PSR | Protective Security Requirements

Version: 1.0 ***Last Review Date: Oct 2025***

Protective Security Requirements (PSR) Policy Framework:

SECURITY GOVERNANCE (GOV)

MANDATORY REQUIREMENTS 1-8

Introduction for document reviewers

What is this document?

This document is the final V1.0 consolidated PSR policy framework on security governance (GOV) implemented on 01 October 2025. It replaces all previous PSR policy information published on the PSR website.

Why has this document been developed?

In the past, PSR policy requirements were expressed on the PSR website and in publications, rather than in authoritative policy framework documents. Similar and overlapping content was spread across multiple webpages and at times expressed unclearly. This made PSR policy requirements difficult for stakeholders to find, understand, and apply.

This document aims to resolve these issues by establishing a clear and appropriate policy for security governance. Separate policy frameworks have been developed for other PSR domains.

What is this document based on?

This consolidated policy framework compiles the security governance policy set out previously on the PSR website, Capability Maturity Model, and relevant PSR guidance publications.

The content of is structured according to the mandatory requirements, with consistent use of sub-headings within each mandatory requirement and numbered paragraphs.

The security measures required to comply with the PSR are expressed clearly, using MUST, SHOULD, and COULD statements.

The intent of this consolidated policy framework is to clarify existing requirements, and to better support agencies to check that they are meeting these requirements. The intent is not to introduce significant or substantive change to these requirements.

Some policy requirement changes have been made, including those required to:

- resolve inconsistencies resulting from repetition and duplication of content
- incorporate new essential elements (for example, reference to Government Procurement Rules, Capability Maturity dimensions)
- align with broader expectations or existing practice (for example, managing potential conflicts of interest for senior security officials).

Has the minimum baseline for PSR changed?

The policy framework has been reviewed and clarified to ensure that it remains a robust protective security policy framework aligned with security best practice. The policy framework now articulates the minimum set of security capability and measures required for all organisations no matter their level of risk.

The minimum requirements are expressed as MUST statements and has been aligned to the PSR Capability Maturity (PS-CMM) level of 2 “Planned and Tracked” (formerly called ‘Basic’).

Table of Contents

Purpose

1. The purpose of this policy framework is to help an organisation govern protective security effectively to protect its people, information, and assets.

Who should read this document

2. This policy framework is primarily intended for use by organisations that implement the Protective Security Requirements (PSR). This includes:

   a. government organisations that are mandated to implement the PSR, and
   b. organisations that implement the PSR on a voluntary basis.

3. As good security practice, non-mandated organisations in the public and private sectors are encouraged to adopt the PSR as appropriate to their context.

4. This policy framework should be read along with the GOV Appendices, PSR Personnel Security (PERSEC), Physical Security (PHYSEC) and Information Security (INFOSEC) policy frameworks.

5. This information should be used by leaders and those with functional responsibility for protective security to establish their own security policies and measures to address their risks.

Introduction to the PSR

6. The PSR is New Zealand's best practice policy framework. It sets out what an organisation must do to manage security effectively. It also contains best practice guidance. See PSR Policy Framework Overview for a summary of the PSR policy requirements.

7. Protective security is a business enabler. It allows organisations to work together securely in an environment of trust and confidence and supports strategic and operational objectives.

Required and recommended measures

8. The PSR describes when an organisation needs to consider specific security measures – also called "controls" – to comply with mandatory requirements.

9. The security measures required depend on the level of risk that an organisation has determined it needs to manage and on its risk tolerance.

Required measures

10. A measure expressed with 'MUST' (or 'MUST NOT') is mandatory for all levels of risk.

11. An organisation must implement all mandatory measures unless it can demonstrate that a given measure is not relevant in its context.

12. If a mandatory measure cannot be directly implemented, suitable compensating measures MUST be in place to manage identified risks.

Recommended measures

13. A measure expressed using 'SHOULD' (or 'SHOULD NOT') is recommended for organisations with moderate and above risks.

14. A measure expressed using 'COULD' is recommended for organisations with high and above risks.

15. Valid reasons for an organisation not implementing recommended measures could include:

    a. a measure is not relevant because there is no apparent risk, or
    b. the residual risk is acceptable, or
    c. an alternative measure of equal strength is in place.

16. Not using recommended measures without due consideration may increase residual risk for an organisation. This residual risk needs to be agreed and acknowledged by an organisation head. Pose the following questions before choosing not to implement a recommended measure.

    a. Is the organisation willing to accept the residual risk? If so, what is the justification for this choice?
    b. Has the organisation considered the implications for all-of-government security? If so, what is the justification for this choice?

17. A formal auditable record of how an organisation considers and decides which measures to adopt is required as part of an organisation's governance and assurance processes.

Compliance with legislation

18. When legislation requires an organisation to manage protective security in a way that is different to the PSR, that legislation takes precedence.

Why governance matters

19. Governance is the system of leadership, direction, and control that enables an organisation to consistently achieve its goals. Governance helps an organisation to grow and achieve its desired objectives, stay ahead of risks, improve compliance, and improve trust and reputation with its stakeholders.

20. Building the right security governance, including security policies, plans, practices, and culture ensures the confident and secure conduct of its business. Protective security commitment and leadership from the top is essential.

Security Governance Policy Framework

21. Embedding protective security governance into an organisation enables it to manage its security risks proportionately and effectively and protect its people, information, and assets. To do this successfully, organisations need to ensure security is part of their organisational culture, practices, and operational plans.

22. An organisation MUST ensure protective security is part of its organisational governance, culture, practices, and operational plans to successfully manage its security risks.

GOV Mandatory Requirements Overview

23. The eight GOV mandatory requirements help organisations to implement robust security governance. These are:

    a. GOV1 – Establish and maintain the right governance
    b. GOV2 – Take a risk-based approach
    c. GOV3 – Prepare for business continuity
    d. GOV4 – Build security awareness
    e. GOV5 – Manage risks when working with others
    f. GOV6 – Manage security incidents
    g. GOV7 – Be able to respond to increased threat levels
    h. GOV8 – Assess your capability.

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.

24. An organisation MUST clearly:
    a. establish a security governance structure that ensures executive commitment to and oversight of protective security, and
    b. assign functional security responsibilities to specific individuals.

GOV 1.1 Ensure executive commitment and oversight

GOV 1.1.a Overall security accountability rests with the Organisation head

25. Organisation heads[1] are responsible for establishing and maintaining an appropriate environment within their organisation to:
    a. safeguard people and clients from foreseeable risks
    b. facilitate the appropriate sharing of government information to conduct business effectively
    c. limit the potential for compromise of the confidentiality, integrity and availability of its government information and assets, recognising risks such as those associated with information aggregation
    d. protect government assets from loss or misuse
    e. support the continued delivery of the agency's essential business regardless of disruptions caused by all types of hazards.

26. To achieve this an organisation head MUST:
    a. Recognise the importance of security and be accountable for all aspects and elements of security within their organisation;
    b. Understand, prioritise, and assign resources needed to manage protective security risks to prevent harm to government resources or disruption to business objectives;
    c. Ensure that effective protective security and business continuity management underpin organisational resilience;
    d. Ensure that security is part of their organisational culture, practices, and

[1] The organisation head is the person responsible for an organisation. They may have the title of Chief Executive Officer (CEO), Director-General, Secretary, Director or similar.

operational plans;
e. Ensure that effective protective security policies are implemented;
f. Establish the governance structures that will monitor the effectiveness of security management across the organisation;
g. Identify who is accountable for security at board or executive level;
h. Ensure they have clear reporting lines to all people with security responsibilities.

GOV 1.1.b The organisation head may delegate authority

27. An organisation head may, in writing, delegate to another person any of the powers or functions prescribed in the PSR but retains overall accountability for organisation security.

28. In delegating accreditation authority for physical or information security, organisation heads SHOULD carefully consider all the associated risks and remain responsible for the decisions of delegates.

