PSR Protective Security Requirements

PSR CAPABILITY MATURITY MODEL (PS-CMM)

Maturity level	PS-CMM 1	PS-CMM 2	PS-CMM 3	PS-CMM 4	PS-CMM 5
Practice	INFORMAL	PLANNED AND TRACKED	STANDARDISED	QUANTITATIVELY CONTROLLED	OPTIMISING
Description	Security capability may be ad-hoc, unmanaged, or unpredictable; success may rely on individuals rather than institutional capability. A partial set of PSR MUST policies may be met. Capabilities may include one or more of the following: • Some base practices are performed but may lack consistent planning and tracking. • Processes may be ad-hoc, informal and undocumented. • Practice is often unmanaged or unpredictable. • Where practice is good, it reflects the expertise and effort of individuals rather than institutional knowledge. • Resources are assigned to work reactively rather than as part of role assignments/competencies. • There may be confidence that some security activities are performed adequately; however, this performance is not measured, may be variable, or loss of key personnel would impact organisational capability and practice. • Tools needed to support security management are lacking. • Improvement activity occurs in reaction to incidents rather than proactively.	Security capability is well formed within the functions responsible for security. The security policies, capabilities, controls, and practices are in place and repeatable. They are designed to meet the organisation's core security requirements. All PSR MUST policies are met. Capabilities include all the following: • The importance of security is recognised, and key responsibilities are explicitly assigned to positions. • General security policies, processes, and procedures are defined to meet minimum compliance requirements; these are reviewed when compliance requirements change. • Policies and processes are used within a minimum core subset of the organisation. • At least, a base set of protective security measures are planned and tracked (PSR MUST measures). These practices are generally repeatable and results consistent within the core subset of the organisation. • Risks and requirements are occasionally reviewed. • Performance against specified procedures can be verified and occasionally are verified (audited). • Tools and technologies supporting security management meet basic needs for compliance. • Corrective action occurs in response to incidents but also a basic multi-year improvement plan is in place. Limited resources are applied to address the highest priority risks.	Security capability is standardised, integrated, understood and consistently followed across the enterprise. Security performance is well governed and managed at an enterprise level. All PSR MUST and SHOULD policies are met. Capabilities include all at PS-CMM 2 plus: • Policies, processes, and procedures are comprehensively defined, approved, reviewed, and routinely used across the enterprise. • Effective and robust security governance and management structures are in place and practices are well managed, governed, and coordinated. • Risk assessment and management activities are regularly scheduled and completed. • Resource allocation is aligned to strategic priorities and risks. • Performance / security metrics are planned, tracked, monitored, verified, and reviewed. • Historic performance information is periodically assessed and used to determine where improvements should be made. • Information from multiple sources informs decisions and planning – evaluating information relevance and reliability. • An annual proactive protective security improvement programme is planned, tracked, and well managed and governed. The programme is well resourced to maintain PS-CMM 3 capability maturity.	Security capability and performance are measured, monitored, and objectively and quantitatively controlled. Security measures are hardened in response to performance alerts. Security is a strategic focus for the organisation. All PSR MUST and SHOULD policies are met. Some COULD policies are met to address its specific risks. Capabilities include all at PS-CMM 3 plus: • Baselined quantitative performance metrics enable effective governance oversight and decisions. • Detailed performance measures are collected and analysed leading to understanding of security vulnerabilities and capability and ability to predict performance (may be daily, weekly, monthly, or quarterly). • Security measures are hardened in response to quantitative measures to withstand security threats. • Performance is objectively managed and quality of work products is quantitatively known. • Recommended 'better practice' measures are implemented in response to its risk assessment (e.g., PSR COULD policies and other recommended best practice frameworks.) • Security is a strategic issue for the organisation; security skills are continuously updated to ensure knowledge remains current. • Long term forecasting and planning is integrated into business planning to predict and prepare for changes in the security environment. • Continuous improvement programme includes continuous monitoring and control with active contribution and management by relevant experts and service providers.	Security capability adapts to a dynamic, high risk operating environment. Practices are generally recognised as world leading and have near real-time measurement and response mechanisms. All PSR MUST, SHOULD, and COULD policies are met. Capabilities include all at PS-CMM 4 plus: • Practices are recognised as international best practice. • Innovative security standards, techniques, and controls are continually reviewed, developed, tested, and implemented to address emerging threats. • Performance measures are across end-to-end processes beyond the enterprise to include all touch points with customers, partners, and suppliers. • Performance measures (goals) measure performance against organisational strategy and goals. • Continuous improvement programme is supported by real-time performance data and automated response mechanisms.
When to target this level	Inappropriate Does not meet requirement.	Target when risks are generally low and can be controlled through repeatable processes and baseline security measures. **Minimum baseline PSR requirement**	Target when standardised and integrated practice is required to effectively manage moderate or greater levels of risk.	Target when greater objective control is required to manage severe (high) or greater risks. This level is appropriate when the organisation must achieve externally set strict performance, control, reporting, and governance requirements.	Target when near real-time response is required to manage critical (extreme) risks. This level is appropriate when the threat environment is continually escalating and the consequence of compromise is extreme.

Table of contents: PSR CMMs for each Mandatory Requirement

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 1

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 1 Establish and maintain the right governance		
GOV 1.1 Ensure executive commitment and oversight		
An organisation head (e.g., Chief Executive) prioritises and resources protective security to manage security risks by: • Ensuring security is part of organisational culture, practices, and plans • Ensuring effective security policies are implemented • Establishing security governance practices • Ensuring that senior leaders regularly consider protective security and are responsible for overseeing organisational security risks. Executive leaders understand and govern protective security issues relevant to their areas of responsibility and their own responsibilities for security by: • Receiving regular, prompt, and proactive reports on security matters • Understanding organisational risk exposure • Setting and reviewing standards for security risk tolerance • Governing the implementation of protective security • Reviewing security performance, risks, incidents, and emerging threats • Ensuring that performance and capability assessments are occasionally independently verified / moderated • Establishing the priorities and activities for improvement.	If authority is delegated, the organisation head considers the associated risks and remains accountable to for the delegate's decisions • Ensures that information security delegates are appropriately experienced and a member of the senior leadership team • Ensures that when delegated to a board or committee, the chair of the group is accountable. The organisation has established a dedicated security governance body. Executive leaders demonstrate and actively promote good security practice.	Executive leaders drive continuous improvement in protective security including approving and sustainably resourcing work on best practice security innovations.
GOV 1.2 Assign functional security responsibilities		
Appoint a CSO		
Assign overall responsibility for security to a senior leader designated as the Chief Security Officer (CSO) who is answerable to and has free access to the Chief Executive on security related matters. Provide a mandate to the CSO for establishing and undertaking the protective security programme for governance, personnel, information, and physical security. Their responsibilities align to recommended CSO responsibilities in the PSR. Any CSO conflicts of interest that may prevent them from providing independent advice and assurance are clearly identified, declared, and actively managed.	The CSO has authority to make decisions on security matters including resourcing security functions.	The CSO has responsibility and authority to commission and deploy protective security initiatives and systems as part of an active and agile continuous improvement programme. The CSO leads regular, structured discussions on protective security matters and responsibilities with the leadership team, management team, and governance bodies. Action points inform priorities, performance measures, and continuous improvement.
Appoint a CISO		
Appoint a Chief Information Security Officer (CISO). If the CISO role is outsourced (e.g. Virtual CISO), accountability and ownership of risk sits with the CSO or equivalent senior leadership member. The CISO: • Is a member of the organisation's senior leadership or an equivalent management position • Is qualified and experienced enough to bring accountability and credibility to information security management [CISO Roles and Responsibilities] • Reports directly to the organisation head or delegated senior executive on matters of information security. CISO (including outsourced) conflicts of interest are identified, declared, and actively managed, especially when dealing with other vendors.	.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 1

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Ensure functional management and governance responsibility		
There is clear allocation of responsibility for personnel security, information security, and physical security management. Protective security leadership and management responsibilities and reporting lines are reviewed when relevant organisation structure, people, or responsibilities change. Tools and technologies supporting security management meet basic needs for measuring security compliance.	Protective security leadership and management responsibilities and reporting lines are reviewed regularly, at least every two years. 'Security Manager' roles and responsibilities are formalised for personnel security, information security, and physical security with a reporting line to the CSO for those responsibilities. The 'Security Manager' responsibilities align to recommended responsibilities in the PSR. • Are visible with active day to day management of security for all security domains including driving understanding and compliance with security policies and procedures • Are known across the organisation, and people are confident to approach them when necessary • Regularly engage with the organisation's security leaders and security governance bodies • Conduct incident drills and discussion-based exercises with lessons learned fed back into planning, policy, and process improvements. There is clear separation between security governance and management to support robust assurance. People leading change or other initiatives work with security managers to assess security implications of their initiatives.	Security managers drive the use of research, environment scans, and long-term planning to ensure security priorities and resource levels remain proportionate. A cross-functional group of management representatives is convened to coordinate security controls and measures. Example responsibilities are: • Agree on security roles and responsibilities • Ensure integration of security into risk management, audit, and assurance • Agree on methodologies and specific security practices • Assess and coordinate implementation of security controls • Review security incidents and recommend specific improvements • Support organisation-wide security initiatives.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 2

