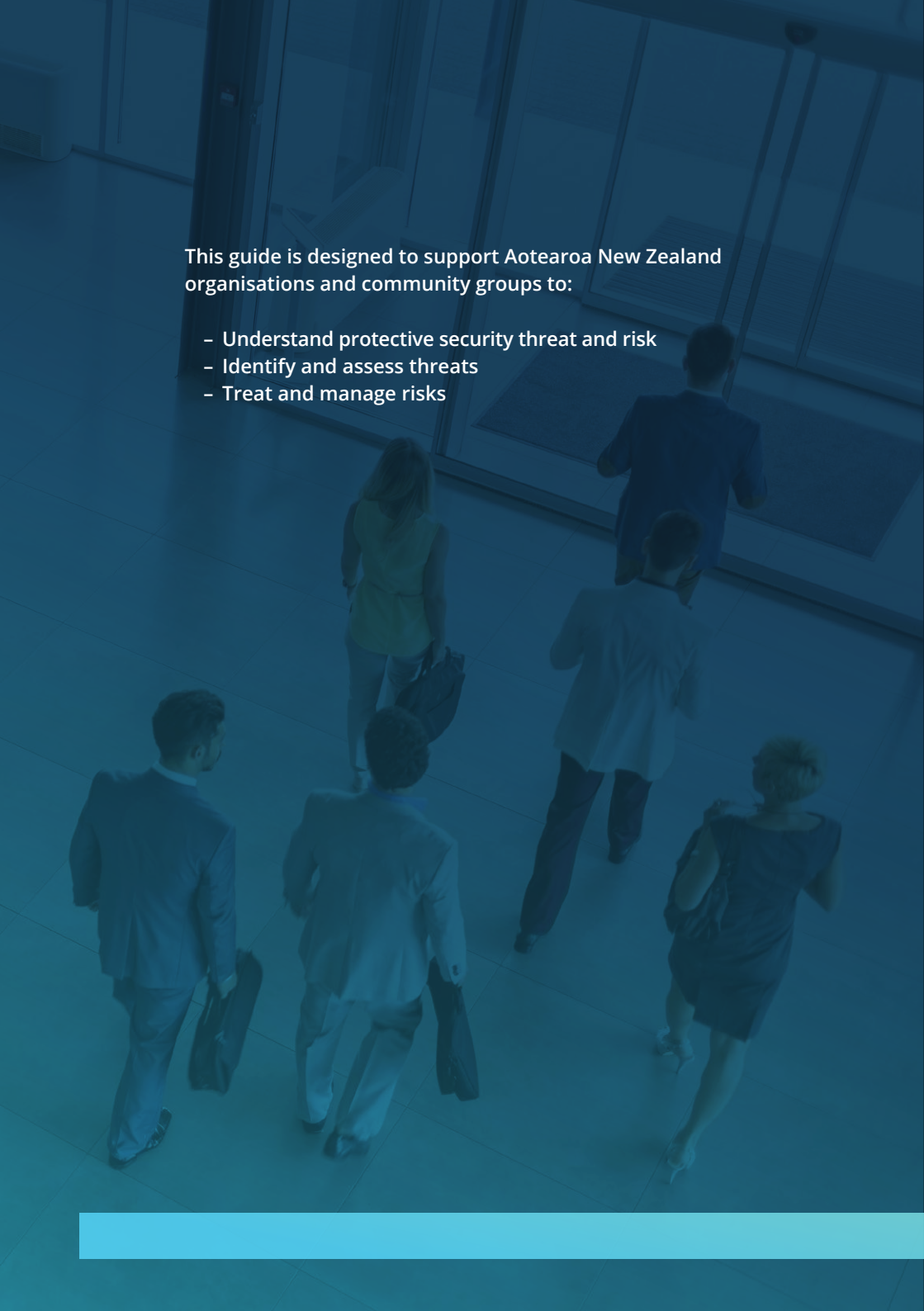
Protective Security Threat and Risk Guidance

PSR | Protective Security Requirements

Te Kāwanatanga o Aotearoa
New Zealand Government



This guide is designed to support Aotearoa New Zealand organisations and community groups to:

- Understand protective security threat and risk
- Identify and assess threats
- Treat and manage risks

Contents

Why is this important?