29. Authority for information security SHOULD only be delegated to senior persons with specialised knowledge in information security and security risk management, preferably your chief information security officer (CISO). If the delegate is not the CISO, they MUST at least be a member of the senior executive team or in an equivalent management position.

30. If authority is delegated to a board, committee, or panel, the requirements of this section apply to the chair or head of that body.

GOV 1.1.c Establish effective security governance oversight

31. An organisation MUST ensure that senior leaders regularly consider protective security and are responsible for overseeing organisational security risks.

32. If appropriate, an organisation SHOULD establish a dedicated security governance body.

33. The appointed security governance leadership or body MUST:

a. understand organisational protective security risk exposure
b. set and review organisational standards for protective security risk tolerance;
c. govern the implementation of the protective security plans;
d. review organisational protective security performance, risks, incidents, and emerging threats;
e. ensure that performance against security measures and capability assessments are occasionally verified (e.g. internally audited/moderated);
f. establish the priorities and activities for protective security improvement.

34. The appointed security governance leadership body MUST receive regular, prompt, and proactive reports on security matters.

GOV 1.1.d Leaders promote and sponsor protective security

35. An organisation's executive leaders MUST understand protective security issues relevant to their areas of responsibility and their own responsibilities for security.

36. An organisation's executive leaders SHOULD demonstrate and actively promote good

security practice.

37. An organisation's executive leaders COULD drive continuous improvement in protective security including through approving and sustainably resourcing work on protective security best practice innovations.

GOV 1.2 Assign functional security responsibilities

38. Governance of security risk requires an effective security management structure with clear allocation of responsibility for all aspects of security.

GOV 1.2.a Appoint a Chief Security Officer (CSO)

39. The organisation head MUST 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 organisation head on security-related matters.

40. An organisation MUST provide a mandate to the CSO for establishing and undertaking the organisation's protective security programme for governance, personnel, information, and physical security with responsibility for the following (refer to **Security Governance** Appendix A: Security Roles and Responsibilities for more information):

    a. Oversight of protective security risk and performance
    b. Circulating and implementing protective security policy
    c. Providing guidance to the organisation head and the security governance body on security matters
    d. Managing and reporting security incidents
    e. Implementing a security awareness programme
    f. Liaison with security agencies in relation to protective security requirements.

41. An organisation SHOULD ensure that the CSO has the authority to make decisions on security matters, including resourcing security functions.

42. Where a CSO also holds a position with operational responsibilities (e.g. ICT, human resources, or finance), an organisation MUST ensure that any real or perceived conflicts of interest are clearly identified, declared, and actively managed.

43. The CSO COULD be responsible for and have the authority to commission and deploy protective security initiatives and systems as part of an active and agile continuous improvement programme.

44. The CSO COULD ensure that the organisation's leadership team, management team, and governance bodies take part in regular, structured discussions about protective security matters and responsibilities, and use action points from these discussions to inform priorities, performance measures, and continuous improvement.

GOV 1.2.b Appoint a Chief Information Security Officer (CISO)

45. The CISO's role is based on good practice in the information security industry and in governance. The role ensures that information security is managed at the senior leadership level. Without a CISO, an organisation is unlikely to be able to effectively manage information security risks.

46. An organisation MUST appoint a CISO.

47. The CISO MUST:

    a. be a senior leader in the organisation
    b. be sufficiently qualified and experienced to bring accountability and credibility to information security management [see **Security Governance Appendix A: Key protective security roles and responsibilities** for CISO roles and responsibilities]; and
    c. report directly to the organisation head or delegated senior executive on matters of information security.

48. If a CISO holds another role, such as also being chief information officer (CIO) or a manager of a business unit, conflicts of interest might arise when operational imperatives conflict with security requirements. Good practice separates these roles. When a CISO holds multiple roles, an organisation MUST:

    a. clearly identify potential conflicts of interest
    b. implement a mechanism to allow independent decision making in areas where conflicts may occur.

Virtual CISO role

49. If an organisation outsources the CISO function (e.g., a Virtual CISO), accountability and ownership of risk MUST sit with the CSO or equivalent senior executive team member.

50. If the organisation appoints a Virtual CISO, it MUST identify and carefully manage conflicts of interest, availability, and response times, so that the organisation is not disadvantaged, and effectively manage possible conflicts of interest when an outsourced CISO deals with other vendors.

GOV 1.2.c Ensure functional management and governance responsibility

Define and allocate security management responsibilities

51. Depending on an organisation's size, risk profile, and the value of its assets, information and equipment, it may be necessary to create a specialist protective security unit and/or appoint specialist security personnel supporting the CSO. Responsibility for security may form only part of a person's role.

52. An organisation MUST ensure there is a clear allocation of responsibilities for personnel security, information security, and physical security.

53. An organisation SHOULD establish and formalise roles and responsibilities for managing protective security (personnel security, information security, physical security) with a reporting relationship to the CSO for those responsibilities. These roles are designated as 'Security Manager' for the specific domain (e.g., Information Security Manager, Physical Security Manager, Personnel Security Manager.) Refer to **Security Governance Appendix A: Key protective security roles and responsibilities** for more information.

54. An organisation MUST review protective security leadership and management responsibilities and reporting lines when relevant organisation structure, people, and/or responsibilities change.

55. An organisation SHOULD review protective security leadership and management

responsibilities and reporting lines at least every two years.

Ensure security management is active and visible

56. Tools and technologies supporting security management MUST meet basic needs for compliance.

57. Security personnel and/or the protective security unit SHOULD work in close association with other business units to ensure that security requirements are managed appropriately.

58. An organisation SHOULD ensure that security managers:

    a. Are active in the day-to-day management of their assigned security domain, including for driving the understanding of, and compliance with, the organisation's security policy and processes;
    b. Are visible and known by people in the organisation and people feel confident to approach them when necessary;
    c. Have access to and engage regularly with the organisation's security leaders and relevant governance bodies on security matters;
    d. Regularly conduct incident drills and discussion-based exercises with lessons learned fed back into planning, policy, and process improvements.

59. An organisation SHOULD ensure that there is a clear delineation between security governance and security management to support robust assurance processes.

60. An organisation SHOULD ensure that people leading change or other initiatives consider potential implications for security and proactively engage with security managers and leaders.

61. An organisation COULD make proactive use of research, environment scans, and long-term planning to ensure security priorities and resource levels remain proportionate to risk.

Convene a cross-functional group when appropriate

62. In larger organisations, it may be necessary to convene a cross-functional group of management representatives to coordinate security controls.

63. An organisation COULD convene a cross-functional group (for example, a Security Reference Group (SRG)). Alternatively, this group's role may be filled by an existing Risk and Audit Committee or equivalent. Example responsibilities are:

    a. agree on specific roles and responsibilities for security across the organisation;
    b. ensure protective security is integrated into the agency's risk management, audit, and assurance processes;
    c. agree on the methodologies and specific processes for security, such as risk assessment procedures and systems for protectively marking information and assets;
    d. assess and coordinate the implementation of specific security controls for new systems or services;
    e. review security incidents and recommend appropriate process improvements;
    f. support organisation-wide security initiatives such as awareness programmes;

g. ensure the availability of internal support is well advertised.

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.

64. Managing security risks proportionately and effectively enables organisations to protect people, information, and assets. Figure 1 below shows how an organisation's policies, plans and processes interlink and are informed by their risk assessment.

