PSR Protective Security Requirements

Capability Maturity Model for Protective Security

newzealand.govt.nz

Contents

About the capability maturity model

The capability maturity model helps you assess your protective security capabilities and identify how you could develop them further.

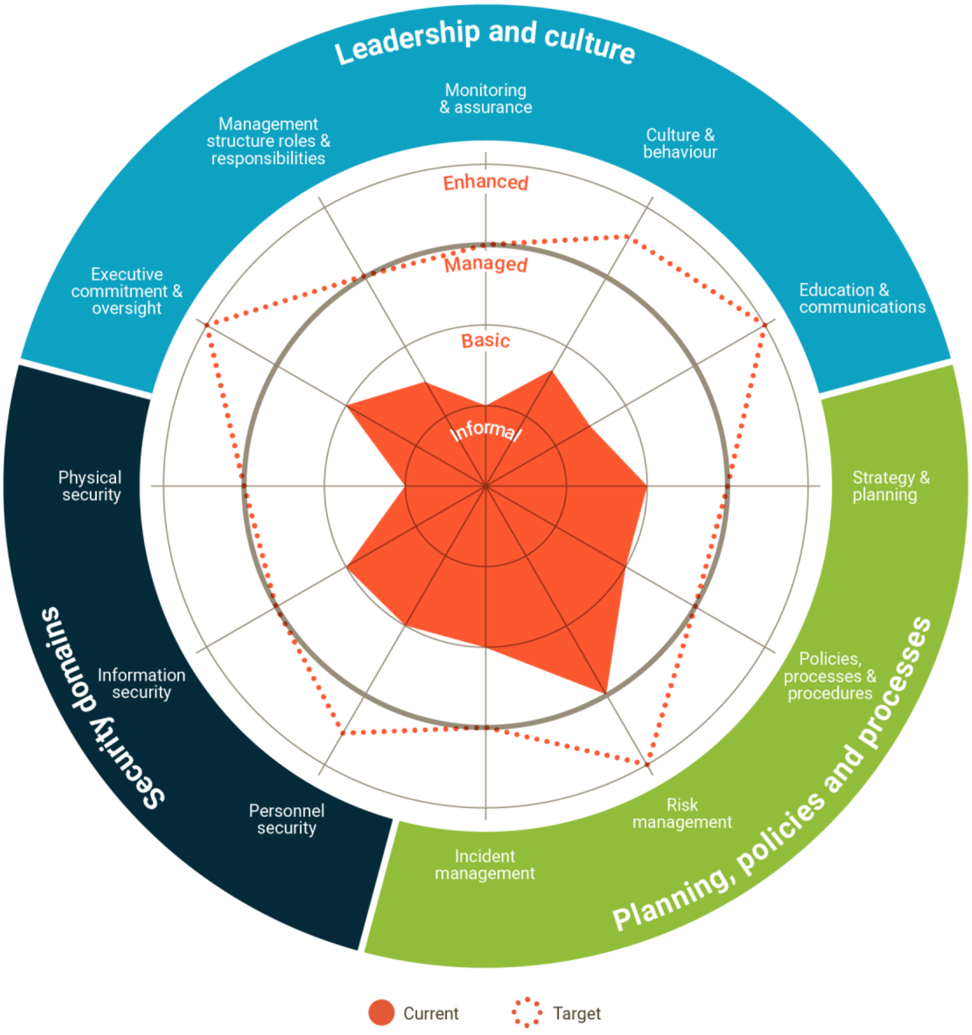
The model recognises each organisation has a unique combination of:

- people, information, and assets it needs to protect
- types and levels of security risks to manage.

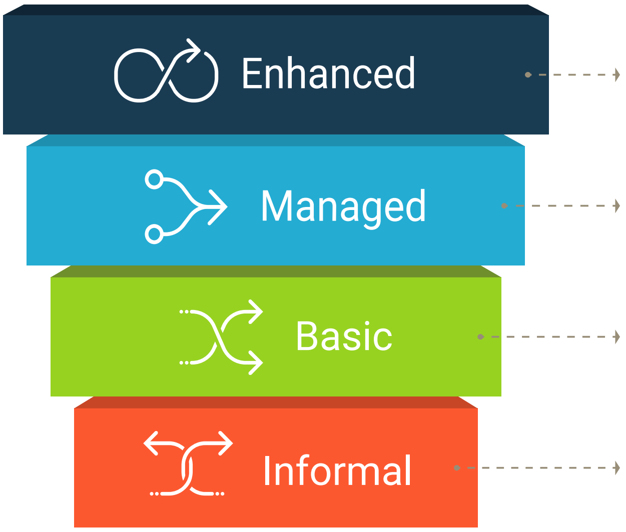
The model assesses capability across 12 dimensions and 4 maturity levels to accommodate a wide range of risks and circumstances. This range includes organisations based across multiple locations and business units within an organisation that have different or unique security risks.

The model is guided by the PSR's mandatory requirements. While the 20 mandatory requirements are 'baseline' objectives, the model helps all types of organisations (organisations facing different types and levels of security risk) to set maturity targets based on their own security risk profile.

One size does *not* fit all.



Security capability maturity levels



Security capability adapts to a dynamic high-risk operating environment. Security posture is in-line with stakeholder expectations.

Risk-based, fit-for-purpose security measures are in place, understood, and consistently followed. Ongoing investment is required to sustain measures at this level.

Foundation policies, capabilities and practice are in place, but are mainly reactive and inconsistent.

Security is ad-hoc, unmanaged, and unpredictable; success relies on individuals rather than processes.

Understand your threats and assess the risks

To assess your maturity, you must understand your operating environment and your risks very well. Deep understanding coupled with a robust risk assessment will help you determine your capabilities and any shortfalls. If you can't conduct a robust risk assessment, seek assistance. Your perception of the operating environment and the risks you face are key to selecting proportionate security measures and preventing potential harm to your organisation and stakeholders.