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 2 Take a risk-based approach		
GOV 2.1 Identify, assess, and manage security risks		
A protective security risk management approach has been adopted that is consistent with the ISO 31000 Risk Management standard. Threat and risk assessments are conducted on the people, information, and assets needing protection. The harm and impacts of compromise of people, information or assets have been assessed appropriately. An organisational security risk management plan is developed and maintained. When working or co-locating with others (suppliers and partner organisations), the organisation identifies and understands the differences in risk and impacts between the organisations and negotiates and agrees the security measures needed to treat the risks for all parties – *assessed as part of GOV 5* Security risks are treated in line with the organisation's assessed level of risk and risk tolerance. Security risks are considered as part of the design phase of processes and systems. Security risks are occasionally reviewed.	The environment is periodically scanned for emerging threats including scheduled and regular review of enterprise risks and security measures for vulnerabilities. Measures are identified to treat the risks. Co-locating and collaborating organisations and suppliers actively contribute to identifying, managing, and reporting on protective security risks – *assessed as part of GOV 5* Security risks are overseen and actively managed as part of the organisation's strategic or enterprise risk management framework. This includes integrating risk reporting and management by its executive team and risk and assurance governance body. Security risk management plans are coordinated, applied consistently across the organisation, and reported regularly to the security governance body.	International and New Zealand security threat information and best practice is routinely used to inform measures to reduce the risks to the organisation. The organisation shares information, expertise, and lessons learned with other organisations that it collaborates with, co-locates with, or works with to improve the resilience of end-to-end processes. Security considerations are embedded into the organisation's change management processes. Security measures are incorporated into automated operational business processes. Security risk management practices and risk response measures have an embedded continuous review and improvement cycle.
GOV 2.2 Formulate security plans		
The organisation's security planning covers all security domains (governance, personnel security, information security, and physical security.) Security planning has been based on an effective risk assessment and the organisation's risk tolerance. Organisation-wide security plans are approved at an executive level.	Security plans are comprehensive and detailed and developed in consultation with people from every section of the organisation, staff involved in security or related work (including health and safety, privacy, and property), and senior management. Security plans demonstrate clear awareness and agreement on acceptable levels of security risk (tolerance) set by the security governance body. Security plans are communicated and accessible to all who need it. Security plans are reviewed: • in response to changes in threats or vulnerabilities • in response to changes to its operating environment • every 2 years to ensure it remains relevant, is sustainable, and informed by changes in the PSR or relevant standards. Security plans are phased into a multi-year roadmap to build and maintain the necessary security capability required to treat its risks in line with GOV8 assessment of current capability. Delivery of security plans is reported to security governance.	Security planning is fully integrated into the organisation's business strategy and planning. Security planning is informed by up-to-date, evidence-based data used to analyse threats, understand trends, and conduct forecasting. **PS-CMM 5** Security planning is continuously monitored, reviewed, and improved in response to real-time data and information.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 2

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 2.3 Define and articulate security policies, processes, and procedures		
Security policies are documented that set out the organisation's approach and commitment to security covering all four security domains. Security policies cover how protective security relates to other organisational governance such as health and safety, recruitment, communications, procurement, audit and compliance, fraud and risk, business continuity and emergency response, policy and procedure management, and operational governance and decision making. Security policies and procedures cover the 20 mandatory requirements, and are accessible, easy to understand, and used effectively by relevant people in the organisation who need them. Security policies and procedures are reviewed whenever security requirements change, or major incidents occur. The review covers: • Policy effectiveness, gauged by security incidents • Cost and impact of security measures • Effects of changes to technology • Levels of user compliance.	The security policies are approved by and overseen by the CSO or appropriate delegated authority. The security policies are based on robust risk analysis, support operations and business continuity, and are cost effective. The security policies are clear on why they are necessary and who has authorised them. The security policies are standardised across the enterprise and monitored to ensure that they are being effectively and routinely used. Security policies and procedures are reviewed at least every two years and in response to: • Changes in threats or vulnerabilities • Changes to the agency's functions, structure, or technical infrastructure. People from across the enterprise contribute to improvement of security policies and procedures.	Security management processes and procedures are continuously improved. Automation is a part of systems and processes to enable security managers to detect, report, and quickly respond to non-compliance with its security policies and procedures.

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 3 Prepare for business continuity		
GOV 3.1 Set the scope of the business continuity programme		
A Business Continuity Management Programme (BCM) is maintained that: • Is agreed with senior management • Covers agreed critical functions • Includes supporting functions and resources required to maintain critical functions or resume them within acceptable timeframes. It is clear how protective security will be maintained during a business continuity event. Security measures are built into the BCM programme. There is a policy that outlines the intent and coverage of the business continuity programme. It is clear who oversees and takes responsibility for business continuity management and development; and management of business continuity plans.	The scope of the programme considers the organisation's legislative responsibilities, overall strategy, objectives, and structure. The policy for managing business continuity covers: • A definition of business continuity management • Reference to standards and guidelines to follow • What the programme covers • How the programme is structured and runs • Links with other policies, processes, and disciplines (e.g. risk management, incident management, heightened alert response, health and safety, emergency management). BCM responsibilities are assigned for: • governance • Senior manager to sponsor the programme • Team to lead the programme implementation • critical function plan owners, and subject matter experts • Security leads to oversee and manage the security measures • Incident response.	
GOV 3.2 Identify critical functions and their requirements		
The organisation's critical functions are identified. A business impact analysis (BIA) has been conducted to evaluate the potential impact over time of disruption on the organisation's critical functions. This has been used to prioritise the organisation's critical services, assets, and information including information exchanges with other organisations and external parties.	Critical functions are assessed including: • The impact over time of a disruption to the functions • Interdependencies between functions • Shared requirements across the organisation. When developing the BIA, the organisation collaborates with people across the organisation responsible for risk management. A risk assessment has been conducted as part of the BIA to identify and quantify the risk of disruption to the function, including risks to the requirements the function needs. Existing identified risks and their measures for reducing them are assessed as part of the BIA.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 3

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 3.3 Develop solutions and plans for maintaining critical functions		

Business continuity solutions, plans, measures, and arrangements are designed and implemented to maintain its critical functions.
Business continuity plans articulate its procedures for responding to disruptions.
Security measures, resources, and requirements are clearly identified and implemented that support business continuity and resilience of agreed critical functions. covering:
• People and capabilities
• Facilities and associated utilities
• Supplies and equipment
• Information and data
• Technology (systems, applications)
• Transportation and logistics
• Suppliers and outsourcing partners.
Business continuity programme is integrated with its incident response processes of other functions including security, health and safety, emergency management, information management, and risk management.
An organisation-wide structure has been established for managing and responding to disruptions with key roles documented and assigned and processes articulated.
	Cost-effectiveness of business continuity solutions has been assessed against recovery time objectives.
	Business continuity plans cover:
	• Processes for notification, activation, and escalation
	• Who will fulfil key roles in a response (strategic oversight, tactical, and operational roles)
	• leadership continuity
	• structures and processes for responding to disruptions
	• response priorities
	• details of critical functions:
	  ○ requirements and timeframes
	  ○ processes for maintaining the function, including where detailed operational procedures or plans can be found
	  ○ changes to security policies and measures during the event. If necessary
	  ○ communication procedures (internal, external)
	  ○ any links to other plans and processes within the organisation.
	Business continuity plans are validated as simple, fit for purpose, and easy to use under the pressure of a response situation.
	Business continuity response teams are trained and have the right skills and competencies to respond effectively during a disruption.
		Business continuity templates, procedures, and checklists are implemented to make plans easy to use.
		People with critical BCM roles do not have competing responsibilities.

GOV 3.4 Monitor organisational preparedness for a disruptive event		
Business continuity exercises are run at least every two years to validate plans and assess preparedness. All people assigned roles in the business continuity programme fully understand the business continuity processes.	Training and awareness campaigns are run on business continuity across all people in the organisation. Additional periodic exercises are run that validate, assess, practice, and improve aspects of business continuity plans.	Business continuity training and exercises include suppliers and cooperating partner organisations.
GOV 3.5 Review and maintain the business continuity programme		
The effectiveness of the business continuity plan is reviewed after activation (either in an exercise or in real-life incidents). The business continuity programme is maintained to enable its critical functions to continue to the fullest extent possible during a disruption. The business continuity programme is maintained when changes occur within the organisation e.g., new functions, changes to organisational structure, changes to third party suppliers, lessons learned from an exercise or incident and findings from an assessment or review.	BCM review recommendations focus on continual improvement.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 4

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 4 Build security awareness		
GOV 4.1 Establish a security awareness and training programme		
Security awareness training needs are identified and used to design security awareness and training programmes to: • Address its identified security risks • Ensure that security policies and procedures are followed • Promote personal responsibility for effective security by all personnel (e.g., employees, secondees, contractors, and temporary staff). Security awareness training covers policies and procedures for: • Maintaining personal safety • Protecting assets • Protecting information Security awareness and training programmes are designed to cover: • All its personnel in its facilities • All its personnel and other people who have access to its information and assets • All holders of a New Zealand national security clearance within the organisation. When relevant, assurance is sought from co-locating and collaborating organisations on their security awareness and training programmes to confirm that: • Personnel based in their facilities receive appropriate security awareness training or briefings • Personnel who have access to its information, systems, or assets receive appropriate security awareness training or briefings on how that information and their systems and assets are to be safeguarded. • Sponsored holders of shared New Zealand national security clearances receive appropriate security awareness training or briefings. Security awareness training covers security measures in: • Facilities, including those shared with other organisations • Other organisation's facilities its personnel operate in. • Places where its personnel work (including working from home or other remote locations). Security awareness programme goals have been set and measured. This includes how it can ensure that its personnel: • Understand the rules and their responsibilities • Understand the threats and the security measures designed to counter • Can perform their security duties effectively. Education needs are actively monitored and reassessed regularly to ensure that security awareness training content remains fit for purpose.	Security awareness training and briefings are designed to cover all people who have access to the organisation's facilities in any capacity. Induction training includes security awareness training, and how to access support.	Security awareness training covers security measures in relation to: • Threats to the organisation/location • Good security standards/behaviours

