procedures • Chief Archivist and Ombudsman feedback	• Security awareness campaigns • Security questionnaires and surveys • Security alerts register/log • Security newsletters (integrated in other communications) • Security incident register/log • Incident review and root cause analysis *Update (July 2022)* • Classification System (incl Information sharing and declassification) awareness campaign • Information Sharing Plan • Information Sharing culture survey • Measurement of changes in classification rates, volumes of declassification, decrease in complaints, positive ombudsman reporting	• Security awareness campaigns • Security newsletters (integrated in other communications) • Annual training plan • Annual training reports (including participation levels) • External supplier training register *Update (July 2022)* • Quality measures for classification system education

This evidence may exist as documents, intranet pages, electronic registers, logs, systems databases, etc. These documents are listed to provide an indicative list of what evidence there might be to support an agency's PSR self-assessment.

EVIDENCE FOR PLANNING, POLICIES, AND PROCESSES

Agencies will need to provide the underlying evidence that support their self-assessment for their capability maturity. While it will vary between agencies, it will typically comprise the following for planning, policies, and processes …

	STRATEGY & PLANNING	POLICIES, PROCESSES, & PROCEDURES	RISK MANAGEMENT	INCIDENT MANAGEMENT
EVIDENCE OF POLICY & PROCESS “What evidence is there that the required policies and procedures are in place?”	• Security policy • Security operational processes and procedures (including reporting) • Business continuity plan (including security) • Security enhancement roadmap	• Security policy • Security operational processes and procedures (including reporting) • Contracts for external providers *Update (July 2022)* • Classification system policy/policies including classification and declassification • Information Sharing Agreements • Information Sharing procedures	• Enterprise risk management framework • Threat assessments • Security risk register • Corporate risk register • Security policy (risk management) • Security operational processes and procedures (risk management) • Development life cycle (including security by design) • JD security requirements (including risk management)	• Incident management procedures, escalation, and reporting processes
EVIDENCE OF PRACTICE “What evidence is there that the policies and procedures are being consistently followed?”	• Security risk register/log • Policy update cycle evidence • Security governance minutes • Annual security assessment • Business continuity plan test results • Security plan review • Security incident register and actions taken • Security reports *Update (July 2022)* • Evidence that information is considered a strategic asset in planning and that its use, sharing and release is considered in organisational plans	• Access to policies and procedures by staff • Policy update cycle evidence • Security plan review • Security incident register and actions taken • Environment scans • Security status and incident reports *Update (July 2022)* • Declassification programme in place including assignment of roles • Proactive declassification is in evidence	• Threat assessments register • Risk register reviews • Information security awareness campaign • Supplier reviews *Update (July 2022)* • Effectiveness and efficiency audits of information management practices including the application of the classification system are undertaken. The agency’s application of the classification system, as a risk management system, is on the enterprise risk management register and is considered by the audit and risk committee	• Supplier briefings on incident reporting • Incident register/log • Incident review and root cause analysis • Incident reports • Incident drills • Staff newsletters

This evidence may exist as documents, intranet pages, electronic registers, logs, systems databases, etc. These documents are listed to provide an indicative list of what evidence there might be to support an agency's PSR self-assessment.

EVIDENCE FOR SECURITY DOMAINS

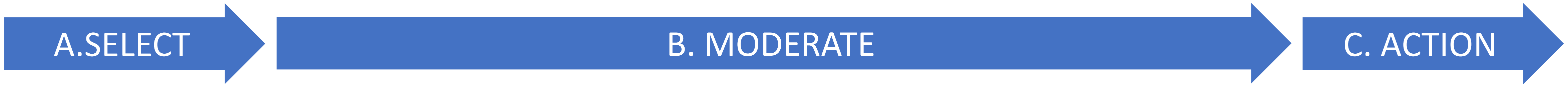
Agencies need to provide the underlying evidence that support their self-assessment for their capability maturity. While it will vary between agencies, it will typically comprise the following for security domains …