You must continuously improve your organisation's ability to manage security risks. Ongoing improvement requires a cycle of assessing your risks, managing those risks, and evaluating the effectiveness of your security measures. As you continually re-calibrate and respond to your risk environment, reassess your current maturity level and your maturity targets to ensure they remain proportionate in an ever-changing threat and risk landscape.

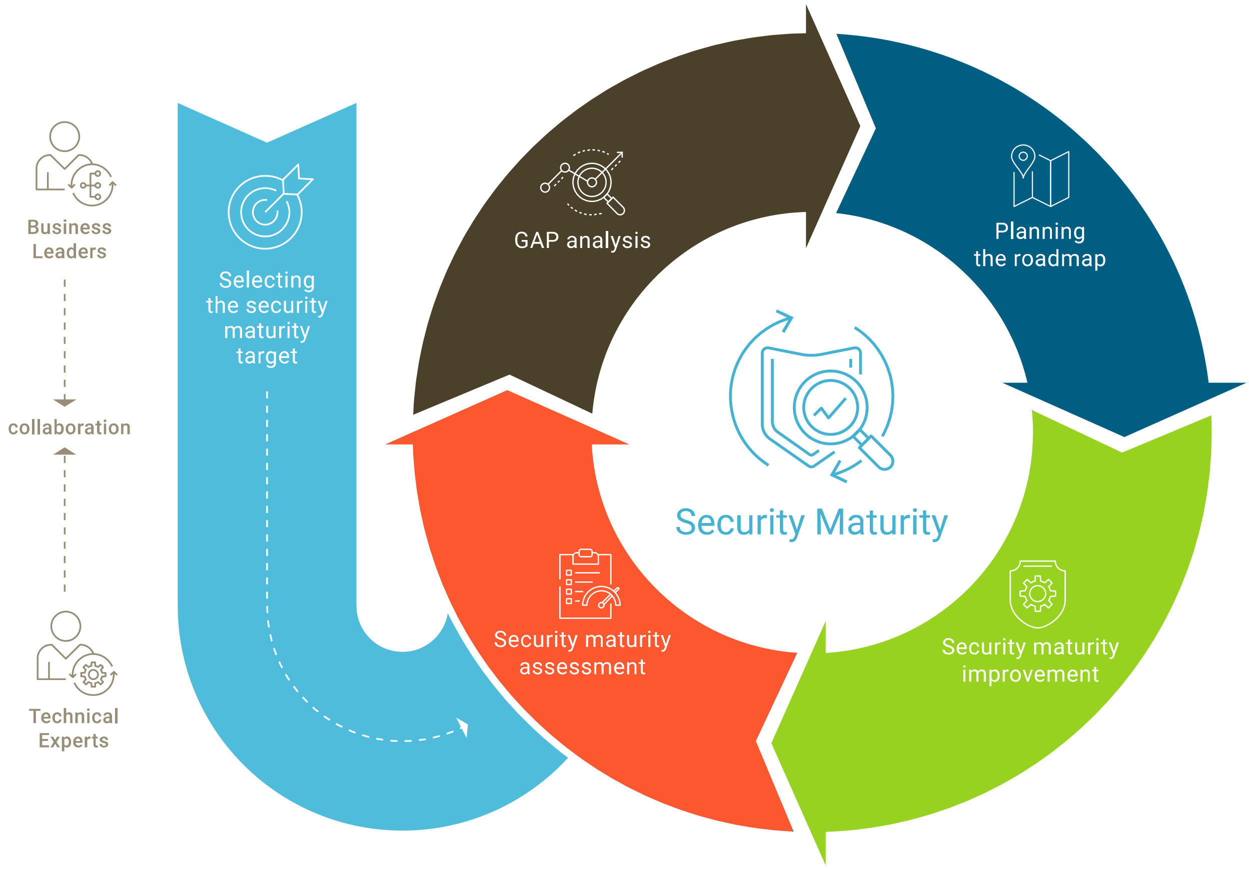
Select the right maturity targets

Your targets must be relevant and stay relevant. Set a target for each of the 12 capability dimensions and determine the level of risk you're willing to accept. This will enable you to make informed decisions on priorities and balance your ability to deliver business objectives with pursuing, achieving, and maintaining the most mature and appropriate security position for your organisation.

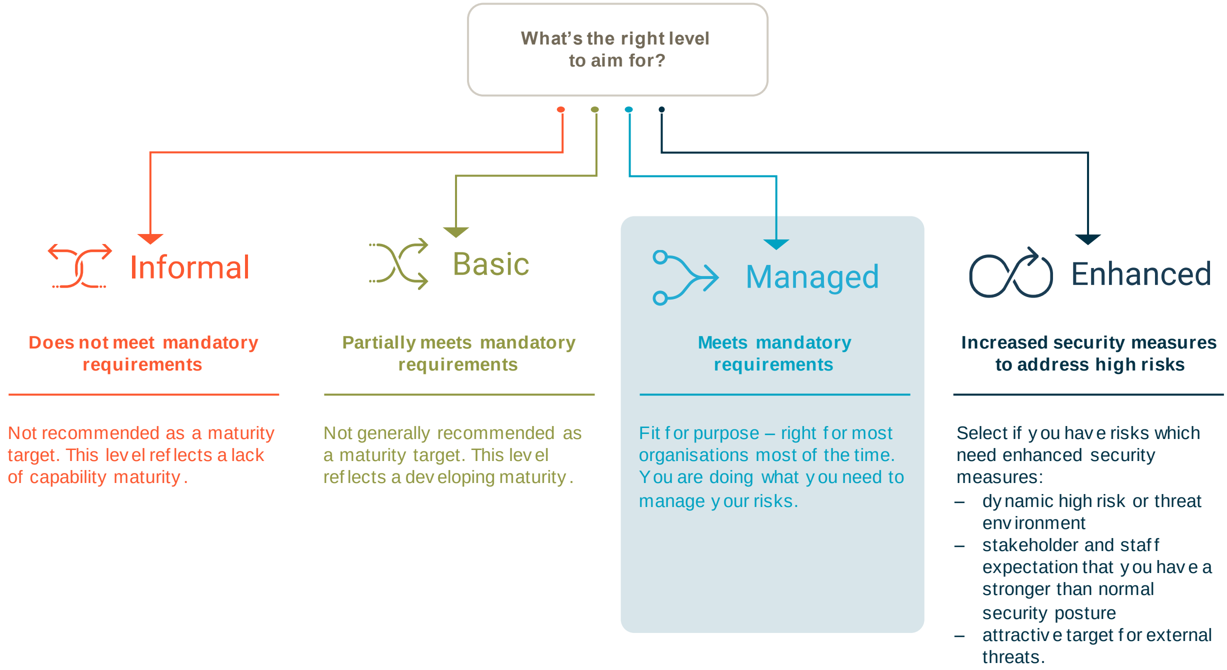
Your targets must be considered and informed by your organisations security context, potential threats, and risk appetite. This approach might drive you to select different maturity targets for different locations, business activities, and dimensions.

