



Protecting our people, information, and assets

What you need to know

PSR

Protective Security
Requirements

The government's expectations for managing personnel, information, and physical security

Public and private sector organisations are targeted by people and groups intent on doing harm. These are real threats that need to be managed.

Security incidents erode the trust and confidence New Zealanders have in both public and private sector organisations.

Protective security is the responsibility of all people working for your organisation, including employees, contractors, and service providers. To successfully manage security risks, you must ensure security is part of your organisational culture, practices, and operational plans.

New Zealand's Protective Security Requirements (PSR)

The PSR outlines the government's expectations for security governance and for personnel, information, and physical security.

Effective security enables New Zealand Government organisations to work together securely in an environment of trust and confidence.

Protecting your people, information, and assets helps your organisation to meet its strategic and operational objectives.

The PSR: A policy framework for security

The PSR sets out what your organisation must do to manage security effectively. It also contains best-practice guidance you should consider following.

As no two organisations are the same, the PSR follows a risk-based approach designed for flexible implementation.

Implementing the PSR will help your organisation to protect its people, information, and assets. This will ensure:

- your people know they are safe when doing their jobs
- your customers feel safe when visiting your sites
- government is assured your people, information, and assets are protected
- you have confidence that the people you employ are trustworthy
- you better manage business risks
- continuity of service delivery is assured.

Mandatory requirements

Government organisations are expected to adopt the PSR and meet the 20 mandatory requirements.

If you're in the private sector, you should consider adopting the mandatory requirements as best practice.

The PSR provides you with management protocols, lifecycle models, and guidance on how to meet the mandatory requirements.

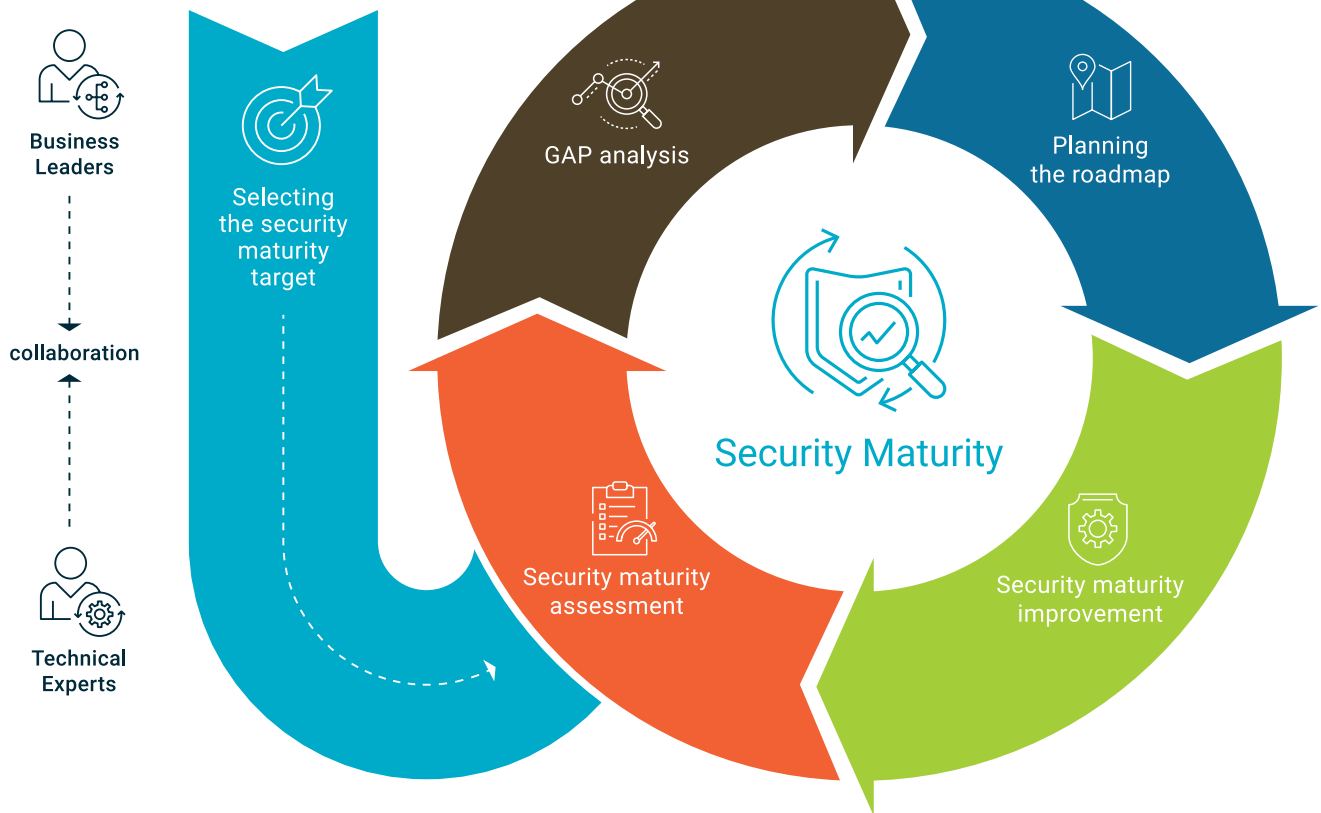


Improving your protective security

Ongoing improvement requires a cycle of assessing and managing your risks, and evaluating the effectiveness of your security measures. As you re-calibrate and respond to your risk environment, you will need to reassess your security measures to ensure they remain appropriate in an ever-changing threat and risk landscape.