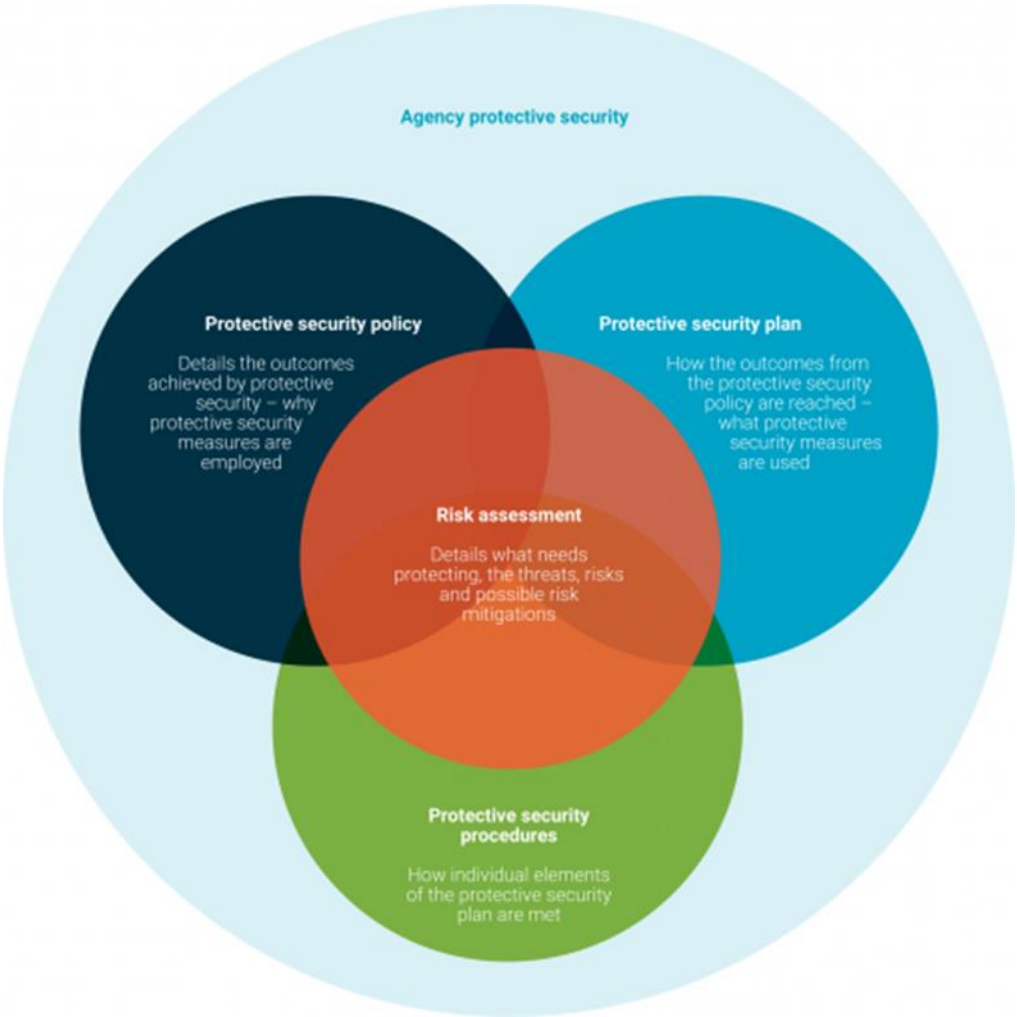

Figure 1: Relationship of security policies, plans, risk, and procedures

65. To successfully manage security risks, organisations MUST:

    a. Identify, assess, and manage security risks
    b. Formulate security plans to address those risks
    c. Clearly define and articulate security policies, processes, and procedures that

establish the expectations and approaches it will use to achieve security.

GOV 2.1 Identify, assess, and manage security risks

GOV 2.1.a Adopt an appropriate risk management approach

66. Following best practice in risk management will help an organisation to:

    a. Identify security threats and vulnerabilities
    b. manage security risks
    c. protect people, information, and assets
    d. give assurance to other organisations you work with.

67. The right risk management approach will vary from organisation to organisation, but the process should be consistent with your enterprise risk management framework, transparent and justifiable.

68. An organisation MUST adopt an appropriate risk management approach that is consistent with the ISO 31000 Risk Management standards when managing protective security risks.

69. An organisation's approach for managing security risks SHOULD aim to:

    a. assess the potential vulnerabilities and threats to the assets (including people, property, information, systems, and reputation) requiring protection and the likelihood of compromise
    b. assess the impact and possible consequences of harm to those assets
    c. assess the security risks
    d. determine levels of acceptable risk
    e. implement security measures to reduce risks to acceptable levels
    f. monitor and evaluate the risks.

GOV 2.1.b Identify and assess protective security risks

70. Organisations face a wide range of risks and threats and need to have systems and processes in place to understand where they are most at risk and assess the impacts should the risk be realised.

71. An organisation MUST conduct threat and risk assessments on the people, information, and assets the organisation needs to protect (as defined in PERSEC, INFOSEC1 and PHYSEC1 - Understand what you need to protect).

72. An organisation MUST assess the impacts of the compromise of its people, information, or assets. Business Impact Levels (BILs) can be used to assess impacts. Refer **Security Governance** Appendix B: Business Impact Levels (BILs) for more information.

73. An organisation MUST maintain an organisational security risk management plan.

74. An organisation SHOULD periodically scan the environment for emerging threats, schedule regular reviews of enterprise risks and security measures for vulnerabilities and identify measures to treat risks.

75. An organisation COULD monitor and use international and New Zealand security threat information and best practice advice on how to reduce the risks to the organisation.

GOV 2.1.c Consider risk measures when working or co-locating with others

76. The impact of similar risks can vary between organisations based on their functions and size.

77. An organisation MUST:

    a. understand any differences in risks and their impacts between organisations that it collaborates or co-locates with,
    b. negotiate and agree the security measures that need to be in place to treat risks appropriately for all parties.

78. As part of GOV5, an organisation MUST establish minimum-security and risk management requirements for suppliers it works with and verify that they have effectively and consistently meet these requirements. Refer to GOV5 for more information.

79. An organisation SHOULD ensure that its people, co-locating and collaborating organisations, and suppliers actively contribute to identifying, managing, and reporting on protective security risks.

80. An organisation COULD share information, expertise, and learnings with organisations that it collaborates with to improve their awareness, capability, and overall security resilience.

GOV 2.1.d Manage your security risks effectively

81. An organisation MUST ensure that risks are managed in line with the organisation's assessed level of risk and risk tolerance.

82. An organisation MUST ensure that security risks and issues are considered as part of the design phase for all processes and systems.

83. An organisation MUST ensure security risks are occasionally reviewed.

84. An organisation SHOULD oversee and actively manage its protective security risks as part of its strategic or enterprise risk management framework. This includes integration into risk reporting and management by its executive team and risk and assurance governance body; as well as ongoing monitoring and analysis of whether:

    a. risks and their risk levels have changed
    b. risk response measures are being applied effectively
    c. risk management improvements are implemented effectively.

85. An organisation SHOULD ensure that:

    a. Security risk management plans are coordinated
    b. Security measures are applied consistently across the organisation
    c. Security risk management is reported regularly to the security governance body.

86. An organisation COULD embed security considerations into their change management processes.

87. An organisation COULD incorporate security measures into automated operational business processes.

88. An organisation COULD embed a continuous review and improvement cycle into its security risk management practices and risk measures.

GOV 2.2 Formulate security plans

GOV 2.2.a Ensure security plans address key risks

89. The objectives of security planning is to:

    a. use risk assessments to identify areas of security risk
    b. outline practical steps to treat the risks
    c. inform organisational decisions on where to invest resources
    d. build needed capability over time based on the organisational priorities
    e. review, update, and monitor progress against the plan.

90. An organisation's security planning MUST cover the security measures required across all four domains to address its key security risks – security governance, personnel security, information security, and physical security.

91. An organisation's security planning MUST be based on its protective security risk assessment and risk tolerance.

92. Organisation-wide security plans MUST be approved at an executive level.

93. An organisation's security plans SHOULD be comprehensive and detailed, and involve consultation with:

    a. people from every section of your organisation
    b. personnel who directly manage security or related work (e.g., CSO, CISO, security managers / advisors, health & safety managers/advisors, privacy officer, property managers)
    c. senior management, to ensure their support and to ensure the plan's success.

94. An organisation's security plans SHOULD demonstrate clear awareness and agreement about acceptable levels of security risk (tolerance) set by the security governance body.