Good threat identification and security risk management protect an organisation's people, information & assets.

They also enhance an organisation's reputation and effectiveness. This is true whether your organisation is a central or local government agency, a commercial enterprise, a research institute, an iwi entity, or a volunteer community group.

The threats an organisation faces are real and need to be managed. If left unmanaged they can:

- lead to a loss of information or assets
- degrade an ability to operate
- erode the trust and confidence New Zealanders have in both public and private sector organisations
- increase the likelihood of misuse or mishandling of an organisation's information or assets (either wittingly or unwittingly).[1]

1. This guide utilises language and concepts from the following sources: ISO 31000:2018 Risk Management – Guidelines, AS/NZS Handbook 167:2006 – Security risk management, and Security Risk Management – Body of Knowledge (Julian Talbot and Miles Jakeman, 2009).

What are security threats?

Security threats are sources of potential harm or disruption and can be a source of a risk.

Threats can be from natural or human-made sources. The following lists detail some of the common threats for New Zealand agencies, organisations and groups. Because of individual circumstances and the dynamic environment in which we live, this list is a prompt and should not be considered exhaustive or complete.

Natural threats could include:

- Cyclone
- Drought
- Heavy rain
- Flood
- Tsunami
- Snow
- Earthquake
- Epidemic

Human-made threats could include:

- Foreign interference
- Espionage
- Criminal behaviour (theft, burglary, terrorism etc.)
- Insider threats
- Threatening behaviour/violence
- Cyber-criminal attack
- Privacy breach
- Compromise of sensitive information

What are security risks?

The International Organization for Standardization's ISO 31000 defines risk as: The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood.

Security risks are identified threats that have been assessed for their **likelihood** of the threat event occurring and **impact** to the organisation and/or third parties should the threat emerge.

Risks are multi-dimensional and include such things as operating, financial, legal, and health and safety risks. Security risk is another dimension of an organisation's overall risk exposure.

Considerations for conducting security threat and risk assessments

Many organisations have an **enterprise risk management** approach to manage risks across their business.

Enterprise risk management generally includes defined functions that provide governance and oversight of risk management; consequently, senior leaders need to be familiar with key principles of risk management and protective security to guide their strategic decision-making.

Effective risk management enables senior leaders to understand the implications of the uncertainties they face so they can prioritise and make informed decisions on how to effectively use their finite resources to manage their risks.

These key steps are involved in undertaking threat and risk assessments as part of overall security risk management.

The threat assessment needs to be undertaken before the risk assessment.

This guide provides an example approach of how to conduct simple security threat and risk assessments. This approach is aligned to the New Zealand Government's Protective Security Requirements (PSR) framework.

Step 01

Identify what to protect

Identify what needs to be protected to deliver organisational or business outcomes.

What needs to be protected can be described in several ways to suit different organisations.

Examples include:

- **Personnel** – employees/contractors/ suppliers/volunteers/other building tenants
- **Physical** – property/buildings/vehicles/ temporary premises/home offices
- **Information** – data (raw and processed)/ customer records/personal information/ classified material/ICT systems

Step 02

Identify the threats

Think about what could harm or disrupt what needs to be protected. Obtain information about potential threats using internal and external information sources such as those below. Focus on the identification of credible threats.