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 4

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 4.2 Implement security awareness training		
People with emergency, safety, or security functions: • Are provided additional training to ensure they can keep everyone safe in times of danger or threat • Conduct exercises to practice their skills and confirm their ongoing competency. Training is provided to people on how to keep assets secure before allowing them access to those assets. Training is provided, assessed, and measured to ensure that people understand and comply with the Classification System and New Zealand Legislation relevant to official information. - *assessed as part of INFOSEC 2.3* Training is provided on how to report security concerns and risks including: • suspicious behaviour • threatening behaviour communicated through letters, bomb threats, and phone calls • lost, stolen, compromised or broken ICT and security equipment/assets • security infringements and breaches (see GOV 6: Manage security incidents) • security vulnerabilities e.g., insecure classified waste bins, doors left insecure, etc. • lost identity or credit cards • lost protectively-marked, official, or government material • serious wrongdoing (within the same organisation or another).	Security awareness training is an ongoing, regular part of operations including: • Defined plans and schedules for delivery of communications • Security awareness training as part of the induction programme • Regular refresher sessions on key risks and security measures • Targeted training when the threat environment changes or there is an increased risk (or recurring) of security breach • Targeted role specific training as needed.	
GOV 4.3 Build a strong security culture		
Metrics and processes are in place to assess the organisation's security culture (it may be part of a workplace culture survey). Anyone suspected of breaching security is treated fairly and made aware of the process.	Security awareness programme supports a strong security culture through: • Using security campaigns to address recurring or major incidents and near misses, ongoing security issues, or specific needs to do with sensitive areas, activities, or periods of time • Promoting security processes and tips through publications, electronic bulletins, and visual displays such as posters • Conducting security drills and exercises • Including security questions in job interviews • Including security attitudes and performance in performance management programme. Participation in security training is tracked and recorded. Processes are in place to evaluate people's adherence to security obligations. Non-compliance and breaches are raised as security incidents. The organisation's leaders: • Deliver consistent and positive messages about how the organisation views and manages protective security • Lead by example, by actively and visibly demonstrating their commitment to good security practice. Protective security is integrated into business processes where possible to help people follow good practice by default.	Security training is reviewed to ensure it is aligned to best practice and stimulates functional security discussions and enhances its security culture and practice. Security culture is regularly monitored to inform improvement plans, security awareness programmes, and education resources.

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 5 Manage risks when working with others		
GOV 5.1 Understand the risks when working with others		
The organisation fully understands who their suppliers are, what they have access to, the supplier's security measures, and the depth of their supply chain involved in the specific elements of their contract. This includes: • Sensitivity of contracts let or that will be let • Value of the information, services, or assets that suppliers hold, access or handle as part of the contracts. • Potential impact of loss or harm to information, services, or assets that suppliers hold, access or handle. The organisation fully understands who it is co-locating/collaborating with, what their respective security risks and impacts are, and have agreed security requirements for all parties. The supply chain security risks (for the supplier and its supply chain) have been identified and assessed as part of the contracting process.	The organisation maintains ongoing visibility of its supplier's and co-locating/collaborating organisation's security risks and ensures they actively contribute to identifying, managing, and reporting on risk when required	
GOV 5.2 Establish effective control and oversight of your supply chain		
Communicate security requirements		
New Zealand Government Rules for Procurements, particularly Procurement Rule 44, are followed if mandated to do so. Minimum-security requirements are identified and defined based on risk when developing tender documents, evaluating proposals, and over the life of the contract. The requirements: • Reflect the organisation's assessment of security risks • Are specific and enforceable • Identify circumstances where exceptions may be allowed • Outline the steps that will be taken to manage security. • Reflect the highest security classification and its associated protective security measures. • Include requirements for terminating or transferring services to another supplier. The organisation communicates its security requirements to suppliers and ensures that suppliers understand their responsibility to protect its information, and products and services. Before awarding the contract, suppliers are required to provide evidence of their approach to security, and their ability to meet the minimum-security requirements is verified. Where justified, the organisation builds assurance requirements into its security requirements. For example, assurance reporting, penetration tests, external audits, and formal security certifications.	Supplier personnel working on a contract are required to be screened to the pre-employment screening standard as defined in PERSEC1 in line with the assessed risk of their role or nature of access. For certain types of contracts, a supplier's personnel are required to sign a non-disclosure agreement. Suppliers are required to pass minimum-security requirements down to all sub-contractors when they have access to the organisation's information and assets.	The organisation conducts the pre-employment checks on behalf of the supplier.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 5

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Build security into contract conditions		
Security considerations are built into contracting processes to ensure that security is managed through the life of the contract, including terminating or transferring services to another supplier. The conditions for when sub-contracting is allowed are defined; noting that formal written approval is required for any supplier with access to government information. When authorising a supplier to sub-contract, the organisation has: • Delegated the authority to allow the supplier to sub-contract • Provided clear guidance on the criteria for sub-contracting decisions including when they need your approval and sign-off • Included security requirements into sub-contracting arrangements. Contracts include the right to terminate the contract if the supplier fails to comply with security requirements. Contracts clearly set out requirements for the return or deletion of the organisation's information and assets on termination or transfer of the contract. When a supplier handles government information classified at CONFIDENTIAL or above, the contract includes conditions: • Explicitly identifies the highest level of classification/protective marking they will handle. • Requires the supplier to ensure that all personnel with access must hold and maintain a relevant national security clearance and comply with all requirements defined in PERSEC 4. • Requires the supplier to report when any of their personnel who do not have a security clearance have any incidental or accidental contact with classified and protectively-marked material. Supplier contracts include the following terms and conditions for government information requiring them to: • Disclose any potential conflicts of interest that would affect security when they work on behalf of the New Zealand Government • Have their premises and facilities meet the minimum standards for storing and handling government information, up to the nominated security classification level. • Have systems that meet designated information security standards for processing, storing, transmitting, and disposing of government information that is in electronic formats as defined in the NZISM. • Follow directions for keeping government information confidential which may extend beyond the end of the contract. Contracts clearly set out requirements for managing and reporting security incidents including timescales and support they can expect. Contracts include a 'right to audit' and require its suppliers to do the same for contracts they sub-let.	Relevant suppliers are required to have personnel, physical, and procedural measures to protect against fraud, theft, and insider threats. Contracts are renewed at appropriate intervals and the supply chain risks are re-evaluated at that time. When there is legal or jurisdictional risk of third-party access (e.g., overseas owners or stakeholders) to the organisation's information or assets, contract terms and conditions are included to limit third-party access and protect from information compromise.	**PS-CMM 5** To manage security at all levels throughout the supply chain, suppliers are: • Provided with supporting security guidance, tools, and processes • Required to use them in their contract • Trained to use them.
Meet your own security responsibilities as a consumer		
When requirements are placed on the organisation as a consumer of information, assets, premises, products, or services, the organisation has: • Incorporated those requirements into the organisation's security obligations and plans • Provided upward reporting to senior management • Passed security requirements down to suppliers and sub-contractors • Enabled audits and reviews • Reported any issues encountered • Worked proactively with customers and partners to improve security.		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 5

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Raise security awareness and provide support for suppliers		
Security threats, information and risks are shared with suppliers and are encouraged to explain the threats and risks to their people. When a supplier's personnel changes, the organisation ensures that: • Supplier personnel who access government information are reminded of the continuing need to maintain confidentiality • New supplier personnel understand the organisation's security requirements. The organisation shares lessons learned from security incidents with all its suppliers, partners, and cooperating organisations to help improve resiliency across the entire supply chain.	A supply chain security awareness and education programme has been established. Suppliers are required to report incidents or suspected incidents that could affect: • Their ability to deliver their contracted services • Your organisation's information (when they are holding or transporting it.) • The security of another client's information, assets, products, or services that identifies a vulnerability or threat that could affect the security of your organisation's information, assets, products, or services.	
GOV 5.3 Check your supply chain arrangements		
When suppliers are key to the security of your supply chain, the organisation requires them to report to the contract manager on security performance. The organisation undertakes audits of contracts where when the right to audit has been stipulated. This may include accessing the supplier's premises, records, and equipment. Where contracted, the organisation undertakes assurance of suppliers' compliance with security requirements (e.g., penetration tests, external audits, assurance reporting, and formal security certifications).	The organisation measures the security performance of its supply chain by: • establishing and monitoring supplier key security performance indicators • reviewing and acting on any findings and lessons learnt • encouraging suppliers to promote good security behaviours.	The organisation performs periodic audits and assessments of security capability when stipulated by contract to confirm their compliance with security requirements and effectiveness of its measures.
GOV 5.4 Continuous improvement		
	The organisation encourages its suppliers to continuously improve their security arrangements: • Advises and supports suppliers as they work on improvements. • Avoids creating unnecessary barriers to improvements. • Allows time for the supplier to improve security but requires them to give timescales and plans that show how they intend to achieve the improvements. • Listens to and acts on any concerns that suppliers highlight — concerns which suggest current approaches are not working. The organisation seeks to build strategic partnerships with its key suppliers by: • sharing issues with them and encouraging and valuing their input • getting their buy-in to the organisation's approach to supply chain security • letting them manage sub-contractors on the organisation's behalf, but requiring them to report on their security performance • maintaining regular and effective communication.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 6