95. An organisation's security plans SHOULD be communicated and accessible to all relevant stakeholders.

96. An organisation's security planning COULD be fully integrated into the organisation's business strategy and planning cycles.

GOV 2.2.b Regularly review, update, and phase security actions

97. An organisation's security plans MUST be reviewed in response to major security incidents; for more detail see GOV6: Manage security incidents and recurring breaches.

98. In addition, an organisation's security plans SHOULD be reviewed:

    a. in response to changes in its threats or vulnerabilities;
    b. in response to changes to its operating environment; and
    c. every two years to ensure it remains relevant to the organisation's risk profile, is sustainable, and informed by changes in the PSR and relevant standards.

99. Based on the organisation's risk level and maturity goals defined in GOV8: Assess your

capability, an organisation SHOULD develop a multi-year roadmap to build and maintain the necessary security capabilities and measures to treat its risks.

100. An organisation SHOULD track and report to its security governance body on progress against security plans.

101. An organisation's security planning COULD be informed by up-to-date, evidence-based data, which is used to analyse threats, understand trends, and conduct forecasting.

102. An organisation's security planning COULD be continuously monitored, reviewed, and improved in response to real-time data and information.

GOV 2.3 Define and articulate security policies, processes, and procedures

103. For security plans and measures to be effective, security policies, processes, and procedures need to be accessible, well-communicated, and easy to understand and follow.

GOV 2.3.a Develop security policies

104. An organisation MUST document security policies that sets out its approach and commitment to security. The security policies MUST cover:

    a. Security governance, including how the organisation addresses all aspects defined in the PSR Governance Policy framework (this document);
    b. Personnel security, including how the organisation addresses all aspects defined in the PSR Personnel Security Governance Policy framework;
    c. Information security, including how the organisation addresses all aspects defined in the PSR Information Security Policy framework, Classification System and NZISM;
    d. Physical security, including how the organisation addresses all aspects defined in the PSR Physical Security Policy framework.

105. An organisation MUST ensure that security policies cover how protective security relates to other components of operational governance, such as:

    a. employee and public health and safety, culture, and well-being
    b. staffing, recruitment, on-boarding, and off-boarding
    c. internal and external communications
    d. procurement and contracts
    e. audit and compliance
    f. fraud and risk
    g. business continuity and emergency response
    h. policy and procedure management
    i. organisational governance and decision making.

106. An organisation's security policies SHOULD be approved by and overseen by the CSO or appropriate delegated authority, who is accountable for implementation.

107. An organisation's security policies SHOULD:

    a. be based on robust risk analysis
    b. support operations and business continuity

c. be cost effective.

108. An organisation's security policies SHOULD articulate why the policies are necessary and who has authorised them.

GOV 2.3.b Define security processes, procedures, and guidance

109. An organisation's security policies MUST be supported by clearly defined processes and procedures including guidance on:

a. security roles and responsibilities (GOV1)
b. security processes and procedures including risk management (GOV2)
c. business continuity (GOV3)
d. supply chain management (GOV5)
e. security incident management (GOV6)
f. threat response (GOV7)
g. security capability assessment (GOV8)
h. guidance on PERSEC, INFOSEC, and PHYSEC, including for individual sites, systems, or services when appropriate
i. clear definitions of responsibility for the handling of protectively marked material, whether in electronic or hard copy form (Classification System)
j. an ongoing programme of user security awareness and education (GOV4).

110. An organisation MUST ensure that the policies and procedures are accessible, easy to understand, and used effectively by the relevant people in the organisation who need them.

111. An organisation SHOULD ensure that relevant security policies and procedures are effectively and routinely used across the enterprise.

GOV 2.3.c Review your security policies and processes

112. An organisation MUST review its security policies and processes, whenever security requirements change, or major incidents occur, including:

a. the security policy's effectiveness, gauged by the nature, number and impact of recorded security incidents
b. the cost and impact of security measures
c. effects of changes to technology
d. levels of user compliance.

113. An organisation SHOULD review security policies and procedures at least every two years – to identify gaps or to reflect changes to risk factors. For example, after:

a. changes to threats or vulnerabilities
b. changes to the agency's functions, structure, or technical infrastructure.

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.

114. Business continuity is the capability of an organisation to continue delivery of products or services within acceptable timeframes, and at acceptable capacity following a disruptive event.

115. Causes of disruptions include natural events such as earthquakes or severe weather, loss of a key resource such as a power failure, technological failure, or supply chain disruption, as well as security threats such as sabotage, espionage, or cyber-attacks. Disruptions can occur at any time, for any reason, and their impact varies.

116. The International Standards Organisation (ISO) 22301 sets the standard for business continuity management (BCM).

117. A programme for managing business continuity helps an organisation to prepare for and manage the impact of disruptions, regardless of cause.

118. An organisation MUST maintain a BCM programme to ensure it is effective and secure during a disruptive event, by:

    a. Setting the scope of the BCM programme
    b. Identifying critical functions and their requirements for business continuity
    c. Developing plans, alternative strategies, and arrangements for maintaining critical functions
    d. Ensuring appropriate protective security arrangements are embedded in planning
    e. Monitoring the organisation's overall level of preparedness for a disruptive event
    f. Validating plans and ensuring continuous improvement.

119. An organisation MUST consider how it will maintain protective security during a business continuity event and build effective security measures into its business continuity programme.

GOV 3.1 Set the scope of the business continuity programme

120. Not everything an organisation does as 'business as usual' can or should be maintained during a disruption. There may also be additional responsibilities that need to be planned for.

121. The scope of the business continuity programme MUST:

    a. be agreed with senior management
    b. cover agreed critical functions
    c. include supporting functions and requirements to maintain critical functions, or resume them within acceptable timeframes.

122. The scope of the programme SHOULD consider the organisation's:

    a. overall strategy

b. objectives
c. structure.

GOV 3.1.a Develop a policy for managing business continuity

123. An organisation MUST develop a policy that outlines the intent and coverage of its business continuity programme.

124. A policy for managing business continuity SHOULD include:

a. a definition of business continuity management
b. reference to any standards and guidelines to follow
c. what the programme covers
d. how the programme will be structured and run
e. links with other policies, processes, and disciplines within your organisation (for example, risk management, incident management, heightened security alert response management, health and safety, and emergency management).

GOV 3.1.b Assign responsibility for business continuity

125. An organisation MUST establish who oversees and takes responsibility for your BCM programme and for developing and approving business continuity plans (see GOV 3.3.c for more information on teams required to manage business continuity).

126. An organisation SHOULD clearly assign responsibility for business continuity including:

a. governance
b. a senior manager to sponsor the programme
c. a team to lead the programme's implementation
d. critical function plan owners, and subject matter experts
e. security leads to oversee and manage the security measures
f. incident response.

GOV 3.2 Identify critical functions and their requirements

127. An organisation's critical functions are those that the organisational leadership have determined are critical to maintain during a disruption, to meet their core responsibilities.

GOV 3.2.a Identify critical functions

128. An organisation MUST identify its critical functions.

129. When identifying critical functions, an organisation SHOULD assess:

a. the impact over time of a disruption to these functions
b. interdependencies between functions
c. shared requirements across the organisation.

GOV 3.2.b Conduct a business impact analysis

130. An organisation MUST conduct a business impact analysis (BIA) to evaluate the potential impact over time of a disruption on the organisation's critical functions.

131. The BIA MUST consider which resources and requirements are essential for maintaining

the organisation's critical functions. Think about:

a. people and their capabilities
b. facilities and associated utilities
c. supplies and equipment
d. information and data
e. technology (systems, applications)
f. transportation and logistics
g. suppliers and outsourcing partners.

132. When conducting a business impact analysis, an organisation SHOULD collaborate with people across the organisation who are responsible for risk management. Consider risks that the organisation has already identified, and any measures for reducing them that are already in place.

133. An organisation's business impact analysis SHOULD include a risk assessment to identify and quantify the risk of disruption to the function, including risks to the requirements the function needs.