	PERSONNEL SECURITY	INFORMATION SECURITY	PHYSICAL SECURITY
EVIDENCE OF POLICY & PROCESS "What evidence is there that the required policies and procedures are in place?"	• Staff management procedures • Personnel on-boarding procedures / induction • Personnel appraisal and review procedures • Personnel termination procedures • National security clearance holder policy • Personnel security review procedures • HR personnel security access policy • JD security requirements • Personnel training policy *Update (July 2022)* • Delegations and position descriptions for staff include specific consideration of delegation/authority for the sharing of information and tools to support consistent decision making by employees	• Information management strategy and policy • Information security framework and policy (including business linkages) • System controls to prevent unauthorised access • Information security operational procedures • Archiving and disposal policies • Mobile device policies *Update (July 2022)* • Classification, info sharing, and declassification policy • You have integrated information security and direction on the application of NZ Classification System in your information management and other policies and processes	• Physical security framework and policy • Visitor security policy • External asset security framework and policy • Archiving and disposal policies • Physical security operational procedures • Threat level change plan • Health and safety policy • Business continuity plan
EVIDENCE OF PRACTICE "What evidence is there that the policies and procedures are being consistently followed?"	• Personnel and contractor security access register (including approvals, briefing evidence, notification evidence, briefing, overseas travel intended, etc) • Annual training plan • Annual training reports • Annual appraisals (incl. security) • Exit interviews • Suspicious and unusual contact register/log • Annual security clearance register/log • Clearance holder personal travel approvals register/log	• Information security awareness campaign • Register of people changes • System certification and accreditation • System security testing (including penetration tests) • Archive reviews • Information audits • Register of information assets and providers • Certifications and accreditations • Accountable documents register/log • Zone 5 security policies *Update (July 2022)* • Classification, declassification, and information sharing audit reports • Incidents recorded regarding classification, declassification, information sharing	• Physical security plan (shows implementation of policy in actual physical locations) • Physical security systems, controls, facilities, provisions • Physical security review report (physical access, adequacy of access controls and monitoring, shared premises, certifications and accreditations) • Register of devices held at reception • Visitor register • Emergency security plan test • Incident register • Physical safety and security concern register / health and safety • Disposal reviews • Business continuity test *Update (July 2022)* • Physical assets that are used to secure, process or dispose of classified material are consistently classified, marked, accessed, disposed of and handled in line with the New Zealand Government Security Classification System

This evidence may exist as documents, intranet pages, electronic registers, logs, systems databases, etc. These documents are listed to provide an indicative list of what evidence there might be to support an agency's PSR self-assessment.

MODERATION FRAMEWORK

Moderation improves the quality of the PSR agency self-assessments. This framework covers moderator selection, moderation, and action …


A.SELECT

B. MODERATE

C. ACTION

	A.1. Agencies volunteer FOR MODERATION	B.1. COLLATE EVIDENCE FOR MODERATION	B.2. MODERATE AGENCY SELF ASSESSMENT	B.3 RESPOND TO MODERATION	B.4. CONFIRM FINAL MODERATION	C.1. CONFIRM NEXT STEPS
SUMMARY	• An agency voluntarily chooses to carry out moderation on itself	Agency collates the evidence supporting the self-assessment to enable moderation to occur	Moderator reviews the self assessment and the supporting evidence and provides moderation report and any suggested rating changes back to agency	Agency reviews moderation and accepts or rejects the changes	Agency and Moderator agree the final assessment between agency and moderator and any dissenting areas	
KEY STEPS	Agency Volunteers • Agency decides whether moderator external or internal • Selects moderator	Agency/Moderator • Moderator and agency meet to discuss the process and respond to any questions Agency • Collates underlying evidence required to support the self-assessment Agency/Moderator • Moderator and agency meet to hand over evidence and discuss any gaps	Moderator • Initial review of self-assessment • Reviews evidence and forms view as to mandatory compliance levels and capability maturity • 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) • Advises Agency of initial moderation results	Agency • Reviews the initial moderation results Agency/Moderator • Agency confirms with moderator any questions or issues • Focus will be on discussing the dissenting areas Agency • Adjusts levels where Agency supports the moderator's view • Documents evidence where Agency has a dissenting view	Moderator • Reviews agency feedback • Provides final moderation output, highlighting any dissenting areas	Agency • CSO signs off any changes and dissenting views • Updates security plan as a result of any changes
TOOLS	• This Moderation Framework document	• Example documentary evidence needed to typically support a self-assessment • Documentary evidence checklist	• Use this Moderation Framework for guidance			

AGENCY BRIEFING

This brief sets out a recommended process to follow for moderation of self-assessments. It includes what agencies should provide, a description of the process, timing, and answers to key questions …

BACKGROUND

Agencies can be over optimistic

- International partners have pointed out that where serious protective security breaches have warranted a deep enquiry into agency capability, the enquiry has routinely found that agencies were over optimistic in their self-assessments compared to the actual evidence, practice or culture in their agency.