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 6 Manage security incidents		
GOV 6.1 Establish an effective approach to managing security incidents		
The organisation has systems in place for security incident management. Incidents are categorised based on its severity. The organisation has formal policies and procedures for managing major security incidents.	The organisation has policies and procedures for managing minor security incidents. Incident management policies and procedures cover: • roles involved in managing and responding to security incidents • procedures for investigating security incidents in line with relevant legislation. The organisation has a well-established security incident management plan that maintains readiness and coordination of major incident responses which includes: • Actions and responses according to incident scenario • A roles and responsibilities matrix • Thresholds and procedures for leadership and other internal and external stakeholder notifications and escalations (including relevant government agencies) • A communication plan and message templates for notifying personnel • Interrelationships with changing threat levels, business continuity, and health and safety responses. Incident drills and exercises are conducted to improve responses and feed lessons learned into policy and process improvement programmes.	The organisation monitors internal and external security environments for issues affecting the appropriate response to an incident and uses this to inform improvements to responses.
GOV 6.2 Ensure that security incidents are raised and detected		
Personnel are required to raise security incidents, weaknesses, and threats as soon as possible after it has occurred or is suspected. Mechanisms that make it easy to raise security incidents are provided for all people. This includes information on: • What a security incident is and when to report • Impacts of security incidents and why it is important to raise them • Consequences for not following security policies and procedures • How to respond and raise security incidents, and who to inform • How the information will be dealt with (with sensitivity, confidentiality, and fairness).	The organisation has mechanisms in place that quickly detect potential security incidents including: • Logging and monitoring of security related events • Alerting of detected anomalous security events • Automating security incident response where appropriate.	Collaboration tools and systems are in place to make it easy for people to understand how to report security concerns and actively engage in enhancing security measures.
GOV 6.3 Record and assess security incidents		
The organisation has appropriate methods for recording and tracking incidents. The organisation assesses the harm caused by security incidents to determine impact on the organisation, New Zealand government, or other stakeholders.	Security incident records include: • the time, date, and location (or when it was reported or discovered) • the type of government resources involved • a description of the incident's circumstances • what may have been compromised (and the type and Business Impact Level (BIL), if relevant) • the names of those involved in the incident if known • whether the incident was deliberate or accidental • an assessment of the degree of compromise or harm • a summary of the immediate and long-term action you will take.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 6

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 6.4 Report security incidents to relevant agencies		
The organisation does an initial assessment of harm and impact of relevant incidents and contacts the relevant agency or agencies as soon as possible following the incident notification. Incidents relating to national security clearance holders are notified to NZSIS including repeated minor security incidents, major security incidents, and any outcome of security investigations that relates to their ability to hold a security clearance. Government organisations report information security incidents to the NCSC as defined in the NZISM. Incidents relating to Cabinet material are reported to the Cabinet Office. The organisation seeks advice from the NZ Police if they suspect the security incident may be a criminal offence. Once reported, the organisation provides the relevant agency any updates or changes to the situation. When reporting suspected major incidents to government organisation, the government organisation is provided with the security incident record details gathered.		
GOV 6.5 Investigate and respond to security incidents		
When undertaking a security incident investigation against an employee, the organisation follows a fair process, acts in good faith, uses natural justice principles, and follows guidance in compliance with the Employment Relations Act. While under investigation, the organisation considers the timing, 'need to know' and the extent to which security incident information can be shared. HR advises on information sharing suitability. While investigations are underway, the organisations interim responses are targeted, temporary, justifiable, and proportionate to the concern held to protect its people, information, or assets.	While investigations are underway, interim measures are considered to reduce the impact of security incidents and support the investigation. If interim measures are taken against an employee, the employee is informed what measures have been taken, that they are temporary while the investigation is ongoing, and that they do not signal predetermination. When security incidents involve people, information, or assets from another organisation, the organisation works with that organisation to manage the incident. The organisation works with relevant government organisations on security investigations and responses.	Major security investigations are subject to independent review to confirm the investigation has been handled appropriately and fairly.
GOV 6.6 Learn from security incidents		
Corrective action occurs in response to relevant incidents and an improvement plan is in place.	The organisation monitors and measures the types, volumes, and costs of security incidents which are used to: • Identify recurring or high-impact problems • Identify when new measures are needed to limit problems • Review the security policy and procedures • Inform additional training requirements The organisation has defined when security incidents are subject to post-incident reviews and undertakes them appropriately. This includes: • Conducting root cause analysis when appropriate • Reporting to security governance on the incident, the measures taken, and outcomes from the actions • Confirming that the incident was raised appropriately and followed good incident management process • Incorporating findings into incident management plans, policies, and procedures and addressing gaps in security culture, awareness, and training.	**PS-CMM 5** The organisation conducts ongoing research into measures for preventing and managing incidents including engagement with external experts.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 7

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 7 Be able to respond to increased threat levels		
GOV 7.1 Identify sources of risk for heightened security alert levels		
The organisation uses information on threats and risks from internal sources to inform its alert response plans including: • Security plans, threat and risk assessments, and risk management plans • Business continuity plans • Post security incident reviews • Security governance reports.	The organisation uses information on threats and risks from external sources to inform its alert response plans including: • National emergency management agency (NEMA) • National terrorism threat level and associated assessment advice • Police, MetService, and Civil Defence advisories • National Cyber Security Centre (NZSC) and CERT NZ • media reports.	
GOV 7.2 Develop alert levels		
The organisation takes an 'all hazards' approach to developing its alert levels and response plans to ensure it is ready to respond to emergency and increased security risk situations.		
GOV 7.3 Plan your response during heightened security alerts		
The organisation uses its assessment of threat and risk sources and operational requirements for each facility it operates in to establish the security measures needed at each alert level following best practice guidance. The organisation has plans, criteria, and process for increasing security alert levels during a heightened event which includes steps to return to normal alert levels after the event has concluded.	The organisation has developed right-sized plans and procedures (balancing protection and cost) for each facility and type of threat or risk, working with local area managers and risk experts to establish them. Plans for responding to heightened alert levels are: • integrated and coordinated with other business continuity and emergency prevention and response plans (fire, bomb threat, hazardous materials, power failure, evacuation, or civil defence.) • flexible to manage changing circumstances in real time.	
GOV 7.4 Monitor the risk environment and change alert level when necessary		
The organisation has successfully used its security alert response plans during emergencies, heightened security risk events, or drills to change (increase or decrease) the alert level in response to changes in risks. The organisation communicates changes in alert levels to its people to inform them on what has changed and what to do.	During alert level changes, communications are targeted to different audiences with different messages, methods, and responsibilities. After the event, the organisation conducts a debrief to review why and how the alert level was changed, the activities and actions undertaken, and identify improvements to make to procedures and communications.	
GOV 7.5 Review and update your processes		
The organisation practices and review activation procedures and the security measures at each level to identify gaps. The plans are updated accordingly.	The organisation reviews its alert level processes: • at least every two years • when it takes on new projects or the risk environment changes • after a significant incident that affects its ability to operate.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 8

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 8 Assess your capability		
GOV 8.1 Monitor and measure your protective security performance		
The organisation regularly monitors the performance of its protective security practices and plans, and reports to its security governance body. Security practices are monitored to ensure they are generally repeatable, verified and results show that they are consistently followed within the organisation.	The organisation has established and monitors key performance indicators and reviews, acts on findings and lessons learned and promotes good security behaviours. Historic performance information is used to understand security effectiveness and trends.	Detailed performance measures are baselined, measured, and reported to understand where vulnerabilities exist. This information is used to inform governance oversight and decisions. The organisation uses continuous monitoring and spot checks to detect breakdowns in its security measures. Monitoring is supported by automation in high-risk areas. Key performance indicators inform continuous improvement and real-time security responses. **PS-CMM 5** Continuous improvement programme includes continuous monitoring and control with active contribution and management by relevant experts and service providers. Protective security performance measures go beyond the enterprise to include all touch points with customers, partners, and suppliers.
GOV 8.2 Assess your protective security capability		
The organisation self-assesses its protective security capability at least annually. The organisation assesses how its capability maturity has changed as a result of changes in the environment such as when: • Key personnel have left the organisation • Technology has changed • The threat environment has changed • Resource assignments have changed. The organisation gathers and uses evidence in its assessment that demonstrates how well its security policies, processes, and measures achieve the objectives set out in the PSR, and reduce the risks identified. Performance against security policies and procedures can be measured and are occasionally verified (audited).	The following types of evidence are used to assess its protective security capability: • Risk management plans, threat assessments, and risk reporting • Documentation of policy, processes, and procedures • Compliance with policies, processes, and procedures • Security programme deliverables • Security incidents including infringements and breaches • Changes in security personnel and responsibilities • Security performance measures and reports • Personnel training, awareness programmes and engagement surveys. The organisation involves people representing different parts of the organisation in its assessment, from executives to specialists. These workshops are used as a learning process that provides a good forum for balancing needs and priorities. The organisation uses PSR-provided self-assessment tools, providing answers and explanations that best represent the organisation's current capability maturity as demonstrated by the evidence gathered.	The organisation conducts effectiveness audits, and these findings are used to inform improvements.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – GOV 8