Be mindful that broad and disproportionately strong measures are not cost-effective and can impede business functions. For example, different business units might have very different security needs, especially when your organisation's functions are diverse. Other scenarios that might give rise to differing security needs are operating across multiple locations or in higher threat environments. In such cases, you might conduct several assessments and prepare separate capability development plans. If you are then asked to report to Government via the PSR team, you can present one set of weighted averaged results.

Some organisations face ongoing serious threats to people's safety. Their targets for physical security and incident management might need to be higher than for other dimensions.


Business Leaders
collaboration
Technical Experts
Selecting the security maturity target
GAP analysis
Planning the roadmap
Security Maturity
Security maturity assessment
Security maturity improvement

‘Managed’ capability is often the right maturity to aim for. However, work towards the ‘Enhanced’ maturity level in areas you identify as high risk.


What’s the right level to aim for?

Informal

Does not meet mandatory requirements

Not recommended as a maturity target. This level reflects a lack of capability maturity.

Basic

Partially meets mandatory requirements

Not generally recommended as a maturity target. This level reflects a developing maturity.

Managed

Meets mandatory requirements

Fit for purpose – right for most organisations most of the time. You are doing what you need to manage your risks.

Enhanced

Increased security measures to address high risks

Select if you have risks which need enhanced security measures:

- dynamic high risk or threat environment
- stakeholder and staff expectation that you have a stronger than normal security posture
- attractive target for external threats.

Conducting maturity assessments

Use the tables on the following pages to inform and then record your assessments of current capability levels and your targets for the future. You don't need to have all the elements of a lower level in place before you rate your organisation at, or aim for, a higher level.

Using the evidence you've collected about your organisation, you just need to determine which level best represents your organisation's capabilities now, and consider where you need to be in the future.

If your capability sits between levels, you could record granular scores (for example, a '2.5' or 'basic +').

To enable a broad picture of your organisation, you're encouraged to involve people representing different parts, from executives to specialists, in your maturity assessments. Group workshops provide a good forum for identifying, discussing, and balancing needs and priorities.

More information

→ Contact the PSR team at psr@protectivesecurity.govt.nz if you would like more guidance on the capability maturity model.

Capability maturity level descriptions

The following descriptions summarise the 12 dimensions used to assess your capability maturity for protective security. If you find any of the 12 dimensions a bit light, refer to the table below for further guidance.

Enhanced	• Security risks are viewed and managed as strategic organisational challenges • Day-to-day activity adapts in response to changes in the risk and threat environment • You continuously develop the skills of your security people to ensure knowledge remains current and relevant to your needs, and supports role succession • You have mechanisms in place to develop and test security improvements • You set and apply evidence-based measures to ensure performance is assessed objectively	• Tools and technology enable collaboration across your organisation and support process efficiency • An effective continuous improvement programme operates that addresses outcomes, people, processes, information, and toolsets. • Long-term forecasting and planning is well integrated, with business planning cycles to predict and prepare for changes in the security environment and resource needs • Security management information is captured, analysed, enriched, and distributed via enterprise services in real-time when needed
Managed	• You meet all the PSR's mandatory requirements and follow most supporting guidance • Your executive team and relevant governance bodies support security • Effective and robust security governance and management structures are in place • Security is recognised and managed across the organisation at a strategic level. Security leaders are fully empowered to make decisions • People responsible for leading security have the skills and resources they need • You review your risk assessment and risk management processes to see if they will meet future needs • You monitor and adapt to the risk environment in a planned and consistent manner	• Resource allocation is efficient and aligns to strategic priorities and risks • Security policies, standards, and processes are well defined, understood, consistently followed, and produce the outcomes you expect • You monitor, assess, and evaluate security metrics to identify trends and patterns and where improvements should be made • Tools and technologies supporting security management are well managed and fit for purpose • Effective processes ensure performance targets are met and processes are well supported by toolsets • Information from multiple sources informs your decisions and planning. You accurately evaluate the information's relevance and reliability
Basic	• You meet the PSR mandatory requirements in most areas • You recognise the importance of security; key leadership responsibilities are assigned and understood • You understand and occasionally review security risks and requirements • Security policies are in place, though they may not yet be well understood or supported by documented procedures • Good practice is more repeatable than at the informal level, and results are more consistent, at least in some business units	• You plan and operate at least basic protective security measures. However, you plan, apply, and review your practices inconsistently • You manage key security information well (for example, personnel records, risk assessments, policies, audit reports) • Tools and technologies supporting security management may meet basic needs, but are not centrally planned or easily integrated
informal	• You meet the PSR mandatory requirements in some areas • You assign resources to security work reactively, based on who is available rather than on role responsibilities or competency levels • Your understanding of security risks is poor and inconsistent across your organisation • You perform some basic security practices well and usually take corrective action when problems are identified. However, you implement improvements reactively after incidents rather than proactively to prevent incidents	• You rely on the expertise and effort of individuals rather than institutional knowledge and security culture; the loss of key people would significantly impair your security capability and practice • Your security information is held in silos, may be duplicated, and may be in incompatible formats • You lack the tools needed to support security management