GOV 3.3 Develop solutions and plans for maintaining critical functions

134. An organisation MUST develop solutions to maintain critical functions and document these in business continuity plans.

GOV 3.3.a Develop solutions

135. When planning for business continuity, there are a range of solutions an organisation can apply to each resource requirement. Solutions include:

a. diversifying (for example, having separate premises where the same activity occurs in parallel)
b. replicating (for example, having people in another location who are trained and able to carry out a critical process, but don't do it as 'business as usual')
c. using standby options (for example, maintaining an alternate facility that can be made operational within the recovery timeframe)
d. acquiring a resource or service after an incident
e. outsourcing the function to a third party
f. having insurance
g. using manual workarounds
h. doing nothing.

136. An organisation MUST get assurance that appropriate security measures and solutions have been identified and implemented (based on the business impact analysis and risk assessment) to all resources that support business continuity and resilience of agreed critical functions — people, facilities, supplies and equipment, information and data, technology, transportation and logistics, and suppliers and outsourcing partners.

137. An organisation SHOULD consider use of supporting expertise or resources, such as information technology when designing business continuity solutions.

138. An organisation SHOULD perform an assessment of cost-effectiveness against recovery time objectives of different responses to help decide which solutions to pursue.

GOV 3.3.b Document business continuity planning and procedures

139. The structure and complexity of business continuity plans depends on the organisation and its needs:
    a. Larger organisations may have separate plans that cover different requirements or business functions. For example, they may have an overall plan which describes the business continuity scope and response procedures, and separate plans for business units, service locations, or specific functions.
    b. Smaller organisations may have a single plan.
140. An organisation MUST document business continuity plans to articulate its procedures for responding to a disruption of any kind.
141. An organisation's plans SHOULD cover:
    a. processes for notification, activation, and escalation
    b. who will fulfil key roles in a response (strategic oversight, tactical, and operational roles)
    c. leadership continuity
    d. structures and processes for responding to disruptions
    e. response priorities
    f. details of critical functions:
        i. requirements and timeframes
        ii. processes for maintaining the function, including where detailed operational procedures or plans can be found
        iii. changes to security policies and measures during the event, if necessary
        iv. communication procedures (internal, external)
        v. any links to other plans and processes within the organisation.
142. Business continuity plans SHOULD be simple, fit for purpose, and easy to use under the pressure of a response situation as evidenced through exercises to validate the plans.
143. Templates and checklists COULD be used to help make plans easy to use.

GOV 3.3.c Establish teams to manage business continuity in a disruption

144. An organisation MUST create a structure for business continuity management, ensuring that key roles and responsibilities are documented, assigned, and that the right processes are in place. For example, an organisation may require separate teams:
    a. a strategic response team to focus on the issues from an organisation-wide perspective. The team is usually led by top management and is often called a crisis management team. This type of team needs to be flexible, and involve experienced managers with the authority to apply the organisation's full resources to the response;
    b. a tactical response team to manage and coordinate the processes required to deliver your critical functions and to ensure resources are appropriately allocated;
    c. an operational response team to keep critical functions running or recover them.

145. An organisation MUST integrate its response to a disruption with the incident response processes of other teams that protect its operations – such as security, health and safety, emergency management, information management, and risk management.

146. If an organisation has responsibilities under the Civil Defence Emergency Management Act 2002, its emergency management arrangements MUST align with New Zealand's Coordinated Incident Management System (CIMS).

147. An organisation SHOULD select people for response teams who have the right skills and competencies and train them appropriately. This includes selecting and training back-up people for critical roles.

148. An organisation COULD make sure that people with critical BCM roles do not have competing responsibilities.

GOV 3.4 Monitor organisational preparedness for a disruptive event

GOV 3.4.a Educate people on your business continuity arrangements

149. Training, education, and awareness are important. An organisation MUST ensure that its business continuity processes are well-understood by all people assigned roles in the business continuity programme.

150. An organisation SHOULD conduct training and awareness campaigns on its business continuity programme across all people in the organisation.

151. An organisation COULD extend its business continuity training and exercises across organisational lines including its suppliers and cooperating partners.

GOV 3.4.b Run exercises to validate business continuity plans and prepare for disruptions

152. Business continuity exercises allow an organisation to validate planning, test assumptions and identify issues or gaps in planning. Exercises also build the capability of response teams.

153. An organisation MUST run an exercise at least every two years to validate business continuity plans and assess the organisation's preparedness for a disruptive event.

154. An organisation SHOULD run additional periodic exercises that validate, assess, practice, and improve aspects of plans for ensuring business continuity.

155. The type of exercises an organisation uses will depend on its exercise objectives. Each type of exercise requires a different amount of time to prepare and facilitate and carries a different level of risk and cost.

Exercise	Description
Discussion exercise	A discussion where participants 'walk through' plans or focus on a particular area for improvement.
Scenario exercise	A discussion exercise with a scenario and timeframe. Participants demonstrate their response plans as the situation unfolds.
Simulation exercise	An exercise with a more elaborate scenario, with information introduced as the situation unfolds, simulating a real incident. Participants rehearse their roles.
Live exercise	A real-time rehearsal of part or all of a response.
Test	Testing of technology, equipment, or procedures, resulting in a pass or fail.

GOV 3.5 Review and maintain the business continuity programme

GOV 3.5.a Review plans regularly to ensure effectiveness and continual improvement

156. Reviews help an organisation to evaluate its policy, plans, and processes to ensure they remain appropriate and effective, and to identify areas for improvement. Types of review include:

    a. audit
    b. self-assessment
    c. quality assurance activities
    d. supplier performance review
    e. management review
    f. appraisal of performance against business continuity roles and responsibilities.

157. After activating business continuity plans (either in an exercise or in real-life incidents), an organisation MUST review the effectiveness of these plans to ensure they remain fit for purpose.

158. An organisation SHOULD ensure that recommendations from the review process focus on continual improvement.

GOV 3.5.b Maintain your business continuity programme

159. An organisation MUST maintain its business continuity programme to enable its critical functions to continue to the fullest extent possible during a disruption.

160. An organisation MUST maintain its business continuity programme when changes occur within the organisation. Changes to a business continuity programme may include:

    a. changes in the organisation, such as a change in organisational structure
    b. new functions, or changes to existing functions, such as a change in the way a function is delivered
    c. changes to the requirements that support functions, such as a new IT system
    d. changes to third party suppliers
    e. lessons learnt from an exercise or incident
    f. findings from an assessment or review.

GOV 4: Build security awareness

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

161. Building security awareness (including through training) helps an organisation to create a strong security culture that protects people, information, and assets.

162. An organisation MUST build security awareness to ensure that its people understand their security obligations, are aware of security risks, and follow security procedures.

GOV 4.1 Establish a security awareness and training programme

163. An organisation MUST use a consistent and structured approach to determine its security awareness and training needs, and design security awareness and training programmes to:

    a. address its identified security risks
    b. ensure security policies and processes are followed
    c. promote personal responsibility for effective security by all personnel working for the organisation (e.g., employees, secondees, contractors, and temporary staff) regardless of role or level of access.

GOV 4.1.a Set the scope of your security awareness and training programme

Who to involve

164. An organisation MUST establish security awareness and training programme for:

    a. all its personnel based in its facilities
    b. all its personnel and other people who have access to its information and assets
    c. all holders of a New Zealand national security clearance within the organisation. (PERSEC 4: Manage national security clearances has more detail.)

165. An organisation MUST seek assurance from co-locating and collaborating organisations about their security awareness and training programmes to confirm that:

    a. Personnel based in their facilities receive appropriate security awareness training or briefings
    b. 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
    c. Sponsored holders of shared New Zealand national security clearances receive appropriate security awareness training or briefings.

166. An organisation SHOULD consider establishing security awareness and training for all people who have access to its facilities in any capacity.