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
GOV 8.3 Set your protective security goals for improvement		
Information from multiple sources informs decisions and planning – evaluating information relevance and reliability.	The organisation sets its goals for capability and maturity in line with its risk exposure and tolerance which are: • Prioritised to address the greatest risk exposure • Realistic based on what can be accomplished • Aligned to strategic goals and priorities • Reflective of the current stage of the protective security capability development journey. Historic performance information is periodically reviewed and used to inform where improvements should be made. An annual proactive protective security improvement programme is planned, tracked, and well managed and governed. The programme is well resourced to maintain capability and maturity.	Protective security performance measures (goals) are set and aligned to organisational strategy and business goals. Security is a strategic issue for the organisation; protective security skills are continuously updated to ensure knowledge remains current. **PS-CMM 5** Continuous improvement programmes are supported by real-time performance data and automated response mechanisms.
GOV 8.4 Provide assurance of your protective security capability and goals		
The organisation has an assurance process that provides its leaders and security governance body with confidence that: • The capability and maturity self-assessment is accurate • Capability gaps are known • Risk response measures and security plans are effective • Goals are appropriate to address its specific risks.	The organisation uses its risk and assurance function to provide internal or external independent assurance of the accuracy of its PSR capability and maturity self-assessment and plans (e.g., conducts an effectiveness audit or independent moderation). The organisation uses independent oversight and assurance expertise to: • confirm protective security performance • independently assess effectiveness of security measures • give expert advice and guidance to security personnel • provide assurance to the organisation head, security leaders, and security governance body that the right investments are being made to address protective security priorities.	The organisation regularly audits the implementation and effectiveness of its security risk measures that are not subject to continuous monitoring. The organisation has a governance or audit committee that provides independent oversight of the effectiveness and efficiency of its security plan. Detailed performance metrics are baselined, measured, and reported to understand where vulnerabilities exist. This information is used to inform governance oversight and decisions.
GOV 8.5 Report on your protective security capability and improvement plans		
The organisation regularly reports to its Chief Executive and security governance body on its security capability, goals, and plans. PSR mandated organisations report to the PSR Unit on their protective security capability, maturity, and compliance with mandatory requirements of the PSR. The reporting confirms and provides detail and evidence on its honest assessment of current capability.		Regular security reporting is provided to senior leaders that supports strategic oversight and decisions to support a secure and effective workforce.

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 1 Recruit the right person		
PERSEC 1.1 Carry out baseline checks for all roles		
Baseline pre-employment checks are undertaken to the standard defined in PSR PERSEC 1.1 policy: • Confirm their identity and nationality • Confirm the right to work in New Zealand and/or the country they will be working in • Check references with former employer • Conduct a Ministry of Justice criminal record check (after receiving the person's written consent) For existing or former employees applying for new roles, the organisation's records (e.g., performance, disciplinary, incidents) are reviewed to confirm suitability. The organisation sights original documentation (or certified copies) such as the candidate's passport or birth certificate. There are policies and procedures to ensure references are: • Recent (last employer) • Relevant (appropriate to the role) • Legitimate (validity of the source) • Free from conflict of interest (e.g., not a close personal relationship). Overseas criminal record checks are considered and undertaken in agreement with the candidate for overseas residents and recent migrants.	There are policies and procedures for assessing concerns and unexplained discrepancies found in baseline checks.	
PERSEC 1.2 Conduct additional checks where an increased security risk is identified		
Roles have been identified requiring additional pre-employment checks based on legislated requirements and/or increased risk. The person's consent is obtained in writing before conducting any additional pre-employment checks. A qualification (or occupational registration) check is conducted when occupation registration is required to work in New Zealand.	Policies and procedures define the additional checks which are conducted and how they are conducted to manage identified risks such as: • Psychometric testing • Qualification (or occupational registration) checks • Credit checks • NZ Police Vetting • Drug and alcohol checks.	The organisation conducts checks to confirm that the educational qualifications, professional body memberships or practising certificates claimed by the applicant are legitimate. The organisation conducts additional checks for higher risk roles/candidates where assessed as necessary: • Credit checks when the role carries a significant financial risk. • Psychometric testing is conducted if there are concerns from baseline checks or if it is difficult to assess if the person has the abilities and traits required for the role. • Drug and alcohol testing are conducted for roles which involved working in safety sensitive areas or directly affect the safety of other people. These are also conducted when other checks suggest the applicant may have problems with drug or alcohol use.
PERSEC 1.3 Address any concerns from pre-employment checks		
There are clear policies and procedures to ensure appropriate personnel are alert to warning signs from pre-employment checks. The organisation records: • Checks completed • Concerns that arose during the pre-employment checks • Risk assessments carried out • Decisions made to reduce or manage risks.	When concerns are raised by pre-employment checks, the organisation has clear policies and procedures to assess the risks associated with the individual performing the role and identify how the risk can be reduced to an acceptable and manageable level. Individual risk management plans are developed with the individual when necessary to support the person in their work and to actively manage the organisation's security.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – PERSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 1.4 Set the right expectations		
Robust practices are in place to ensure personnel are educated on security policies and expectations when joining the organisation – *assessed as part of GOV 4.1* Induction is conducted with new personnel, including on organisational values, code of conduct, health, safety and security procedures, and workplace expectations.		

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 2 Ensure their ongoing suitability		
PERSEC 2.1 Minimum requirements to ensure ongoing suitability		
There are policies and procedures in place to: • enable its personnel to report personnel security concerns and incidents (assessed in GOV4) • assess and respond to relevant personnel security concerns and security incidents to ensure contain events and manage consequences (assessed in GOV 6) • provide ongoing security awareness updates and training tailored to the organisations security risks and the risks associated to individual roles (assessed in GOV4).	The organisation has clear guidelines and procedures for assessing and managing personnel suitability and integrity concerns, both at initial hiring and ongoing through their tenure. Managers are provided with tools and support to help them manage concerning behaviour relating to security, poor performance, or unacceptable conduct. Personnel are provided with access to support such as the confidential employee assistance programme.	An insider threat programme is in place to address insider risks. **PS-CMM 5** Personnel have access to a dedicated internal wellbeing support service.
PERSEC 2.2 Carry out ongoing suitability checks for higher risk roles		
The organisation has policies and processes for undertaking ongoing suitability checks for higher risk roles including contractors (not holding a national security clearance.)	Ongoing suitability checks are used when there is increased security risk or where concerns arise from reports or incidents as defined in policies and procedures on when the following apply: • reporting changes of circumstances • reporting suspicious, ongoing, unusual, or persistent (SOUP) contacts • encouraging people to report any suspicion of insider threat • briefing and debriefing people on the risks of international travel • conducting engagement surveys • requiring regular police vetting • carrying out periodic financial or credit checks • requiring drug and alcohol testing • checking regularly for conflicts of interest, and • obtaining copies of annual practising certificates. Insider risks are identified and managed associated with high-risk roles, or groups of people, who have greater potential to cause harm due to their access to sensitive, valuable, or highly classified information or assets.	Role specific risk assessments are reviewed regularly to confirm they are accurate and up to date (e.g. when role, personnel, process, information, system changes).
PERSEC 2.3 Manage role changes		
Before confirming an existing person into a different role, the organisation makes sure that all required pre-employment checks and/or on-going suitability checks have been completed to the level required for that role.		
PERSEC 2.4 Manage contractors		
The same personnel security measures are used with contractors as are applied to permanent employees including pre-employment checks, induction, ongoing suitability assessment, role changes, and departure.	The organisation actively monitors and manages the insider threat of contractors in line with best practice guidance (e.g., PSR guide to hiring and managing contractors).	

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 3 Manage their departure		
PERSEC 3.1 Remove access and collect assets		
The organisation manages personnel departures by: • Removing the person's permission and ability to access electronic resources, documents, systems, and physical sites. • Collecting all identification cards and access passes (including any tools that allow remote access to information systems) • Collecting all property belonging to the organisation.		
PERSEC 3.2 Conduct debriefs and confidentiality agreements		
N/A	When there is higher risk associated with a particular role or a person's circumstances, the organisation conducts an exit debrief to: • Remind the person of any ongoing obligations relating to the organisation's people, information, and assets, in particular intellectual property or official information • Invite them to discuss their reasons for leaving, and their perception of the organisation and its people • Enable assessment and management of any risks identified with the departure.	The organisation uses confidentiality agreements with the outgoing person to protect the organisation's proprietary information or intellectual property.