Internal:

- Surveying staff and interviewing management
- Reviewing internal notifications and reporting
- Physical spot checks and inspections
- Examining previous security incidents
- Consulting security expertise and monitoring international emerging threats and trends
- Identifying specific targets of interest

External:

- Threats identified and reported by similar organisations e.g. other public service agencies
- NZ Police statistics public reporting
- New Zealand Security Intelligence Service (NZSIS) public reporting of the New Zealand national terrorism threat level and threat environment
- Advisories and guidance issued by Protective Security Requirements (PSR) and National Cyber Security Centre (NCSC)
- Media and academic articles

Here is a list of common threats an example organisation may face:

Vector	Group	Subgroup	Threat
People	Employees	Office workers	Intimidating or threatening language or behaviour by a member of public
			Assault / serious harm by a member of public
Physical	Offices	Public and work areas	Vandalism
			Protests
	Offices Remote working	Physical assets e.g. computers and physical files	Theft of agency equipment or information
Information	IT systems	Customer data-base and case management system	Cyber-attack on IT systems
			Privacy breach
	Information Management	Document management system	Inappropriate access and unauthorised disclosure by a trusted insider
	IT systems	Claimant payment systems	Denial of service attack preventing payments and/or corruption of data

Step 03

Assess the likelihood of the threat occurring

Likelihood is assessed using the information available and requires a level of objective and subjective assessment. It should be applied to credible threats and is best conducted in collaboration with others to test the assessment.

For human-made threats, consider:

- Does the threat actor have the **knowledge** of your people, information, assets, security measures, vulnerabilities or have the ability to obtain the knowledge?
- Do they have the **resources** and means to undertake an attack?
- Do they have the **opportunity, determination, and intent** to undertake an attack? What level of intelligence do you have that an attack is possible?
- What is the **likelihood** based on the above?

The below table provides an example of descriptors for different considerations of likelihood:

Likelihood	Descriptors
Almost Certain	Expected to occur, almost inevitable
Likely	Expected to occur in most circumstances
Possible	Might occur at some stage
Unlikely	Not expected but could occur in some circumstances
Rare	May occur but only in exceptional circumstances

Taking our example organisation, here is how likelihood could be applied to the threats it previously identified:

Vector	Group	Subgroup	Threat	Likelihood
People	Employees	Office workers	Intimidating or threatening language or behaviour by a member of public	Almost certain
		Office workers	Minor assault by a member of public	Likely
Physical	Head office	Public and work areas	Minor vandalism	Possible
		Physical assets e.g. computers and physical files	Theft of office equipment	Likely
Information	IT systems	Customer database and case management system	Cyber-attack on ITC systems	Possible
	Official information	Document management system	Inappropriate access and unauthorised disclosure by a trusted insider	Likely
	IT systems	Claimant payment systems	Denial of service attack preventing payments	Possible

Step 04

Assess the consequence

Use Business Impact Levels (BILs) to assess the potential consequence of threats. BILs are available on the PSR website and should be utilised by New Zealand government agencies.

These BILs may also be used and adapted by other organisations, entities and groups to consider specific organisational requirements.

A six-level scale is used:

Taking our example organisation, the following table illustrates the application of BILs to the existing assessment:

Vector	Group	Subgroup	Threat	Likelihood	Business Impact Level
People	Employees	Office workers	Intimidating or threatening language or behaviour	Almost certain	Medium
		Office workers	Minor Assault	Likely	Medium
Physical	Head office	Public and work areas	Minor vandalism	Possible	Low
		Physical assets e.g. computers and physical files	Theft of office equipment	Likely	Medium
Information	IT systems	Customer database and case management system	Cyber-attack on IT systems	Possible	Very high
	Official information	Document management system	Inappropriate access and unauthorised disclosure by a trusted insider	Likely	High
	IT systems	Claimant payment systems	Denial of service attack preventing payments	Possible	Medium