Training programme coverage

167. An organisation's security awareness training MUST cover security measures in:

    a. its facilities, including those shared with other organisations

b. other organisations facilities its personnel operate in
c. places where its personnel work (including working from home or other remote locations).

168. An organisation's security awareness training MUST cover policies and procedures for reporting including security incidents, changes of personal circumstances, and any mandatory or legislative reporting requirements.

169. An organisation's security awareness training MUST cover policies and procedures for:

a. maintaining personal safety
b. protecting assets
c. protecting information
d. attending security briefings (when required).

170. An organisation SHOULD ensure that induction training covers security awareness training and how to access support.

171. An organisation's security awareness training COULD cover security measures relating to:

a. threats to the organisation/location; and
b. good security standards/behaviours.

GOV 4.1.b Set security awareness programme goals

172. An organisation MUST establish how it will measure the security awareness programme performance goals and ensure that its personnel understand the organisation's security rules and any specific responsibilities that apply to their roles or work areas. This includes giving personnel the knowledge they need to perform their security duties effectively. Personnel need to understand the threats an organisation's security measures are designed to counter, so they can help maintain security.

173. An organisation MUST actively monitor education needs and reassess security awareness training content to ensure it remains fit for purpose.

GOV 4.2 Implement security awareness training

GOV 4.2.a Ensure security awareness is an ongoing and regular part of operations

174. An organisation SHOULD make security awareness training an ongoing, regular part of its operations by:

a. having defined plans and schedules for delivering relevant security communications
b. starting security awareness training when new people join, by making it a part of your organisation's induction programme
c. holding regular refresher sessions to remind people about security measures and let them know about any new measures
d. providing targeted security awareness training when the threat environment changes or there's an increased risk of a security breach
e. providing targeted role-specific security training as needed.

GOV 4.2.b Provide additional training for people in emergency, safety, or security functions

175. An organisation MUST keep its people and visitors safe by designing extra training for people with emergency, safety, or security functions, so they can help to keep everyone safe in times of danger or threat, and by conducting exercises to help them practise their skills and confirm their ongoing competency. For more information, refer to:

    a. GOV3 Preparing for business continuity
    b. GOV7 Be able to respond in increased threat levels
    c. Health and Safety at Work Act 2015
    d. Relevant codes and standards, such as AS/NZS 4804:2001 - Occupational Health and Safety Management System.

GOV 4.2.c Train personnel on how to protect assets

176. An organisation MUST ensure that its people know how to keep its assets secure. Before allowing access to assets, an organisation MUST provide training about:

    a. using access control systems and other measures to protect assets
    b. meeting legal requirements to protect assets
    c. reporting lost, damaged, or stolen assets
    d. auditing and stocktaking requirements for assets.

GOV 4.2.d Provide guidance on upholding legislation for protecting official information

177. People who work in government organisations need to be aware of the requirement to protect official information.

178. An organisation MUST provide guidance for its personnel on protecting official information, including the:

    a. Standards of Integrity and Conduct for public servants
    b. Official Information Act 1982, sections 6, 9, 27, 31
    c. Privacy Act 2020, privacy principles
    d. Crimes Act 1961, sections 78, 78A, 78B, 78C, and 79
    e. Summary Offences Act 1981 – section 20A
    f. Protected Disclosures Act 2022 (i.e. whistleblowing)

179. An organisation MUST provide its personnel with timely and ongoing training on classifying information, assess their understanding, and ensure that they have the ability to comply with the Classification System. This includes training on how to securely handle government information, including how to classify it, how to share it, and how to declassify it. See Classification System for more information.

GOV 4.2.e Train personnel to report security concerns

180. An organisation MUST train its people to report any security risks they encounter, including:

    a. suspicious behaviour
    b. threatening behaviour communicated through letters, bomb threats, and phone calls
    c. lost, stolen, compromised or broken ICT and security equipment/assets

d. security infringements and breaches (see GOV 6: Manage security incidents)
e. security vulnerabilities e.g., insecure classified waste bins, doors left insecure, etc.
f. lost identity or credit cards
g. lost protectively-marked, official, or government material
h. serious wrongdoing (within the same organisation or another).

GOV 4.3 Build a strong security culture

GOV 4.3.a Communicate effectively to enhance your security culture

181. Security culture refers to the set of shared security-related values, beliefs, attitudes, and assumptions that are inherent in the organisation. Security culture is reflected in how people think about and approach security. Leadership commitment to a positive security culture and getting security culture right helps to develop a security aware workforce that adopts and promotes secure behaviour.

182. To support a strong security culture, an organisation SHOULD run an ongoing security awareness programme to regularly remind people of security responsibilities, issues, and concerns. Some ways to keep security awareness high include:

    a. 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
    b. promoting security processes and tips through publications, electronic bulletins, and visual displays such as posters
    c. carrying out security drills and exercises
    d. including security questions in job interviews
    e. including security attitudes and performance in your performance management programme.

GOV 4.3.b Monitor training effectiveness

183. An organisation SHOULD track and record participation in security training.

184. An organisation COULD review security training to ensure it is aligned to best practice and it stimulates cross functional security discussions and enhances its security culture and practice.

GOV 4.3.c Monitor security behaviours and culture

185. An organisation MUST have metrics and processes in place to assess its security culture. This can be assessed as part of a workplace culture survey.

186. An organisation's leaders SHOULD lead by example, by actively and visibly demonstrating their commitment to good security practice e.g. not wearing lanyards outside the office.

187. An organisation SHOULD have processes in place to evaluate people's adherence to security obligations. Suspected security policy non-conformance and breaches should be raised as security incidents. See GOV6: Managing security incidents for more information.

188. An organisation SHOULD integrate protective security into business processes, helping

people to follow good practice by default.

189. An organisation COULD continuously monitor its security culture and use this information to inform development of improvement plans, security awareness programmes, and education resources.

GOV 4.3.d Manage poor security behaviour effectively

190. An organisation MUST ensure that anyone suspected of breaching security is treated fairly and are made aware of the process as part of inductions and security awareness programmes.

191. An organisation SHOULD have a formal process for people who breach your security policies and processes. Use breaches as learning opportunities. For major and ongoing issues, formalise it as part of managing misconduct. See GOV 6 Manage security incidents for more information.

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.

192. Organisations rely on suppliers to deliver products, systems, and services. This includes your partners, cooperating organisations, and customers. These suppliers broaden the risks the organisation is exposed to. Suppliers can be a weak point in an organisation's security defences when they are not managed well.

193. A 'supply chain' can be described as 'a network of organisations connected by a series of relationships involving the supply of goods or services.

194. Supply chains can be large and complex, involving many suppliers doing many different things. For example, some organisations may:

    a. outsource payroll to a provider whose systems are hosted in the cloud and maintained by another software provider
    b. partner with another organisation (for example, an NGO) to provide front-line services, which in turn uses several providers to support their business.

195. Securing supply chains can be challenging because it can be difficult to identify vulnerabilities or recognise where they could be introduced and exploited. Many organisations are not aware of all of the suppliers who make up their supply chain.

196. An organisation MUST consider adopting twelve principles of supply chain security[2] to manage the protective security risk of its supply chain. The principles discussed in this section are:

    a. Understand the risks from your supply chain
        i. Understand what needs to be protected
        ii. Know who your suppliers are, and understand their security measures
        iii. Understand the security risks posed by your supply chain.
    b. Establish control
        iv. Communicate your view of security needs to your suppliers
        v. Set and communicate minimum security requirements for your suppliers
        vi. Build security considerations into contracting process and require suppliers to do the same
        vii. Meet your own security responsibilities
        viii. Raise awareness of security within your supply chain
        ix. Provide support for security incidents
    c. Check your arrangements

[2] Best practice principles developed by the UK Government for managing supply chains.

x. Build assurance activities into your supply chain management

d. Seek continuous improvement

xi. Encourage the continuous improvement of security within your supply chain

xii. Build trust with suppliers.