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 4 Manage national security clearances		
PERSEC 4.1 Determine the clearance level needed		
The national security clearance level required for the role is defined based on the security classification of the government information, assets, or work locations that the individual needs access to. It is not based on rank, seniority, or status. To determine the level of national security clearance, the organisation: • Analyses the duties of the position • Identifies the highest level of classified information, assets, or work locations the person will need access to • Determines if they will need access to SCI • Decide how long the person will need the clearance for (i.e., short-term or permanent role) • Consults its security staff throughout the process.		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – PERSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PERSEC 4.2 Determine eligibility and suitability for a national security clearance		
Before submitting a request for vetting, the organisation checks the candidate's eligibility for vetting for the clearance level including that they: • Meet citizenship and visa requirements • Meet minimum requirements for checkable background for the clearance level requested. Before submitting a request for vetting, the organisation ensures that it has trust and confidence in the candidate's suitability for holding a clearance by undertaking a review of records (such as performance or disciplinary records.) Any records that show dishonesty, misconduct, or breaches of the code of conduct are reviewed to ensure they are suitable to hold a clearance. The organisation reviews the vetting recommendation by the NZSIS Vetting Service before deciding whether to grant the clearance. If the NZSIS Vetting Service recommendation includes qualifications, the organisation follows the specific recommendations that the NZSIS has made for managing security concerns. It establishes an individual security risk management plan with the clearance holder. If a complaint is lodged with the IGIS on the vetting process, the organisation waits for the IGIS' complaint process is finished before taking further action. Once granted a clearance, the clearance holder is provided with: • A briefing on their responsibilities to protect classified information, assets, and work locations • Requirements for reporting any change in circumstances or suspicious contacts • Details of the organisation's security awareness training programme. • Briefings relevant to any sensitive compartmented information they require access to.	When positions are advertised that require a clearance, the potential applicants are informed that they will need to be vetted for a clearance and to which level and includes an outline of the eligibility criteria or links for eligibility self-check. For roles requiring a clearance, obtaining, and maintaining a clearance is a formal condition of employment in the candidate's employment agreement (or contract for services). The organisation does not grant a clearance when they receive an 'adverse' recommendation from the NZSIS.	When deciding to grant a clearance to a foreign national, the organisation makes gaining New Zealand citizenship a condition of maintaining their clearance.
PERSEC 4.3 Ensure the ongoing suitability of clearance holders		
The organisation provides clear policies and procedures that explain the requirements specific to clearance holders. Clearance holders have clear and regular communications to ensure they understand and acknowledge their specific responsibilities. Security awareness training is provided for clearance holders at the time their clearance is granted and at least every five years as a condition for re-validating the clearance renewal. Clearance holders are provided with tailored security briefings and debriefings when appropriate.	Clearance holders are supported to meet their responsibilities to ensure they remain suitable to hold a clearance. This includes: • Annual security awareness training covering the clearance holder's responsibilities.	.
Prepare clearance holders for international travel		
The organisation has an overseas travel policy requiring clearance holders to: • Consult the policy and security team to understand security risks and obligations while traveling • discuss their travel plans before booking overseas travel (for personal or business reasons) • get formal permission from the organisation before finalising travel plans, and • obtain a travel briefing before travelling when deemed necessary by the security team. The organisation seeks approval from GCSB for clearance holders with SCI briefings to travel to specified countries.	Clearance holders are provided with security guidance to help prepare them for overseas travel.	Restrictions are set on places clearance holders with SCIs can visit, airlines they can use, and activities that they can take part in.

PSR CAPABILITY MATURITY MODEL (PS-CMM) – PERSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Ensure clearance holders report changes in personal circumstances		
The organisation requires clearance holders to report any significant change in personal circumstances to the organisation as soon as it happens. The following are considered significant changes: • starting or ending a close personal relationship • living in or visiting foreign countries • relatives living in foreign countries of security significance • changes in citizenship or nationality • changes in financial circumstances (for example, significant increases in wealth or debt) • changes in health or medical circumstances • involvement in criminal activity, accidentally or deliberately • involvement with any individual, group, society or organisation that may be of security concern • disciplinary procedures or security incidents that the organisation is involved in, and • any other changes in circumstance that may be of concern to the organisation. The organisation conducts an annual security appraisal process on all its clearance holders requiring them to report any significant change in personal circumstances or anything of security concern. When a change in circumstance is raised, a risk assessment is conducted to determine whether the organisation needs to take further action (i.e. an individual security risk management plan).	When a change in circumstance risk assessment indicates a serious issue that cannot be managed, the security clearance is suspended or cancelled until the risk is mitigated or the risk is no longer present.	
Ensure clearance holders report security concerns and suspicious contacts		
The organisation requires clearance holders to report concerning behaviours or incidents relating to themselves or other people they work with. The organisation requires clearance holders to report suspicious contacts or requests to access their organisation's information, assets, or work locations.	Clearance holders complete a contact reporting form when an official or social contact appears suspicious, ongoing, persistent, or unusual (SOUP) in any respect. The organisation has a clear process to undertake assessment of SOUP contact reports that may have serious implications requiring notification of appropriate authorities to conduct further investigation.	
Ensure clearance holders minimise risks from social media use		
The organisation ensures that clearance holders are informed on what they should and should not reveal, share, and use on social media.		
PERSEC 4.4 Manage security clearances		
Monitor for concerning behaviour and incidents		
Managers of clearance holders monitor the clearance holder's behaviour for any security concerns, poor performance, unacceptable conduct, or signs that could suggest that the person is unreliable or susceptible to pressure. When behavioural issues are identified, managers support the clearance holder through any resolution process. The organisation keeps records of all clearance holders' security infringements, breaches, and violations.		
Assess and respond to security breaches		
When there is evidence that a clearance holder has made a security breach and/or violation, the organisation establishes an appropriate response which may include: • Providing additional security awareness training • Advising NZSIS or the GCSB • Initiating a 'review for cause' • Suspending access to classified information, assets, or work locations while undertaking a security incident investigation • Reviewing if the clearance should be revoked if they no longer have confidence in the suitability of the clearance holder to hold a clearance. – *assessed as part of GOV 6.4*		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – PERSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Manage changes to security clearances		

The organisation actively uses Tiaki to manage and administrate clearances and the vetting process according to PERSEC 4 policy. This includes:
• The organisation ensures that all sponsored active clearances remain valid if still required for the role.
• Extensions to clearances are only granted:
  ○ before a clearance expires and if there are no qualifications on the clearance
  ○ for up to six months at a time and for no longer than a maximum 12 months
  ○ Due diligence indicates the clearance holder remains suitable
  ○ In agreement with other government organisations when the clearance is shared.
• When agreeing to transfer a clearance holder's clearance, it ensures that:
  ○ The clearance ls less than five years old
  ○ The clearance level meets the requirements for the new role
  ○ The clearance is at the same level as the last vetting recommendation
  ○ The clearance holder moves directly from one organisation to another without an intervening period with no security oversight
  ○ The new organisation obtains the vetting recommendation including any risk management advice
  ○ Written assurance of the clearance holder's continuing suitability to hold a clearance
  ○ Notification of any relevant clearance holder's personal circumstances after they were last vetted.
• Before agreeing to share a clearance holder's clearance, the sponsoring organisation:
  ○ Obtains permission from the clearance holder to share personal information with the other organisation
  ○ Informs the other organisation of the last vetting recommendation
  ○ Shares any risk management plans in place for the clearance holder
• Clearance renewal requests are initiated early enough to maintain continuity of the clearance
• When needing to upgrade a clearance to a higher level, the sponsoring organisation:
  ○ Ensures the holder is eligible to hold the clearance at the higher level
  ○ Initiates the request to upgrade the clearance via Tiaki
  ○ Grants the clearance after NZSIS recommendation is received
Before submitting a renewal request to the NZSIS Vetting Service, the organisation assesses that the clearance holder remains suitable for holding a clearance, there is still a role-based need for a clearance.
When agreeing to share a clearance holder's clearance, the sharing organisations:
• Share ongoing security concerns about the clearance holder
• Agree how the clearance will be managed what each organisation is responsible for
• Inform each other about any changes in the clearance holder's personal circumstances
• Ensure the clearance holder receives appropriate security briefings
• Review and confirm that the sharing agreement is still acceptable
• Manage sharing agreement suspensions or cancellations.
• Briefs the holder on any new obligations associated with the higher clearance level
• Agrees a plan for managing concerns or requirements in the NZSIS' vetting recommendation.		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – PERSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
Manage emergency access to information, assets, and locations that require a national security clearance		
The organisation does not grant emergency access to information, assets, or work locations that are classified CONFIDENTIAL or above to anyone who does not hold a clearance. Emergency policies and processes are in place to ensure emergency access to information, assets, and locations classified CONFIDENTIAL or above are managed in line with the PSR requirements. This includes that emergency access is: • Approved by the CE or their delegate and recorded in writing • Limited to specified information, assets, or work locations required for the emergency • Only for the duration of the emergency • Governed by a very strict application of the need-to-know principle • Provided at no more than one level above a person's current clearance • Supervised by a manager with a suitable clearance • When access is required to SCI, approved by the NZSIS and GCSB. Once approved, the emergency access is recorded, and the clearance holder is briefed ahead of the access provided and debriefed when the emergency access ends. Emergency access is not used for: • Administrative or management purposes • When an individual is reassigned duties while waiting for a security vetting recommendation • Access to classified information, assets, or locations that carry a SCI marking.	The organisation has the clearance holder acknowledge that they have been briefed on the emergency access in writing.	
PERSEC 4.5 Manage the clearance holder's departure		
When a clearance holder leaves the organisation, the organisation carries out the baseline PERSEC 3 activities and: • reminds them of their continued need for discretion and their lifelong obligation to protect government information, assets, and work locations. If the exiting clearance holder had access to SCI, the organisation: • ensures that the holder is debriefed from any SCI briefings they hold, unless the GCSB has given alternate advice • conducts an exit appraisal with the clearance holder • maintains post-separating contact with the departed clearance holder.	In some circumstances, the organisation also asks departing clearance holders to: • provide written acknowledgement of their lifelong obligations to protect classified information, assets, and work locations • maintain post-separation contact with the organisation if they held SCIs.	