Leadership and culture

Executive commitment and oversight

How your executive or board promote security as a business enabler.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced	• Leaders across your organisation drive continuous improvement, including through approving and sustainably resourcing work on innovations and enhancements to solutions and practice	
Managed	• Your executive team and relevant governance bodies receive regular updates on protective security • Governance meetings include discussion of security risks, issues, trends, and the effectiveness of security measures; protective security is a standing agenda item for a governance body overseeing organisational risks • Your executive team and relevant governance bodies receive prompt and proactive reports on security matters • Your executive team members demonstrate and actively promote good security practice	• Each aspect of protective security management is resourced commensurately with your risk profile, and resourcing may include engaging specialist external expertise • Your executive team takes a proactive approach to overseeing and integrating protective security management, including prioritising and driving improvements • Your executive team supports collaboration with other organisations on security matters
Basic	• Your organisation head understands protective security issues and their own leadership responsibilities • Your executive team understands the protective security leadership lifecycle and may discuss security matters, though usually only in response to security incidents • Your executive team is aware of the resources needed to manage protective security effectively; however, additional resources may be needed	• People with day-to-day responsibility for security management can engage with your executive team and relevant governance bodies; however, this engagement generally only occurs when there are specific issues or events that need to be addressed
Informal	• Your executive team has little awareness of, or pays little attention to, protective security risks and management • Leadership commitment to, and involvement with, protective security is not demonstrated or visible to your people • You have no governance body responsible for providing direction on protective security risks	• You have no resources assigned to managing protective security • While you may have some security reporting mechanisms in place, information tends not to reach your executive teams • People with security-related responsibilities have little or no access to your executive team

Management structure, roles, and responsibilities

How you allocate and support human resources to achieve your security objectives.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to**:**

Enhanced	• Your security leaders drive the use of research, environment scans, and long-term planning to ensure priorities and resource levels remain proportionate • Your security leaders have the capacity and authority to commission and deploy protective security initiatives and toolsets as part of an active and agile continuous improvement programme	• Your Chief Security Officer (CSO) ensures your executive leadership team, governance groups, and senior managers take part in regular, structured discussions about protective security matters and responsibilities. Your CSO ensures the action points from their discussions inform priorities, performance measures, and continuous improvement
Managed	• A senior leader has been appointed CSO and is accountable to the organisation head for security management function • A senior leader has been appointed Chief Information Security Officer (CISO) and is responsible for your organisation's information security • Your CSO has the authority to make decisions on security matters, including resourcing security functions • Your CSO actively oversees security risk and performance against the PSR's security lifecycles • Day-to-day management responsibilities have been formally defined and assigned for each aspect of protective security, including for driving understanding of, and compliance with, your policies and processes • Security leaders are known and your people are confident in approaching them if necessary	• Leaders at all levels across your organisation view protective security as an important part of their management responsibilities. Managers most directly responsible for protective security periodically conduct incident drills and discussion-based exercises. The lessons learned are fed back into planning, policy, and process reviews • The delineation between protective security governance and day-to-day management responsibilities is distinct and supports robust assurance processes • Your security leaders directly contribute to broader business risk assessment and change initiatives • People leading change or other initiatives consider potential implications for security and proactively engage with security leaders • Reporting lines and responsibilities are well understood and proportionately resourced
Basic	• A senior leader has been assigned responsibility for protective security management, though in practice that person may have limited involvement • Other security management responsibilities have been assigned, at least for personnel security, information security, and physical security	• You occasionally review protective security leadership responsibilities and reporting lines • While individual managers may effectively oversee security responsibilities within their own business units, you lack central oversight and coordination
Informal	• While people may have an idea of who is responsible for aspects of protective security, day-to-day functional leadership responsibilities have not been formally assigned and you haven't assigned overall responsibility to a senior manager	• You have limited or no defined reporting lines for protective security management, issue resolution, or practice improvement • Security management is insufficiently resourced

Monitoring and assurance

How you provide confidence that your protective security measures are effective, efficient, and proportionate for the risks.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- You have continuous monitoring and spot checks in place to detect and prevent control breakdowns. This monitoring is probably supported by automation, at least in key high-risk areas
- You regularly audit the implementation and effectiveness of security risk measures not subject to continuous monitoring
- As well as supporting scheduled assurance work, performance indicators relating to your most significant security risks are captured and used to inform both continuous improvement and real-time responses
- You periodically report to everyone in your organisation on how well you're meeting your key performance indicators for security, except where there is a compelling reason to restrict access to that information
- A governance or audit committee provides independent oversight of the effectiveness and efficiency of your security programme
- You audit relevant service providers and suppliers for compliance with your security requirements, and they are held accountable for the results

Managed

- You complete an annual re-assessment of your protective security needs and capabilities
- Internal management reporting on security risk and management is to a schedule and level of detail you have determined is right for your organisation.
- Assurance is routinely considered as part of protective security planning, governance, and operational management
- You apply evidence-based performance measures to help track and assess the ongoing success of your security solutions
- Security risk reporting is well integrated into wider management reporting and regularly reviewed by your executive team and relevant governance bodies
- The measures you select for monitoring, and the frequency with which they are evaluated, are set on a case-by-case basis according to agreed criteria
- You set and apply evidence-based performance measures when feasible
- Your measures of security performance are linked to your organisation's business strategy and — as far as possible — are designed to support it
- You periodically commission independent assurance reviews, at least of your solutions for managing your most significant security risks
- The outputs of assurance activity automatically inform changes to your security policies and measures
- Ongoing monitoring includes analysis of whether risk levels have changed, measures are being applied effectively, and risk management improvements are being implemented effectively
- On an ongoing basis, you obtain evidence that demonstrates whether your policies, processes and measures are complied with and effective. This evidence also helps you identify exceptions
- You perform appropriate due diligence checks on external suppliers against the requirements of their contracts