Moderation of self-assessments

- To help agencies gain a more accurate assessment of their mandatory compliance and capability we have implemented a moderation process for the PSR self-assessments.
- An external or internal moderator will review your self-assessment against the supporting evidence to provide assurance as to the self-assessed ratings.

Timetable

- The key events for the moderation occur over a two to three-week timeframe.

Event	Date
1. Moderator kick-off meeting with agency	Week 1
2. Meeting to hand over documentary evidence and discuss	Week 1
3. Moderator provides initial assessment to agency	Week 2
4. Moderator and agency meet to discuss initial moderation	Week 2/3
5. Moderator provides final moderated report to CSO	Week 2/3

MODERATION PROCESS

Moderator conducts kick-off meeting with agency

- The appointed moderator will contact you and meet to brief you on the process and advise you of the evidence you will need to collect to support your self-assessment.
- Previous pages in this guidance list the kind of evidence that we would expect to see to support a "meets" assessment for the mandatory requirements and a "managed" assessment for capability maturity. This documentation list is provided as indicative only. Each agency will have varying approaches to its policy development and monitoring of compliance.

Moderator meets with agency to hand over documentary evidence and discuss

- The moderator will meet with you a second time to pick up the evidence and discuss any gaps or issues you have identified (if you cannot provide the evidence pack at the first meeting).
- Each agency will need to think about what evidence it will need to support its self-assessment.

Moderator conducts initial moderation

- The moderator will then go through your self-assessment and undertake the moderation, adding moderation comments into your self-assessment so you can clearly see the comments and note dissenting views.
- The moderator may have clarifying questions regarding the evidence you have provided. This may involve requests for additional evidence to support your self-assessment. Additional evidence may be provided via documents or through meetings and/or interviews.

Moderator and agency discuss initial moderation

- The moderator will send you the initial moderation for you to consider. The moderator will meet with you to discuss your feedback on the initial moderation and discuss any further evidence you may have. This meeting will generally focus on the dissenting views.
- As you review the moderations and discuss the assessment with the moderator you may find that this leads you to reassess parts of your self-assessment. You can make these changes and note the additional evidence you are providing in your revised self-assessment. Note that you do not have to accept the moderator's views.
- Revising the self-assessment will support your agency in any re-prioritisation it needs to make in its security enhancement planning for the next 12 months.

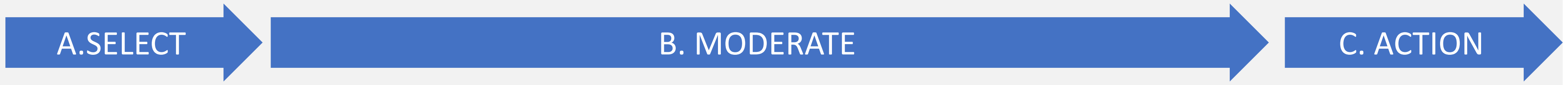
• QUESTIONS AND ANSWERS

What do I need to have ready?

- You will need to have available your self-assessment and documentary evidence supporting your self-assessment. Included in this Guidance are the kinds of evidence you might provide. This can be discussed with the moderator at the first meeting.
- Where there are long lists of similar documents (e.g. Business Continuity Plans for a large number of branches) it may be more appropriate to provide a register of documents, their status, review date, validation activities, etc.

How should we provide the evidence documents to the moderator?

- It is up to each agency. Some agencies may be happy to provide the documents to an external party (e.g. using a secure USB or providing them a hard copy). Others may require the moderator to access these documents on-site or in a redacted manner.



AGENCIES VOLUNTEER FOR MODERATION	B.1. COLLATE EVIDENCE FOR MODERATION	B.2. MODERATE AGENCY SELF ASSESSMENT	B.3 RESPOND TO MODERATION	B.4. CONFIRM FINAL MODERATION	C.1. CONFIRM NEXT STEPS
• Agency volunteers to carry out own moderation	Agency collates the evidence supporting the self-assessment to enable moderation to occur	Moderator reviews the self assessment and the supporting evidence and provides moderation report and any suggested rating changes back to Agency	Agency reviews moderation and accepts or rejects the changes	Agency and Moderator agree the final assessment between agency and moderator and any dissenting areas	Agency implements any required changes

MODERATION PHASES & TASKS

The moderator will manage the engagement with the agency according to the time budget assigned. Recommended time for the moderation is two weeks but will depend upon how quickly the agency can turn-around information …