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4** **COULD** statements, recommended for **HIGH** risk and above
INFOSEC 1 Understand what you need to protect		
INFOSEC 1.1 Understand the value of your information		
An information assets and ICT system inventory has been carried out. For each item in the inventory, the organisation assesses and understands the impact and harm that could eventuate if the information were compromised. Compromise of collections of information (aggregated information) can have greater impact and harm than the compromise of any single item. Extra security measures are considered and applied when appropriate for collections of information.	An information and ICT system inventory is comprehensive enabling a clear understanding of business value, function, and security requirements: • How it is used, processed, shared, stored and by whom • Confidentiality, integrity, availability, privacy, or legislative requirements that apply • How long it needs to keep and protect the information • Minimum level of system performance and accessibility required for the organisation to function • What destruction and disposal requirements apply • Its location and physical security requirements	
INFOSEC 1.2 Assess the risks to information security		
Capability assessed as part of GOV2.		
INFOSEC 2 Design your security measures		
INFOSEC 2.1 Adopt an appropriate information security management framework		
An information security management framework has been adopted that is relevant, appropriate, and consistent to address the organisation's risks and integrates with other security governance and management frameworks used.		
INFOSEC 2.2 Design and implement information security measures		
Information security measures are designed and implemented in line with New Zealand Information Security Manual (NZISM). Appropriate and up to date information security design approaches are used when designing security measures to address its specific risks (e.g., defence-in-depth, zero trust architectures, security by design). Access control measures are in place for controlling access to all information, ICT systems, networks (including remote access), infrastructure and applications. These are designed in consideration of: • Classification of the information being protected • Threat environment • User access management applying least privilege • User responsibilities and segregation of duties • Network and resource access control • System access control and login security • Privileged user access management including policies and governance • Application and information access control • Risks associated with other working situations (e.g. mobile computing, remote working, BYOD). Appropriate security measures are in place to address relevant specific information security scenarios identified as part of INFOSEC 1.		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – INFOSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4** **COULD** statements, recommended for **HIGH** risk and above
INFOSEC 2.3 Follow the Classification System		
Adopt Classification System Principles		
Principle 1: Organisational Accountability		
Organisational classification policies and procedures have been established that ensures its people handle government information correctly and securely. The policy and procedures include: • The obligations set out in relevant legal, regulatory, or other agreements (e.g., Official Information Act (OIA), Privacy Act, Public Records Act, International agreements) for managing official, private, partner, and government information • How information is protected in line with these obligations and its classification and protective marking (including relevant PERSEC, INFOSEC, and PHYSEC security measures) • How to classify appropriately (at the lowest possible level) based on a risk assessment of the level of harm and impact and the likelihood of compromise. • How the organisation meets its obligation to make government information available • How originator control is maintained over the information lifecycle. Personnel are provided with relevant, timely, and ongoing classification training (e.g., how to securely handle, classify, share, and declassify) and their training understanding is assessed. Classification capability and performance are assessed as part of the organisation's overall protective security programme.	The classification policy and procedures include: • That information is considered open by default unless there is a compelling reason to withhold it The criteria and conditions for ongoing review of classification levels and protective markings. Outcomes of the reviews are tracked, reported, and used for learning and improvement. Classification practices are regularly reviewed to establish how well it is working for the organisation including: • Review of vulnerability assessments, incidents (including minor breaches), and audit outcomes by internal staff, the Ombudsman, or the Chief Archivist • Assessment of resource effectiveness (including roles, responsibilities, policies, procedures, training programmes and materials). • Based on the organisation's policy, protective marking durations are set to expire for agreed information types. On reaching the date, information is automatically declassified or is reviewed for manual declassification.	
Principle 2: Personal responsibility		
Personnel who work with protectively marked government information take personal responsibility to understand and fulfil the obligations to classify, declassify, and handle government information correctly in line with the organisation's classification policy and legislative, regulatory, and other organisational obligations. Personnel do not use classification to withhold information inappropriately such as to: • Hide violations of law, inefficiency, or administrative error • Prevent embarrassment • Restrain competition • Prevent or delay the release of information that does not need protection in the public interest.	Policies and practice ensure that personnel consider all audiences who could benefit from the information's use and look for ways to reach the widest audience to achieve the greatest benefit. Policies and training ensure that personnel feel confident and are open to challenge and be challenged on classification decisions and security behaviours. There is a culture of no blame that focuses on learning and improving classification and handling decisions.	
Principle 3: Information sharing		
The organisation has identified the stakeholders who could benefit from information sharing and their needs. Organisational policies and procedures reinforce the value of information sharing and outline their information sharing obligations under relevant legislation, regulatory, and partner agreements that enable and hinder information sharing. This includes documented declassification policies, information sharing agreements, and information management policies. Effective and safe information sharing practices are implemented through effective information sharing procedures, training, and systems.	The organisation has identified information-sharing stakeholders within other sectors, international partners, local government, civil defence, hapū, iwi, and/or local communities. The barriers to effective information sharing have been identified (e.g. lack of awareness, misunderstanding, fear of getting it wrong) and programmes are in place to remove those barriers (including training, awareness campaigns, and formal information sharing agreements). The organisation uses available government information sharing instruments that clearly articulate the criteria and rules for sharing between parties.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – INFOSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4** **COULD** statements, recommended for **HIGH** risk and above
Principle 4: Information declassification		
The organisation understands what classified information it holds, how the information is scheduled for release, and the public value the release would hold in compliance with relevant legislation. The organisation has a declassification policy that enables effective declassification decisions including: • Identifying a systematic approach to declassifying government information, and • prohibiting the indefinite classification without transparent criteria. Declassification criteria is defined in the declassification policy. Declassification governance framework is in place that enables effective declassification decisions. Declassification programme is resourced and established in line with the policy and priorities for declassification. Programme results and progress are reported transparently to the governance body and NZ government when requested.	The declassification policy is made available to the public to improve transparency and accountability of declassification decisions. Declassification criteria are integrated within the organisation's classification and information management policies including setting the rules and standards for how classified information will be managed, durations for classification, review cycles, and the process for declassification.	
Classify and assign protective markings		
Government information is classified and protectively marked in line with the Classification System. Government systems and equipment are classified and labelled in line with the NZISM 12.3 Product Classifying and Labelling Standards. When information is derived from protectively-marked sources it is at minimum given the highest classification and protective marking of any of the source material unless the originator agrees it can be changed. Originator control principle is adhered to. No protective marking is changed without the originator approval.		When information is shared with other organisations, those organisations are informed of changes to protective markings.
Protect classified information / Handle government information securely		
Policies, processes, and systems are in place for controlling protectively marked information, media, and equipment in line with Classification System and NZISM including: • Managing and controlling 'accountable material' • Having registration systems for receiving, tracking, and auditing • Undertaking auditing and monitoring • Undertaking spot checks if applicable (TOP SECRET and ACCOUNTABLE MATERIAL at minimum) • Raising audit / spot check discrepancies and signs of tampering as security incidents • Verifying 'Need to know' and access authority • Managing reciprocal protections under bilateral or multilateral agreements and arrangements • Managing OIA requests and how it interacts with protections on protectively-marked information (including foreign government information) • Managing access restrictions for foreign nationals when NZEO or REL endorsements are used • Obtaining NZEO exception waivers when necessary • Authorising and managing transport and removal • Managing security arrangements when people are authorised to work away from the office (including from home, remote sites, and offshore) • Managing waste and destruction (including when using third party contractors) Where relevant and necessary to treat additional risk, policies, processes, and systems are also in place for controlling protectively-marked information, media, and equipment in line with Classification System and NZISM including: • Tracking of received and copied TOP SECRET and ACCOUNTABLE MATERIAL • Using a Classified Document Register for SECRET or below information • Using a receipting process for received protectively-marked materials • Undertaking spot checks for SECRET and other information and assets		