Basic

- You have some confidence you at least partially meet many of the PSR's mandatory requirements
- You have the capability to perform assurance activity effectively; however, this capability is only activated reactively
- A lack of planning may mean you need to reassign responsibilities and re-gather the same information every time assurance work is commissioned
- Performance of your protective security programme is informally monitored
- You obtain, or plan to obtain, evidence that demonstrates whether your policies, processes, and measures are complied with and effective

Informal

- You have no defined structure or monitoring in place for assessing or reassessing your protective security risks, needs, policies, plans, or controls
- You have no structured system for providing assurance regarding security matters
- Protective security is not considered part of your organisation's strategic risk management activity
- You do not audit the effectiveness of security policies, processes, and measures

Culture and behaviours

How your people demonstrate security behaviours and actions.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced	• Leaders at all levels in your organisation work collectively and visibly to identify new ways to improve security practice • Your people are comfortable reporting areas needing improvement and actively engage in enhancing security measures. You may use collaboration tools to support this engagement	• Transparency, accountability, and trust are your cultural norm; issues are aired and resolved promptly, positively, and effectively • You continuously collate security-related information and use it to inform security management planning and the development of education resources
Managed	• You clearly communicate your needs, values, and expectations for protective security • Your people understand and accept their security responsibilities, and those responsibilities are documented • Your executive team and other managers lead by example, actively and visibly demonstrating their commitment to good security practice • You have processes in place to evaluate your people's adherence to expectations • Leadership groups work together to deliver consistent and positive messages about how your organisation views and manages protective security	• Protective security is well integrated into business processes, helping your people to follow good practice by default • You periodically re-assess your organisation's security culture, possibly as part of a broader organisational culture survey • Your people are aware of their responsibility to foster a positive security culture, and have enough information and training to support this culture • The importance of security and developing a strong security culture is substantially recognised by your executive team and other managers. • Your people's behaviour reflects their protective security obligations
Basic	• Your people commonly view security as the responsibility of a few managers and specialists • Your executive team and senior managers recognise the importance of an effective security culture, but are inconsistent in their approaches to developing one • You have some metrics in place to assess your security culture	• You have documented some security principles and expectations in policy; however, they're not reflected in business processes or practice • Behaviours displayed by your people do not reflect your organisations security values
Informal	• Modelling of good security practice by your organisation's leaders is limited or non-existent • Your people are not actively informed, encouraged, or supported to follow good protective security practice	• You do not, or have limited ability to, use metrics to measure security culture • You have no documentation or guidance on why security is important and what it means in practice and principal, for your people or organisation

Education and communications

How you build security knowledge, awareness, skills, and keep your people informed about security.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- Communication on security matters is ongoing and two-way. Tools and processes are in place to ensure feedback is received and understood, and that issues raised by your people are addressed
- Your people and any service providers are actively engaged in improving security education resources, as part of your continuous improvement programme
- Your security training is reviewed to align with best practice and continuously stimulates your people. Training is role-specific
- Learning is shared across your organisation to ensure best practice is consistent

Managed

- You have defined plans for delivering relevant communications on security to all your people and to a schedule that is proportionate to your needs
- Your people receive induction training on your security risks, policies, and processes, and how to access support
- You deliver ongoing security refresher training and people understand they are expected to participate
- Your people undertake security training, with more practical job-based training delivered as needed
- Your people have access to information that addresses safety requirements and procedures, including for emergency situations
- You ensure people holding national security clearances understand their obligations
- Your communication on security matters is regular, informed by the PSR's security lifecycles, and delivered through channels that effectively reach all your people
- You actively monitor education needs and reassess training content to ensure it remains fit for purpose
- You ensure people who work on critical business functions maintain awareness of emerging threats
- You assess your people's understanding of security requirements, and supplement their knowledge when necessary before you give them access to information and assets that require protection
- You track and record participation in security training
- You ensure and confirm service providers receive targeted security training when appropriate, either through requiring it be delivered or delivering it yourself
- Your executive team and security leaders communicate clearly and frequently about your risk environment and security management arrangements
- You have defined values and aspirations for managing security and communicate them in clear terms, so they're consistently understood throughout your organisation

Basic

- You have some systems in place for informing all your people about security matters; however, education is not ongoing
- You generally only detect a lack of understanding of security requirements following an incident
- Communication is primarily one-way and that is top-down
- Some business units deliver training; however, your organisation lacks central planning and oversight for security education
- People responsible for developing communications and training have access to the information they need
- Security management communication systems exist, but they have not been defined

Informal

- You have no structured security training plan or materials; your people may receive information about security expectations informally on the job
- You do not have processes in place for issuing communications on security matters
- You may provide your people with some information about protective security; however, it's generic and doesn't address your organisation's specific needs or priorities
- You have little or no ability to detect gaps in people's understanding of protective security requirements
- Your people have limited or no awareness of the PSR and its relevance to your organisation
- Your business units do not seek expert guidance when they should