GOV 5.1 Understand the risks when working with others

197. The threats from an organisation's supply chain come in many forms. An organisation may fail to clearly communicate its security requirements, or a supplier may:

a. fail to adequately secure their systems
b. have a malicious insider working for them
c. carry out malicious acts for their own gain.

198. An organisation could be exposed to a combination of the following risks:

a. harm to your people or customers
b. loss of data
c. privacy breaches
d. loss of intellectual property
e. disrupted services
f. financial risks
g. reputational risks.

199. An organisation MUST assess the risks its supply chain poses to its operation.

GOV 5.1.a Principle 1: Understand what needs to be protected and why

200. To understand the risks that a supply chain contract may pose, organisations need to first understand the sensitivity, value, and impact of the information, services, and assets (including third-party services) that the supplier will have access to.

201. An organisation MUST know:

a. the sensitivity of contracts it lets or will let
b. the value of the information, services, or assets that suppliers hold, access, or handle as part of these contracts
c. the potential impact of loss or harm to information, services, or assets that suppliers hold, access, or handle (see INFOSEC1 and PHYSEC1 for more information.)

GOV 5.1.b Principle 2: Know who your suppliers are and understand their security measures

202. Organisations need to have confidence in their suppliers' and sub-contractors' security measures to ensure that they can meet the organisation's security requirements. This requires understanding the maturity and effectiveness of the supplier and sub-contractors' security arrangements.

203. An organisation MUST understand who its suppliers are, and who are their sub-contractors. Think about how far down your supply chain you need to go to understand who your suppliers are, and to have confidence in them.

204. An organisation MUST understand its suppliers' security measures by considering the following questions, with a focus on the parts of its suppliers' business or systems that handle the organisation's contracted information or assets or deliver the contracted products or services.

    a. How effective are the supplier's current security arrangements? How long have their arrangements been in place?
    b. Which security measures have you asked your immediate supplier to provide? Which measures have they, in turn, asked their sub-contractors to provide?
    c. Has the supplier and their sub-contractors provided the security requirements asked for?
    d. What access (physical and technological) will the supplier have to your systems, premises, and information? How will the organisation control that access?
    e. When the supplier works on the organisation's premises, what other information (beyond the information explicitly granted access to) might they be able to access or view?
    f. How will the immediate supplier control their subcontractors' access to, and use of, your information and assets? (Including the organisation's systems and premises).

205. An organisation SHOULD maintain ongoing visibility of the supplier's security risks.

GOV 5.1.c Principle 3: Understand the security risks posed by your supply chain

206. An organisation MUST assess the risks its contract arrangements pose to its information or assets, to the products or services to be delivered, and to the wider supply chain.

207. In line with GOV2, an organisation SHOULD incorporate supply chain risks into an organisation-wide risk assessment and management process (see GOV2 for more information).

GOV 5.2 Establish effective control and oversight of your supply chain

GOV 5.2.a Principle 4: Communicate your view of security needs to your suppliers

208. An organisation MUST ensure that its suppliers understand their responsibility to protect the organisation's information, and their products and services. Make sure they understand the implications of failure.

209. An organisation MUST define the conditions under which it is willing to let suppliers sub-contract work. In authorising sub-contracting, an organisation MUST:

    a. delegate authority appropriately to allow them to do so
    b. give suppliers clear guidance on the criteria for these decisions, including which types of contracts they can sub-contract without referring to you, and which types need your approval and sign-off.
    c. include your security requirements in any sub-contracting arrangements

GOV 5.2.b Principle 5: Set and communicate minimum security requirements for your suppliers

Specify security requirements to a supplier

210. An organisation MUST identify minimum-security requirements when developing tender documents, and for the life of the contract including when evaluating proposals or tenders.

211. An organisation MUST define the minimum-security requirements its suppliers need to meet for its assets and information as part of the contract, as well as the products or services they will deliver.

212. An organisation MUST ensure that the supplier's minimum-security requirements are justified, proportionate, and achievable, and cover:

    a. security governance
    b. personnel security
    c. information security
    d. physical security.

213. An organisation's minimum-security requirements for suppliers MUST:

    a. reflect the organisation's assessment of security risks, while also taking account of how well established your suppliers' security arrangements are, and their ability to meet your intended requirements
    b. be specific (a general condition in the contract that the service provider must comply with the PSR is unlikely to be appropriate or enforceable)
    c. identify and document circumstances where it might be disproportionate to expect suppliers to meet your minimum-security requirements (for example, suppliers who only need ad hoc or occasional access to limited and specific data, or to premises)
    d. outline the steps an organisation plans to take to manage its security requirements. This guidance could reduce workload and avoid additional unnecessary work for contractors.

214. In setting security requirements, an organisation SHOULD explain the rationale for them to the supplier and require the supplier to pass these requirements down to any sub-contractors.

215. An organisation SHOULD consider setting different security requirements for distinct types of contracts, based on their associated risks. Avoid forcing all your suppliers to deliver the same set of security requirements when it may not be proportionate or justified.

Personnel security

216. An organisation MUST:

    a. specify the minimum pre-employment screening checks that suppliers conduct for their personnel with access to the organisation's information, facilities, or assets
    b. ensure that the checks align with the baseline pre-employment checks conducted

by government organisations (see PERSEC 1)

c. consider on the basis of a risk assessment if the organisation should conduct the checks on behalf of the supplier.

217. An organisation SHOULD consider if additional checks are necessary due to an increased security risk related to a specific role or the nature of the access a supplier has. For example, an IT administrator for a managed service provider may have broad access to an organisation's information. Refer to PSR PERSEC policy framework for more information.

218. An organisation SHOULD consider if the supplier's personnel should sign a non-disclosure agreement. See example non-disclosure agreement for more information.

GOV 5.2.c Principle 6: Build security considerations into contracting process and require suppliers to do the same

219. An organisation MUST build security considerations into its contracting processes to help manage security throughout the contract, including terminating and transferring services to another supplier.

Before awarding a contract

220. As directed by Cabinet, an organisation MUST follow the New Zealand Government Rules for Procurement if mandated to do so.

221. An organisation MUST require prospective suppliers to provide evidence of their approach to security and their ability to meet the minimum-security requirements you have set.

222. If a supplier is unable to meet minimum-security requirements that could pose a threat to national security or the confidentiality of sensitive government information, an organisation SHOULD consider excluding the supplier from participating in a contract opportunity. See Rule 44 (Reasons to exclude a supplier) in the Government Rules for Procurement.

223. If an organisation awards a contract subject to a supplier meeting the security requirements, it MUST verify that these requirements are met before allowing their contract to start.

224. An organisation MUST consider including the right to terminate the contract if a supplier fails to comply with security requirements. Failure to comply includes the supplier being unwilling or unable to remedy security breaches.

225. An organisation SHOULD ensure that contracts clearly set out requirements for the return and deletion of the organisation's information and assets on termination or transfer of the contract.

During the contract

226. An organisation SHOULD require contracts to be renewed at appropriate intervals and reassess risks at the same time.

227. So that the organisation and their suppliers can effectively manage security at all levels throughout your supply chain, an organisation COULD:

a. provide or develop supporting guidance, tools, and processes
b. require their use in contracts
c. train all parties in their use.

Contract conditions

Conditions for classified government information at CONFIDENTIAL or above

228. When a contract involves access to material classified CONFIDENTIAL or above, an organisation MUST include conditions to:

    a. Explicitly identify the highest level of classified information the supplier will access during the contract.
    b. Require the supplier to ensure that all personnel with access to classified material must hold and maintain a relevant national security clearance and comply with all requirements defined in PERSEC 4.
    c. Where relevant, include conditions requiring the supplier to report to you when any of their personnel who do not have a security clearance have any incidental or accidental contact with classified material. This condition is particularly important in contracts for security guards, cleaning, and ICT services.

Conditions for government information

229. An organisation MUST include the following terms and conditions for government information.

Permission for sub-contracting

230. The supplier MUST not subcontract a service or function that may require access to government information without the organisation's written approval. Once a subcontracting agreement is in place, the service provider cannot change the subcontractor without the organisation's written approval.