Step 05

Determine the inherent risk rating

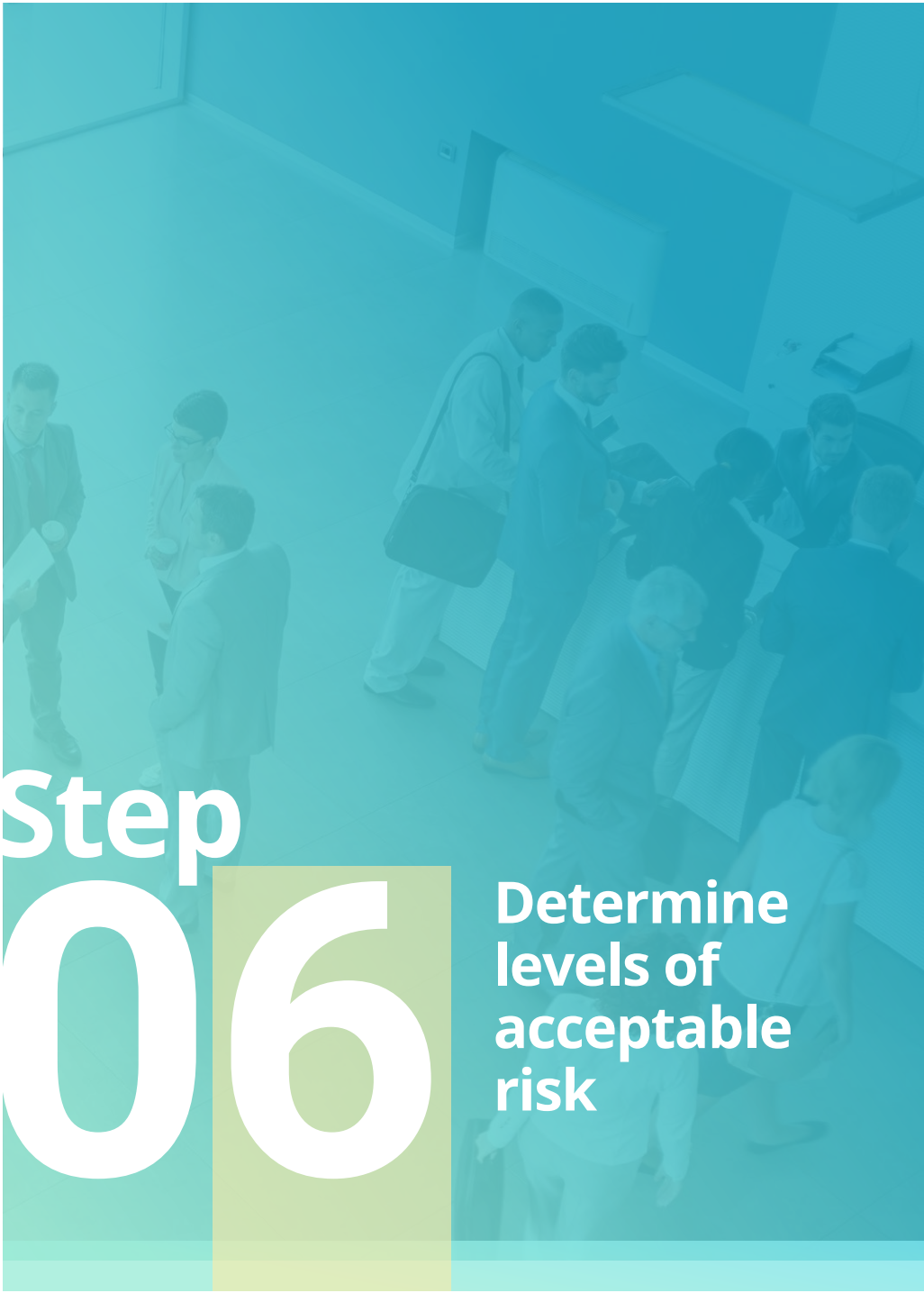
Assign an inherent (raw or untreated) risk rating based on the following risk matrix:

Master risk matrix

Consequence (Business Impact Level)

Likelihood	LOW	MEDIUM	HIGH	VERY HIGH	EXTREME	CATASTROPHIC
ALMOST CERTAIN	Moderate	Severe	Severe	Critical	Critical	Critical
LIKELY	Moderate	Moderate	Severe	Severe	Critical	Critical
POSSIBLE	Low	Moderate	Moderate	Severe	Severe	Critical
UNLIKELY	Low	Low	Moderate	Moderate	Severe	Severe
RARE	Low	Low	Low	Moderate	Moderate	Severe

You will note that as **likelihood** or **consequence** increase, so does the inherent risk rating.