Planning, policies, and processes

Strategy and planning

Formulating your security plan and bringing it to life.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced	• Protective security considerations are fully integrated into your business strategy and planning cycles • Business strategies, security plans, and ongoing reviews are well informed by up-to-date, evidence-based data, which you use to analyse threats, understand trends, and conduct forecasting	• Continuous improvement work helps ensure opportunities to enhance security planning are efficiently identified, assessed, and actioned • Your business continuity programme is continually planned and improved. You conduct exercises to ensure you are prepared for disruption. Business continuity is embedded in your culture and practice
Managed	• Your protective security planning comprehensively addresses the protection of people, information and assets; and is well informed by the PSR's security lifecycles and guidance • Your plans demonstrate clear awareness and agreement about acceptable levels of security risk • You review your security plan at least every 2 years to ensure it remains relevant to your risk profile, is sustainable, and informed by any changes in the PSR or related standards • Your executive team and relevant governance bodies regularly review your tolerance for security risk, and may subsequently drive out-of-cycle changes to your security plan • Each area of your organisation is effectively represented when security plans are developed • Your security plan is flexible to accommodate changes in your wider business environment or the results of assurance activity	• Your security planning is well informed by access to historic data. You use root cause analysis to inform solutions to systemic security issues • You track and regularly report to your executive team and relevant governance bodies on progress against your security plan • A business continuity management programme is in place to enable your critical functions to continue to the fullest extent possible during a disruption • You periodically test and review your business continuity programme and other important risk mitigations where it's feasible • Your security plan is communicated and accessible to those who need it • Your plan is used to determine your security objectives and clearly supports your broader organisational goals • You have a plan to increase your security levels at a time of heightened threat
Basic	• You consider your protective security risks and needs when developing strategies and business plans, but you may not be well informed by analysis or recent threat and risk assessments • You have a protective security plan in place that has been approved at an appropriate level of seniority, but this plan may or may not be up to date • Your security planning may effectively mitigate some key risks	• People responsible for security planning are appropriately skilled, but they may not have all the time or support they need to ensure plans are robust • Security planning is not subject to central coordination or guidance, so improvement activity is inconsistently and/or inefficiently applied across your organisation • You have a basic business continuity programme in place • You have an ad-hoc plan to increase your security levels at a time of heightened threat
Informal	• Some security risks and requirements are considered when your organisation's strategies and any business unit plans are developed; however, this practice is neither widespread nor consistent • Your organisation has some understanding of protective security issues; however, you're doing little to discuss or address the issues and you can't be confident you have a good grasp of where you need to focus your attention	• Security planning is ad-hoc. Your security plan is partially developed and implemented but may not be current or comprehensive • Tolerance levels for protective security are not specified • You have no documented business continuity programme in place • You have no plan to increase your security levels at a time of heightened threat

Policies, processes, and procedures

Clearly defining your expectations and approaches for achieving security.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced	• As part of your continuous improvement programme for security, your people and relevant service providers actively contribute to optimising your processes and procedures. You have tools in place that make it easy for them to contribute	• Issues and/or emerging risks relating to contracting and contract management processes are analysed. Mitigation strategies are put in place to improve existing and future contracts
Managed	• You have security policies, processes, and procedures in place that meet your needs for protecting your people, information, and assets • Policy and procedures are easy for people to access and are understood • You review security policies at least every 2 years. You also periodically review processes and procedures to ensure they remain appropriate • Security management processes are embedded, consistently followed, and deliver the outcomes you expect • People coordinating policy development and compliance activity ensure security needs are considered when designing any business processes or systems – it's not just security management people who take responsibility • Your procurement contracts include standard terms and conditions relating to security	• Your policies and procedures include aspects on working with external suppliers where relevant • People from across your organisation contribute to designing your security management policies, processes, and procedures • You proactively scan your environment for relevant changes and emerging threats, amending your security policies, processes, and procedures when appropriate • You set and apply evidence-based performance measures for your security management processes, and performance targets are consistently met • Your security management processes and procedures are supported by automation when that makes them more effective and efficient • You have documented and effective procedures in place to ensure that proposed changes to your processes, or new processes, are assessed for their impact on security management requirements
Basic	• You have elements of protective security policy in place, but they're not yet sufficiently supported by documented processes and procedures • Where security management processes do exist, they usually perform as you expect. However, process discipline may be lax • You occasionally review your security policies, though generally only in response to an incident or prompt	• When applicable, your procurement contracts identify requirements for protecting people, information, and assets • Levels of due diligence on the security policies and measures of external suppliers vary across your organisation • You have a limited or inconsistent process in place for considering how new processes, or changes to existing ones, will affect security management
Informal	• You have no documented protective security management policies, processes, or procedures in place • Undocumented processes tend to change depending on the situation at the time or who is following them; and the purpose and value of these informal processes may be unclear • Protective security needs may be considered when business processes are developed or reviewed, but you can't be confident this happens	• You don't ask external suppliers for information about their security policies and measures before you share sensitive information with them • Security is not considered in procurement decisions or factored into supply contracts for products or services

Risk management

How you identify, assess, and mitigate your potentials risks, opportunities, and adverse effects.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced	• Your people and relevant service providers actively contribute to identifying, managing, and reporting on protective security risks • Well-defined, best-practice, and efficient risk identification and assessment processes are accepted and integrated into business functions across your organisation. These processes cover vulnerabilities and threats	• Security leaders engage continuously with business units to support them in following best practice and improving risk measures • Your business processes are designed to reduce security-related risks with security considerations embedded into change management processes
Managed	• You have fit-for-purpose security risk management measures in place that align to the standards set out in the PSR, and to your organisation's broader risk management approach • You periodically review your protective security risks and threats, including scanning the environment for emerging risks • Protective security risks are overseen and actively managed as part of your strategic or enterprise risk management framework • The most appropriate business units take 'hands on' ownership of individual security risks and issues • Your security leaders coordinate risk management plans and ensure measures are applied consistently across different areas affected by the same types of risks	• Your people understand and accept security risk management is an important part of protecting them and the continuity of your business functions • Your security risk management requirements are effectively, consistently, and verifiably met by your service providers • You are proactive in identifying and assessing protective security risks before issues occur, which your people perceive as adding value • You have requirements in place to consider security risks and issues in the design phase for all processes and systems
Basic	• You have some understanding of the threats, risks, and vulnerabilities that affect the protection you need for your people, information, and assets • You have some security risk mitigations and other measures in place; however, they're not yet comprehensive, well documented, or tracked over time • Your security risk definitions are often generic and not analysed in enough detail to be useful • Your focus is mainly on mitigating a few high profile security risks	• There is at least some relationship between your protective security functions and wider risk management functions • You occasionally update your risk assessments, but this may be viewed as simply a compliance requirement • You consider security risks and issues when designing and redesigning key business processes and systems; however, it's not compulsory
Informal	• You have no structured or consistent mechanisms in place for identifying, assessing, monitoring, or reporting on protective security threats and risks, so you can't be confident you understand them • You have no planned measures in place to mitigate protective security risks • Your people's awareness of protective security threats and risks is generally poor	• Protective security functions are neither linked to, nor integrated with, your organisation's overall risk management framework • You have no processes for ensuring your security risks and issues are considered when designing or reviewing processes