The PSR has a capability maturity model that enables you to:

- understand and select security maturity targets
- assess your current protective security capabilities
- identify security areas you need to focus on more
- make security decisions and allocate resources for protecting your people, information, and assets
- form the basis of your security plan and roadmap
- assure stakeholders you are progressing towards your security maturity targets.



Mandatory Requirements

Security Governance

GOV 1

Establish and maintain the right governance

Establish and maintain a governance structure that ensures the successful leadership and oversight of protective security risk.

Appoint members of the senior team as:

- Chief Security Officer (CSO), responsible for your organisation's overall protective security policy and oversight of protective security practices.
- Chief Information Security Officer (CISO), responsible for your organisation's information security.

GOV 2

Take a risk-based approach

Adopt a risk-management approach that covers every area of protective security across your organisation, in accordance with the New Zealand Standard ISO 31000:2018 Risk management –Guidelines.

Develop and maintain security policies and plans that meet your organisation's specific business needs. Make sure you address security requirements in all areas: governance, information, personnel, and physical.

GOV 3

Prepare for business continuity

Maintain a business continuity management programme, so that your organisation's critical functions can continue to the fullest extent possible during a disruption. Ensure you plan for continuity of the resources that support your critical functions.

GOV 4

Build security awareness

Provide regular information, security awareness training, and support for everyone in your organisation, so they can meet the Protective Security Requirements and uphold your organisation's security policies.

GOV 5

Manage risks when working with others

Identify and manage the risks to your people, information, and assets before you begin working with others who may become part of your supply chain.

GOV 6

Manage security incidents

Make sure every security incident is identified, reported, responded to, investigated, and recovered from as quickly as possible. Ensure any appropriate corrective action is taken.

GOV 7

Be able to respond to increased threat levels

Develop plans and be prepared to implement heightened security levels in emergencies or situations where there is an increased threat to your people, information, or assets.

GOV 8

Assess your capability

Use an annual evidence-based assessment process to provide assurance that your organisation's security capability is fit for purpose. Provide an assurance report to Government through the Protective Security Requirements team if requested.

Review your policies and plans every 2 years, or sooner if changes in the threat or operating environment make it necessary.

Personnel Security

PERSEC 1

Recruit the right person

Ensure that all people working for your organisation (employees, contractors, and temporary staff) who access New Zealand Government information and assets:

- have had their identity established
- have the right to work in New Zealand
- are suitable for having access
- agree to comply with government policies, standards, protocols, and requirements that safeguard people, information, and assets from harm.

PERSEC 2

Ensure their ongoing suitability

Ensure the ongoing suitability of all people working for your organisation. This responsibility includes addressing any concerns that may affect the person's suitability for continued access to government information and assets.

PERSEC 3

Manage their departure

Manage people's departure to limit any risk to people, information and assets arising from people leaving your organisation. This responsibility includes ensuring that any access rights, security passes, and assets are returned, and that people understand their ongoing obligations.

PERSEC 4

Manage national security clearances

Ensure people have the appropriate level of national security clearance before they are granted access to CONFIDENTIAL, SECRET, and TOP SECRET information, assets or work locations.

Manage the ongoing suitability of all national security clearance holders to hold a clearance and notify NZSIS of any changes regarding their clearance.

Information Security

INFOSEC 1

Understand what you need to protect

Identify the information and ICT systems that your organisation manages. Assess the security risks (threats and vulnerabilities) and the business impact of any security breaches.

INFOSEC 2

Design your information security

Consider information security early in the process of planning, selection, and design.

Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with:

- the New Zealand Government Security Classification System
- the New Zealand Information Security Manual
- any privacy, legal, and regulatory obligations that you operate under.

Adopt an information security management framework that is appropriate to your risks.

INFOSEC 3

Validate your security measures

Confirm that your information security measures have been correctly implemented and are fit for purpose.

Complete the certification and accreditation process to ensure your ICT systems have approval to operate.

INFOSEC 4

Keep your security up to date

Ensure that your information security remains fit for purpose by:

- monitoring for security events and responding to them
- keeping up to date with evolving threats and vulnerabilities
- maintaining appropriate access to your information.

Physical Security

PHYSEC 1

Understand what you need to protect

Identify the people, information, and assets that your organisation needs to protect, and where they are. Assess the security risks (threats and vulnerabilities) and the business impact of loss or harm to people, information, or assets. Use your understanding to:

- protect your people from threats of violence, and support them if they experience a harmful event
- protect members of the public who interact with your organisation
- put physical security measures in place to minimise or remove risks to your information assets.

PHYSEC 2

Design your physical security

Consider physical security early in the process of planning, selecting, designing, and modifying facilities.

Design security measures that address the risks your organisation faces and are consistent with your risk appetite. Your security measures must be in line with relevant health and safety obligations.

PHYSEC 3

Validate your security measures

Confirm that your physical security measures have been correctly implemented and are fit for purpose.

Complete the certification and accreditation process to ensure that security zones have approval to operate.

PHYSEC 4

Keep your security up to date


Ensure that you keep up to date with evolving threats and vulnerabilities, and respond appropriately.

Ensure that your physical security measures are maintained effectively so they remain fit for purpose.

Assessing your security maturity using the capability maturity model

Example of a self-assessment showing current capability and security maturity targets.





Get security support

The New Zealand Intelligence Community can help you to develop a positive security culture through their active outreach programme and resources available online.

Contact the PSR team

psr@protectivesecurity.govt.nz
+64 4 472 6170

View resources

www.protectivesecurity.govt.nz
www.nzic.govt.nz

New Zealand Government