Step 06

Determine levels of acceptable risk

Once the inherent risk ratings of all threats have been determined, organisations need to decide whether the assessed risk is consistent with the organisation's risk appetite, and if not, what treatments are required to bring the risk back to acceptable levels. This should help to determine any priority areas to focus on.

Executive leaders need to be involved to determine what risk level they are willing to accept based on the importance of:

- organisational goals and expectations
- critical functions and capabilities
- customer and stakeholder expectations (for government agencies, including ministers)
- personal security of staff and visitors
- general expectations about confidentiality
- continued availability of resources.

Executive leaders also need to be aware of their legal obligations e.g. Health and Safety.

Prioritisation can help to determine which risks are acceptable or unacceptable and where resources must be allocated to address unacceptable risk. It is helpful to determine a threshold for risk response as shown in the example table in the next section of this guide.

Step 07

Treat the risks

Establish the possible treatment appropriate to the risk and its inherent risk rating. Treatments or controls are generally aimed at reducing the likelihood of the threat event occurring or the level of impact (harm or disruption), or both.

The PSR policy framework contains security measures that help to treat risks across four domains – governance, personnel security, information security, and physical security. Identify possible risk treatments and ask yourself the following:

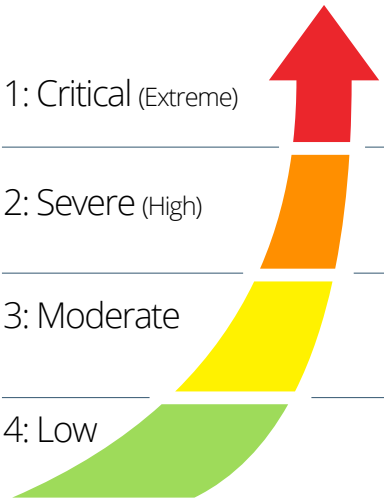
- What processes and controls are needed to reduce risk to an acceptable level?
- Who has responsibility for managing the risk?
- What resources are needed to treat the risk?
- Are the proposed measures cost effective for the level of impact if the risk is realised?
- Is the proposed treatment necessary, proportionate, and justifiable?

Treatments may include design and implementation of:

- new or altered procedures
- monitoring and reporting on systems and procedures
- new equipment
- ICT security controls
- physical security arrangements
- training or security awareness campaigns
- security clearing particular staff or positions
- avoiding, terminating or eliminating the activity causing the exposure.

Consider treatments that may already be in place and assess their ongoing suitability and sufficiency, whilst also considering other treatments. Consider their scalability and flexibility to adjust to future changes in risk profile including heightened risk/threat scenarios. This will help to future proof your work.

Example risk management response levels



1: Critical (Extreme)	Senior management owned. Immediate action is required to reduce the risk impact and/or likelihood through treatment. Formal risk management plan. Reviewed at least monthly at senior management meetings.
2: Severe (High)	Senior management owned. Urgent attention is required to reduce the risk impact and/or likelihood through treatment. Reviewed quarterly at senior management meetings.
3: Moderate	Senior management input required. Management responsibility is specified. Risk response should be to treat but may be accepted with a contingency plan in place. Regularly monitored and reviewed annually.
4: Low	Management responsibility is specified. Risk can be accepted with routine procedures in place. Occasionally monitored.