Incident management

Expecting the unexpected and being ready to manage it.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- All significant security incidents are verifiably managed in full accordance with your emergency or crisis management approach
- Security investigations are subject to independent or at least semi-independent review. All investigations into significant incidents are reviewed
- You conduct ongoing research into measures for preventing and managing incidents as part of your continuous improvement programme for processes and systems, which includes engaging with external experts
- Internal and external security environments are monitored for issues affecting the appropriate response to an incident. Improvements to processes are made as a result

Managed

- Mechanisms are in place for recording, responding to, escalating, and evaluating security incidents. These mechanisms are communicated well and consequences are clearly defined
- Your people and relevant service providers understand what a security incident is, how to respond, and who to inform
- You are confident that, when it's appropriate based on the nature of an incident, the correct external agencies will be contacted in a timely fashion
- You have a comprehensive, consistent, and responsive approach to incident management across your organisation; a well-defined hierarchy of response and escalation triggers exists
- Security incidents and suspicious activities are consistently well recorded, tracked, and investigated
- You perform root cause and trend analyses to inform practice improvements
- You periodically conduct incident drills and exercises with your people to improve responses, and feed what you learn into policy and process reviews
- Incident management is clearly and effectively integrated with your business continuity programme and your health and safety regime
- Your incident management system integrates business continuity, health and safety, and security
- You have specified your security requirements clearly to external suppliers
- Reported incidents are subject to a post-incident review to assess the incident response. Any resulting improvements are implemented in a timely manner
- Your executive team and management receive information on security incidents, the measures taken to remedy them, and action taken
- You are confident security incidents are reported and that all reported incidents are managed appropriately
- Your people are encouraged to report security incidents, and are comfortable doing so; incidents are acted on and not simply dismissed
- Information about significant security incidents are communicated to your people
- You clearly communicate to your people the consequences of serious incidents, particularly where there has been a conscious choice to bypass your security policies

Basic

- Your incident management measures to monitor, detect, respond to, and manage security incidents are loosely defined, with limited central oversight, control, or tracking
- Your people have limited awareness of the nature and types of security incidents, and how likely they are to occur
- Your people understand what to do in the case of an emergency, such as a bomb threat or 'white powder' incident
- Your people are encouraged to report security incidents; however, their level of comfort in doing so varies by group or location

Informal

- You have no structured or consistent approach in place for detecting, responding to, and managing security incidents, and you have little support from security specialists
- You haven't defined or communicated expectations for reporting security incidents
- Security incident management responsibilities are unclear; your response to an incident might be delayed while responsibilities are defined and assigned
- Security infringements and incidents are generally ignored

Personnel security

Knowing who you have working for you and ensuring they are, and remain, suitable.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- Any change that could lead to responsibilities being reallocated within your organisation automatically includes an assessment of the implications for personnel security
- You actively explore opportunities to enhance personnel security as part of your continuous improvement programme for security
- When you sponsor the vetting and national security clearances of people employed by third parties, you periodically perform spot audits to ensure pre-vetting employment checks have been completed, ongoing management occurs, and appropriate records are maintained. You also ensure contract terms allow for such audits to take place

Managed

- You have robust pre-employment practices that are based on the risk of the role and are consistently applied
- Effective, ongoing mechanisms are in place for assessing and managing your people and external suppliers
- When people cease working for you or change roles, their physical and systems access privileges are revoked. They understand any ongoing security obligations
- The way you manage positions requiring a national security clearance is consistent with the PSR
- Your people understand how security expectations apply to them, including the standards they must meet and the rules they must follow
- Your people actively contribute to the wellbeing of their colleagues, and to effectively detecting, reporting, and managing concerning behaviour
- You have mechanisms in place throughout the personnel security lifecycle to manage people in higher-risk positions or vulnerable situations
- You ensure your personnel security measures are consistent with your risk profile and changes are communicated promptly

Basic

- You have pockets of good personnel security practice; however, wider awareness is limited and measures are not consistently followed
- Pre-employment screening practices are in place and security vetting requirements (where relevant) mostly followed
- You have some mechanisms in place to assess and manage the ongoing suitability of your people and external suppliers
- People most directly responsible for personnel security understand the personnel security management cycle
- When people require access to classified information or resources, you ensure they first gain a national security clearance. However, you have no ongoing arrangements in place to manage clearances
- Information of security concern that could affect the ongoing suitability of personnel is sometimes shared with your security people. However, this practice is not widespread and measures for preventing personnel risks are not consistently followed

Informal

- You don't proactively assess what your organisation most needs to protect it from insider threats or consider how an insider might breach security
- Your people are generally dismissive of personnel security risks and awareness of your security expectations is poor
- You don't usually perform any identity or background checks before hiring new people
- Your measures for ensuring only appropriately authorised people can access your facilities, information, and other assets are limited and/or inconsistent
- You can't be confident that you would detect an insider breaching protocols
- You have no processes in place for managing national security clearances, and no central register of clearance holders
- You don't effectively manage the ongoing suitability of your people