PSR CAPABILITY MATURITY MODEL (PS-CMM) – INFOSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4** **COULD** statements, recommended for **HIGH** risk and above
The organisation has policies that implements secure handling requirements in line with the Classification System (and Classification Quick Guides), PSR Security Zones, and NZISM for each classification on controlling: • Personnel access • Use, copy or share • Remove or transport • Store and file • Archive or disposal. The organisation has clearly registered with the accreditation authority, the highest classification level and accreditation status of all ICT systems which hold or process protectively-marked information. These systems meet NZISM minimum standards Policies, procedures, and monitoring are in place to ensure that information is not copied, transmitted, or stored on devices or systems that it is not authorised for. Information is not stored at higher classifications than the system or device is accredited to hold. The organisation uses approved procedures for destroying ICT media and information with protective markings.	The organisation has implemented security controls for reducing the risks of information compromise when copying, printing, and transmitting protectively-marked information. When information is stored electronically, the classification and protective markings are stored within its metadata. The organisation's classification policies and procedures detail users requirements for recording and filing protectively-marked information into ICT systems that they use.	
INFOSEC 3 Validate your security measures		
INFOSEC 3.1 Ensure appropriate certification and accreditation		
The organisation validates its information security measures to find out if they have been correctly implemented and are fit for purpose. ICT systems are certified and accredited in line with the NZISM to ensure that information is securely stored, transmitted, and used electronically.		
INFOSEC 4 Keep your security up to date		
INFOSEC 4.1 Analyse evolving security vulnerabilities and threats		
The organisation manages information security vulnerabilities by • Monitoring its systems, networks, and processes for security vulnerabilities and security events. • Getting alerted to known security vulnerabilities and flaws in the technical environment • Assessing its security measures against best practice • Documenting, analysing, prioritising, and reporting on vulnerabilities that pose the most immediate risk to the organisation. • Applying identified fixes and tracking them to completion to mitigate the risk of an organisation's information being compromised. The organisation manages threats to information security by: • Undertaking information security threat assessments (capability assessed by GOV 2)	The organisation actively monitors international information security threat catalogues to stay ahead of emerging threats and treatments.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) – INFOSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; recommended for **MODERATE** risk and above	**PS-CMM 4** **COULD** statements, recommended for **HIGH** risk and above
INFOSEC 4.2 Keep information security measures up to date		
The organisation ensures that its security measures are effective to address the risks faced by: • Documenting and maintaining its operating procedures and making them available to all users who need them. • Keeping access control systems up to date as personnel join, change jobs, and leave the organisation, and when access measures are introduced or changed. • Protecting its ICT equipment from malware, including personal devices that have access to an organisation's information. • Applying security patches and updates regularly. • Testing its business continuity and disaster recovery plans and ensuring the organisation is adequately prepared for a significant service interruption, attack, or other serious security incident -*capability assessed by GOV 3*		
INFOSEC 4.3 Respond to information security incidents		
Capability assessed as part of GOV 6.		
INFOSEC 4.4 Review security measures		
The organisation regularly monitors, reviews, and audits the degree to which its information security policies are being implemented and followed. This includes: • use of operational procedures • handling of protectively-marked materials • supply chain and partners services, reports, and records, and • compliance with relevant legislation, requirements, and standards. There are security controls in that limit unauthorised access to information system audit tools to reduce the potential to misuse or compromise. When changes occur in the environment, the organisation identifies how these changes will affect information security and when required restart the information security lifecycle (INFOSEC1).	To minimise the risk of disruption to organisational business processes, the organisation plans, reviews, and agrees suitable monitoring requirements for operational systems.	
INFOSEC 4.5 Retire information securely		
The organisation archives, repurposes, or securely destroys information and supporting ICT systems that are no longer required in compliance with relevant legislation, Classification System, NZISM, and best practice standards.		

PSR CAPABILITY MATURITY MODEL (PS-CMM) - PHYSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PHYSEC 1 Understand what you need to protect		
PHYSEC 1.1 Identify what you need to protect		
There is clear understanding of what the organisation needs to protect (people, information, and assets) including where they are located, their value and sensitivity, and health and safety requirements. There is a clear understanding of how the organisation's facilities and work locations are used, by whom, who visits them, and what is stored in them. Threat assessments are conducted to understand the physical security threats and vulnerabilities that exist and their impacts and consequences.		
PHYSEC 1.2 Assess physical security risks		
The organisation has assessed the physical security risks for each site that it operates in and selected appropriate security measures to address the risks. When selecting new sites, the organisation has a process to evaluate the physical security risks when assessing if the site is suitable. Capability for physical security risk management is also assessed in GOV2.		
PHYSEC 2 Design your security measures		
PHYSEC 2.1 Apply good practices for physical security design		
Physical security measures are designed to address the identified physical security risks and vulnerabilities and in line with its legislative, Government Property Group, and health and safety obligations. Physical security measures are selected and designed early in the process for: • Planning new sites and buildings • Selecting new sites • Planning alterations to existing buildings. The organisation has designed and implemented physical security zones that meet the requirements defined in PSR Security Zone Requirements and NZSIS Technical Notes for Zones 3 and higher. The organisation has designed and implemented security in depth through use of: • a combination of security measures to protect and control access to its people, information, physical assets, and premises • physical security products that provide the right levels of protection (as determined by its risk assessment).	Good practice physical security design practices have been implemented such as 'Deter, Detect, Delay, Respond, Recover' and Crime Prevention Through Environmental Design.	
PHYSEC 2.2 Develop security plans		
Site security plans are in place for all sites and facilities the organisation operates in including both existing and new sites. Site security plans are updated when facilities undergo refurbishment. For facilities under construction, construction security plans are developed, and relevant security measures are included in construction design briefs and requests for tender and contracts. The site security plans address the organisation's specific risks to: • provide enough delay to allow planned security responses to take effect • protect people, information, and assets from threats • complement and support other operational procedures • include any necessary measures to protect audio and visual privacy • do not unreasonably interfere with the public.	Site security plans are comprehensive representing containing detailed information on the risks and measures as identified in site risk assessments.	

PSR CAPABILITY MATURITY MODEL (PS-CMM) - PHYSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PHYSEC 2.3 Implement specific physical security measures		
The organisation uses NZSIS-approved products when they are necessary to meet security zone requirements (Zone 3 and above) and address its risks. The products are verified as being installed and configured in accordance with any conditions of approval. As appropriate, the organisation has implemented relevant site-specific security measures required to address each site's risks (as outlined in the site security plans) in line with PHYSEC Appendix K (Specific Security Measures). As appropriate, the organisation uses best practice physical security measures for the applicable specific scenarios including when working away from the office or hosting secure events. When working with others (including suppliers, co-tenants, and landlords) the organisation understands and agrees shared physical security requirements and builds those into contracts and agreements. (GOV5). Records are maintained throughout the design, build and implementation of physical security to support certification and accreditation.	When implementing physical security measures, the organisation uses relevant standards, handbooks, and codes.	
PHYSEC 3 Validate your security measures		
PHYSEC 3.1 Ensure security zones are certified and accredited		
The organisation ensures that it conducts the appropriate certification and accreditation process required for the type of physical security measures and security zones being implemented. All security zones (Zones 1 to 5) are certified and accredited. If applicable, all security zone 5 areas have been certified by the NZSIS. Zone 5 areas where SCI is handled are certified and accredited by the NZIC. The person certifying a facility or zone (certification authority) sight the required certification documentation and agree that they are satisfied that security measures specified are correctly implemented and tested to confirm that they are working as required to address the identified risks. The person accrediting a facility or zone (accreditation authority) sight the required accreditation documentation, formally endorse its certification, and accept all residual risks. Facilities and security zones are not granted approval to operate unless accreditation has been granted by the accreditation authority.	Based on the organisation's policies and procedures, facilities or zones are recertified and reaccredited periodically based on risk and when threats, vulnerabilities, risks, or security measures change.	
PHYSEC 4 Keep your security up to date		
PHYSEC 4.1 Analyse security vulnerabilities and threats		
The organisation manages physical security threats and vulnerabilities by monitoring its physical security systems, assets, people, and processes for security vulnerabilities, security events, and emerging and evolving threats and vulnerabilities. The organisation applies identified fixes to physical security measures and tracks them to completion to mitigate the risk of the organisation being compromised.	The organisation manages physical security threats and vulnerabilities by getting alerted to known security vulnerabilities and flaws in the physical environment. The organisation assesses its security measures against best practice standards (See PHYSEC Appendix G: Relevant standards for design of physical security measures). The organisation documents, analyses, prioritises, and reports on vulnerabilities that pose the most immediate risk to the organisation, including after a security incident has occurred.	The organisation actively and continually monitors the security environment to stay ahead of emerging threats and treatments.
PHYSEC 4.2 Keep physical security measures up to date		
The organisation ensures that its physical security measures are effective to address the risks faced by documenting, maintaining, and testing its operating procedures and making them available to all users who need them. The organisation maintains its physical access control systems as people (including contractors and suppliers) join, change jobs, and leave the organisation, and when access measures are introduced or changed.	The organisation tests its physical security emergency response procedures to ensure they are fit for purpose and the organisation is adequately prepared for a significant service interruption, attack, or other serious security incident. – *Capability assessed in GOV 6*	

PSR CAPABILITY MATURITY MODEL (PS-CMM) - PHYSEC

PS-CMM 2 **MUST** statements; mandatory for **ALL** risk levels	**PS-CMM 3** **SHOULD** statements; mandatory for **MODERATE** risk and above	**PS-CMM 4 / PS-CMM 5** **COULD** statements, recommended for **HIGH** risk and above
PHYSEC 4.3 Respond to physical security incidents		
Capability for incident management is assessed as part of GOV 6.		
PHYSEC 4.4 Review security measures		
Regular reviews are undertaken of the physical security framework. The frequency of the review is dependent on identified risks associated with the site and documented in the organisation's policies and procedures. There are security controls in place that limit unauthorised access to physical system access control and audit tools to reduce the potential to misuse or compromise.	The organisation regularly monitors, reviews, and audits to know if: • Its physical security policies and procedures are being followed • Its physical security measures are working as planned • Any changes or improvements are necessary. When changes occur in its use of facilities or in the threat environment, the organisation identifies how these changes will affect physical security and when required restart the physical security lifecycle.	
PHYSEC 4.5 Retire securely		
The organisation has a process and procedures for redeploying or destroying of its facilities or assets securely. Capability for securely archiving, repurposing, or disposing of physical information are assessed as part of INFOSEC 4.		