Step 08

Assess residual risk

Area Name: _____ Updated by: _____ Date Last Updated: _____

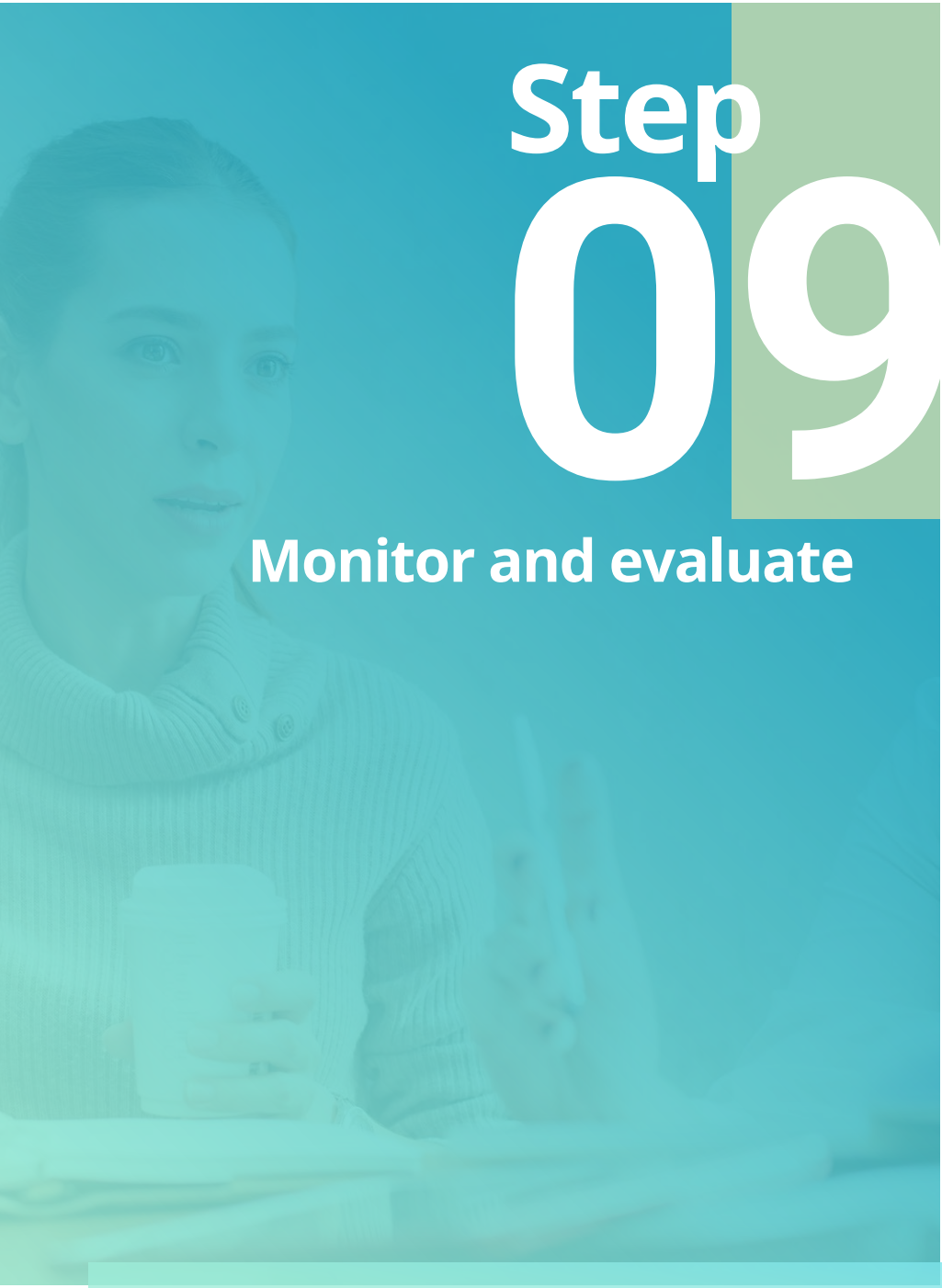
Unique ID	Risk Description	Caused by & Consequences	Risk Owners (s) *Name and Role*	Inherent Risk (Without controls)			Control (s)	Control Owners (s) *Name and Role*	Residual Risk (With controls)		
				Likelihood	Consequence	Risk Rating			Residual Likelihood	Residual Consequence	Residual Risk Rating
1	Risk 1	Caused by: Consequence:	aaa	Rare	Low	Low			Rare	Low	Low
2				Rare	Extreme	Moderate			Rare	Low	Low
3				Possible	Medium	Moderate			Rare	Very High	Moderate
4				Possible	Extreme	Severe			Rare	Low	Low
5				Possible	Catastrophic	Critical			Almost Certain	Catastrophic	Critical