Information security

Showing critical awareness on how to protect information in all its forms.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- You actively explore opportunities to enhance information security as part of your continuous improvement programme for security
- Information security measures are responsive, adaptable, efficient, robust, and benefit from strategic intent

Managed

- You have mechanisms in place to assess and manage requirements for protecting, sharing, and assuring information. These mechanisms are well understood and updated as required
- You have proportionate measures in place to prevent, detect, and respond to unauthorised or inappropriate access to information and ICT systems, including during systems development and throughout the information lifecycle
- You observe the certification and accreditation process for new and existing ICT systems
- You appropriately archive or otherwise dispose of information holdings when they are no longer required
- Mobile devices and remote working solutions are managed securely
- Information or other assets you hold are consistently classified, marked, accessed, and handled in line with the New Zealand Government Security Classification System
- Your systems ensure access controls are updated when your people change roles or leave your organisation
- You ensure changes made to information management measures are consistent with your security risk profile and wider protective security policies. Changes are promptly communicated
- You periodically conduct both scheduled and unannounced tests and audits of information security
- Information security measures account for privacy obligations, applicable international standards, data sovereignty, and jurisdictional considerations
- When appropriate, your access controls enforce segregation of duties to reduce opportunities for unauthorised or unintentional access to, or misuse of, information assets
- Your information security measures are appropriate to mitigate known cyber intrusions and emerging threats
- Performance monitoring is appropriately applied to all information security measures
- You have a clear understanding of where and how information and data assets are shared with service providers

Basic

- People most directly responsible for protective security understand the information security lifecycle
- You have a certification and accreditation programme in place for new and existing ICT systems; however, it is inconsistently followed
- You have simple information security measures in place for areas holding physical records, ICT equipment, and basic ICT system access controls
- You understand emerging cyber intrusions and threats and have put in place simple information security measures to mitigate targeted cyber intrusions
- You have pockets of good information security awareness and practice, but standards aren't applied consistently across your information holdings and your overall compliance is not well understood. This may be particularly true when your information is held or managed by external suppliers
- You have some security mechanisms in place for ICT systems development
- You have limited understanding of where and how information or data assets are shared with service providers

Informal

- You have limited understanding of your information assets and don't proactively assess the information assets you most need to protect
- You have limited information security measures in place to protect your information assets and ICT system development
- You do not have a certification and accreditation programme in place for new or existing ICT systems
- You can't be confident you would detect unauthorised access to, or the compromise of, electronic or physical information holdings
- You don't usually assess whether information or other assets require a national security classification. You also can't be confident that classified resources are managed correctly
- You can't be confident you implement measures for information assets that are proportional to their value, importance, and sensitivity
- You have limited information security measures in place for targeted cyber intrusions, and have a reactive approach to emerging cyber intrusions and threats
- You do not understand where and how your information or data assets are shared with service providers

Physical security

Providing a safe and secure physical environment for your people, information, and assets.

Choose the level which ***best*** represents your organisation. Indicators of maturity may include, but are not limited to:

Enhanced

- You actively explore opportunities to enhance physical security as part of your continuous improvement programme
- You have mechanisms in place to continuously detect and monitor irregular access and controls
- You constantly monitor the performance of physical security measures and regularly conduct audit checks. Your people appreciate the importance of these measures and checks, and accept the consequences of significant or repeated incidents

Managed

- You have effective mechanisms in place for protecting people (including customers and members of the public when relevant), information, and assets. These mechanisms are well understood and updated as required
- You ensure physical security and safety needs are actively considered from the early stages of any plans for relocating, constructing, or refurbishing premises. You comply with relevant security zone design, certification, and accreditation requirements
- You have proportionate measures in place to monitor access to facilities and to deter, detect, delay, respond to, and recover from any attempts to attack or remove (without authorisation) your physical assets and information holdings
- You appropriately destroy or otherwise dispose of assets when they are no longer required, including information that has been held or processed on ICT equipment
- Your physical security measures extend to protecting people and assets for which you are responsible, but are not located on your premises
- Your people are encouraged and supported to report concerns about physical safety and security, and actively contribute to designing improvements
- Any changes made to physical security measures are consistent with your risk profile and wider protective security policies, and are promptly communicated
- You have systems in place to deter, detect, delay, respond to, and recover from incidents
- You have measures in place for managing the security of special events, such as conferences, including those held away from your facilities
- If your organisation co-locates with, or sub-leases from, another organisation, you have joint arrangements in place to periodically review physical security measures
- Your physical security measures adapt in response to emergencies, and your people understand their responsibilities in such situations

Basic

- People most directly responsible for protective security understand the physical security lifecycle
- Physical security is acknowledged as forming part of your health and safety responsibilities
- You have pockets of good physical security awareness and practice, but standards are not consistently followed and your overall compliance is not well understood
- You have some physical security measures in place that minimise the risk of resources being made inoperable or inaccessible, or being accessed or removed without proper authorisation
- In most cases, you consider physical security when planning, selecting, designing, and modifying facilities and physical security requirements are integrated into your facilities

Informal

- You don’t proactively assess the physical security threats and risks your organisation faces, or what it is you most need to protect
- Your people’s awareness of physical security risks and expectations is generally poor
- You can’t be confident you would promptly detect unauthorised access to your facilities
- You can’t be confident you would promptly detect an attempt to steal or attack your physical assets or information holdings
- You can’t be confident your physical security measures minimise or remove the risk of harm to your people, information, and assets
- You don’t consider physical security in the early stages of planning, selecting, designing, and modifying your facilities
- You have simple physical security measures in place to detect suspicious activity and monitor your facilities, but these measures are inconsistent across your organisation