PHASE	TASK	ACTIVITIES	SMALL AGENCY	LARGE AGENCY	COMMENTS
A. INITIATION	Meet to brief agency	• Moderator meet with CSO and staff who will gather evidence and respond to questions • Moderator provide document list and framework document • Moderator arrange for evidence gathering	1 hour	1 hour	• Moderator to send document list and framework to agency before meeting
	Ensure evidence gathered	• Moderator meet with agency to confirm the evidence provided against the checklist	2 hours	2 hours	• Review evidence with agency against checklist • Use the checklist to note where there is missing information and how this might impact the assessment
B. MODERATION	Moderation self assessment against the evidence	• Moderator review self-assessment against requirements and evidence provided, going through each mandatory requirement and each maturity requirement – start with mandatory requirements • Note observations and conclusions highlighting dissenting views – use the template tables • 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 back to agency by email and confirm initial moderation review meeting	8 hours	16 hours	• See next page for moderation approach and activities • Expect to spend about half the time on mandatory requirements and half the time on capability maturity • May be easier in some cases to discuss the issues with the agency, especially when it is a large agency
C. AGENCY FEEDBACK	Meet with agency to discuss initial moderation	• Meet with CSO to discuss initial moderation • Review dissenting areas especially	2 hours	3 hours	• Focus on dissenting areas • Moderator should have examples of what evidence is missing to support agency self-assessment
	Agency provides additional evidence	• Agency provides additional evidence regarding dissenting requirements	-		• If the agency dissents, it will need to provide evidence
D. FINALISATION	Review any additional evidence provided by agency and update moderation	• Examine evidence to see if moderation should change	2 hour	4 hours	• Time will depend on the amount of additional evidence
	Finalise moderation and provide to agency and Protective Security	• Finalise moderation to ensure consistent and provide to agency and to Protective Security • Advice agency that all documents provided have been deleted	1 hour	2 hours	• Tidy-up and e-mail
		Contingency	-	4 hours	
		TOTAL	16 hours 2 days	32 hours 4 days	

MODERATION PHASES & TASKS

There are 20 mandatory requirements and 12 capability assessments to be moderated …

CATEGORY	AREA	REQUIREMENT		MODERATOR APPROACH & TIMING
MANDATORY REQUIREMENTS 20 requirements	Security governance	GOV1	Establish and maintain the right governance	• Review each requirement against the description in the self-assessment • Check each assertion against documentary evidence – use the mapping of the documents against the requirements • Assess the evidence against the self-assessed rating from the agency and recommend whether concur or raise or lower • Record the moderation in terms of "Observations" regarding the evidence and "Conclusions" regarding the self-assessment level
		GOV2	Take a risk-based approach	
		GOV3	Prepare for business continuity	
		GOV4	Build security awareness	
		GOV5	Manage risks when working with others	
		GOV6	Manage security incidents	
		GOV7	Be able to respond to increased threat levels	
		GOV8	Assess your capability	
	Personnel security	PERSEC1	Recruit the right person	
		PERSEC2	Ensure their ongoing suitability	
		PERSEC3	Manage their departure	
		PERSEC4	Manage national security clearances	
	Information security	INFOSEC1	Understand what you need to protect	
		INFOSEC2	Design your information security	
		INFOSEC3	Validate your security controls	
		INFOSEC4	Keep your security up to date	
	Physical security	PHYSEC1	Understand what you need to protect	• Divide time equally between mandatory requirements and capability maturity • Expect to spend ½ to one day on the *Mandatory Requirements* depending on the size of the agency – this means 10 to 20 minutes on each requirement • Expect to spend 1 to 1½ days on the *Capability Maturity* depending on the size of the agency – this means 40 to 60 minutes per requirement
		PHYSEC2	Design your physical security	
		PHYSEC3	Validate your security controls	
		PHYSEC4	Keep your security up to date	
CAPABILITY MATURITY 12 requirements	Leadership and culture	LC1	Executive commitment and oversight	
		LC2	Management, structure, roles and responsibilities	
		LC3	Monitoring and assurance	
		LC4	Culture and behaviours	
		LC5	Education and communications	
	Planning, policies and processes	PPP1	Strategy and planning	
		PPP2	Policies, processes and procedures	
		PPP3	Risk management	
		PPP4	Incident management	
	Security domains	PERSEC	Personnel security	
		INFOSEC	Information security	
		PHYSEC	Physical security	