Once treatments or controls have been applied to manage identified risks, an organisation should establish whether any residual risk remains. Re-use the process described in step five to assess residual risk.

Record all assessments in a risk assessment table.

The information in the risk assessment table can be used to develop an organisational risk management plan (roadmap) to document, prioritise, and monitor the development and implementation of further risk treatments or controls.

An example of a risk assessment table is shown at left:



Step 09

Monitor and evaluate

Monitor the threatscape on a regular basis and periodically evaluate the effectiveness of the security risk management plan and specific treatments in place to ensure that the treatments remain appropriate. An organisation's designated security lead, security team, or responsible person should conduct regular audits, inspections, and monitoring of:

- audit and inspection logs and findings
- security alerts from security experts and suppliers
- insider risk indicators
- security incident registers and investigations
- feedback on security treatments or procedures
- implementation progress and effectiveness of treatments
- changes to organisation goals, plans, functions, or responsibilities
- increased public attention to any policy or service.

In all cases, at a minimum, an annual review of security threats and risks is recommended.

As the security landscape in Aotearoa New Zealand continues to evolve, it is important for all organisations to have a clearly defined framework in place for assessing threats and risks to their people, information, and assets. Protecting these from harm is an important foundation and enabler for organisations as they carry out their mahi.

For further information and guidance on protective security best practice and policy, please visit the PSR website.

Resources

This section includes a range of useful resources to help guide organisations on identifying and managing their threats and risks.

Protective Security Requirements (PSR) website

The Protective Security Requirements is New Zealand's best practice security policy framework. The website outlines the Government's expectations for how its agencies should manage security governance, as well as personnel, physical and information security. Find the framework at **protectivesecurity.govt.nz**

National Cyber Security Centre (NCSC) website

The NCSC enables the protection, wellbeing and prosperity of Aotearoa New Zealand by providing trusted cyber security services. Find out more at **ncsc.govt.nz**

New Zealand Information Security Manual (NZISM) website

The New Zealand Information Security Manual (NZISM) is the New Zealand Government's manual on information assurance and information systems security. Find out more at **nzism.gcsb.govt.nz**

It Happens Here

This guide explains what insider threat is, how it happens, and what we can all do about it. It also includes case studies that illustrate the risks and consequences of not managing insider threats.

New Zealand's Security Threat Environment

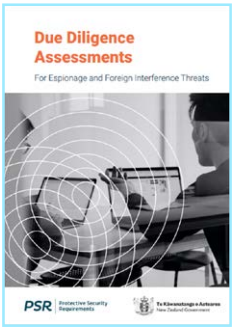
An assessment by the New Zealand Security Intelligence Service which contains insight the reader can use, with a focus on foreign interference, espionage and violent extremism.

Managing inwards visits

This advice helps organisations assess possible security risks around visiting delegations from overseas.

Espionage and Foreign Interference Threats

Security advice for members of the New Zealand Parliament and locally elected representatives.



Due diligence

This guide helps organisations identify and mitigate the risks associated with foreign interference when working with others.

For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

Te Kāwanatanga o Aotearoa
New Zealand Government

PSR | **Protective Security Requirements**