Conflicts of interest

231. The supplier MUST disclose any potential conflicts of interest that would affect security when they work on behalf of the New Zealand Government.

Storing and handling protected information

232. The supplier's premises and facilities MUST meet the minimum standards for storing and handling government information, up to the nominated security classification level.

Information security

233. The supplier MUST meet the requirements for the return and deletion of the organisation's information and assets on termination or transfer of the contract,

234. The supplier SHOULD have systems that meet designated information security standards for processing, storing, transmitting, and disposing of government information that is in electronic formats. Refer to the NZISM for more information.

Confidentiality

235. The supplier MUST follow directions included in the contract for keeping government information confidential. Confidentiality obligations may extend beyond the end of the contract.

Conditions for your organisation's information

236. An organisation SHOULD consider legal and jurisdictional risk associated with a contract — such as where supplier's overseas owners or other stakeholders may have legal rights that could allow them access its information. If this is a risk, the contract SHOULD include terms and conditions to protect against third party access. However, in some cases these contractual conditions may not provide sufficient protection.

Conditions for business continuity

237. An organisation SHOULD consider including conditions relating to the assurance activities of suppliers and outsourcing partner's business continuity plans. These SHOULD include:

    a. that the third party has a business continuity programme
    b. the frequency in which they validate and assess their business continuity plans
    c. reporting requirements for assurance purposes.

GOV 5.2.d Principle 7: Meet your own security responsibilities as a consumer

238. When working with others, an organisation may function as a consumer of information, assets, premises, products, or services; or have shared responsibilities under legislation. It is important that an organisation can meet any security requirements placed on them by others. This includes requirements set in partnership, information-sharing, or co-tenancy agreements.

239. When requirements are placed on the organisation as a supplier or consumer of information, assets, premises, products, or services, an organisation MUST:

    a. Incorporate those requirements into the organisation's security obligations and plans
    b. Provide upward reporting to senior management
    c. Pass security requirements down to its suppliers and sub-contractors
    d. Enable audits and reviews
    e. Report any issues you encounter
    f. Work proactively with customers and partners to improve security.

GOV 5.2.e Principle 8: Raise awareness of security within your supply chain

240. Supplier relationships can interact with many of an organisation's touchpoints. It is important to educate people about how contracts will operate and what the associated security arrangements are.

241. An organisation MUST share security threats and risks with suppliers and request suppliers to explain the threats and risks to their people, so they know their responsibilities to help manage them.

242. A supplier's personnel may change over time due to personnel turnover or role changes. An organisation MUST ensure that a supplier's:

    a. personnel who access government or protectively-marked information are reminded of the continuing need to maintain confidentiality
    b. new personnel understand the organisation's security requirements.

243. An organisation MUST share security information across its supply chain to keep suppliers up to date with emerging security threats.

244. An organisation SHOULD consider establishing a supply chain security awareness and education programme. See GOV4 Build security awareness for more information.

GOV 5.2.f Principle 9: Provide support for security incidents

245. It is reasonable to expect suppliers to manage security risks according to their contracts. But an organisation should be prepared to provide support and assistance to suppliers if necessary. This includes when security incidents could potentially affect the organisation's operations or the wider supply chain.

246. An organisation MUST ensure that its contracts with suppliers clearly set out requirements for managing and reporting security incidents. This includes:

    a. The timescale for reporting the incident to the organisation, who to report to and how
    b. What support they can expect from the organisation during the incident including support for any required clean-up actions or handling losses.

247. An organisation SHOULD share lessons learned from security incidents with its suppliers, partners, and cooperating organisations to help improve resiliency across the entire supply chain and encourage them to do the same. Consider the 'need to know' when identifying what information to share.

248. An organisation MUST ensure that suppliers report incidents or suspected incidents that affect:

    a. Their ability to deliver their contracted services
    b. Your organisation's information (when they are holding or transporting it.)
    c. Any other security incidents that identify 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

GOV 5.3.a Principle 10: Build assurance activities into supply chain management

249. When suppliers are key to the security of your supply chain, an organisation MUST require them to:

    a. report to the contract manager at a minimum on security performance
    b. follow any risk management policies and processes the organisation specifies.

250. An organisation MUST build the 'right to audit' into all contracts, exercise this right, and require its suppliers to do the same for contracts they sub-let. Audits may include accessing the supplier's premises, records, and equipment. (However, this may not always be possible or desirable, particularly when a service is cloud-based.)

251. An organisation COULD consider building in an audit programme for suppliers' security capability to confirm their compliance with security requirements and effectiveness of measures.

252. Where justified, an organisation MUST build assurance requirements into its security

requirements. For example, assurance reporting, penetration tests, external audits, and formal security certifications.

253. To measure the performance of its supply chain security, an organisation SHOULD (see Assessing your supply chain security for examples of good and bad supply chain security):

    a. establish and monitor key performance indicators
    b. review and act on any findings and lessons learnt
    c. encourage suppliers to promote good security behaviours.

GOV 5.4 Continuous improvement

GOV 5.4.a Principle 11: Encourage the continuous improvement of security within your supply chain

254. An organisation SHOULD:

    a. encourage its suppliers to continuously improve their security arrangements.
    b. advise and support suppliers as they work on improvements.
    c. avoid creating unnecessary barriers to improvements. Be prepared to recognise any existing security practices or certifications they have that demonstrate how they meet the minimum-security requirements.
    d. allow time for the supplier to improve security but require them to give timescales and plans that show how they intend to achieve the improvements.
    e. Listen to and act on any concerns that suppliers highlight — concerns which suggest current approaches are not working. Suppliers might raise issues during performance monitoring, through reporting, or after responding to security incidents.

GOV 5.4.b Principle 12: Build trust with suppliers

255. An organisation SHOULD seek to build strategic partnerships with its key suppliers by:

    a. sharing issues with them and encouraging and valuing their input
    b. getting their buy-in to the organisation's approach to supply chain security so that they take account of their needs as well as yours
    c. letting them manage sub-contractors for you, but requiring them to report on their security performance
    d. maintaining regular and effective communication.

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.

256. A security incident is an event caused by an individual or group that has or could have resulted in loss or harm to an organisation's assets, information or people, or an action that breaches the organisation's security procedures. This may include:

    a. an attack or attempted attack against a computer or network
    b. an attempt or approach from anybody seeking unauthorised access to organisational resources, or
    c. any other occurrence that results, or may result, in negative consequences for the security of the organisation, New Zealand government, its institutions, or programmes.

257. Incident management is the process of identifying, recording, analysing, reporting, investigating, acting upon, and learning from incidents.

258. Security investigations establish the cause and extent of an incident that has, or could have, compromised your organisation or the New Zealand Government.

259. The process of investigating and reporting security incidents also helps an organisation understand its vulnerabilities and reduce the risk of future incidents.

GOV 6.1 Establish an effective approach to managing security incidents

GOV 6.1.a Follow a structured approach for security incident management

260. An organisation MUST have systems in place for managing security incidents. (Also see GOV2 for more information on requirements for security policies and procedures.) This includes:

    a. Ensuring that security incidents are detected and raised
    b. Recording, categorising, and assessing security incidents
    c. Reporting security incidents to relevant agencies
    d. Investigating, responding to, and managing security incidents
    e. Learning from security incidents.

261. An organisation MUST be able to categorise incidents based on severity.

GOV 6.1.b Establish policies and procedures for managing security incidents

262. An organisation MUST have formal policies and procedures for managing major security incidents.

263. An organisation SHOULD develop policies and procedures for managing minor security incidents.

264. An organisation SHOULD ensure the policies and procedures cover the roles and responsibilities involved in managing and responding to the security incident.

265. An organisation SHOULD set policy and procedures for investigating security incidents in line with the Privacy Act 2020, Employment Relations Act 2000, Protected Disclosures

Act 2022, and any other relevant legislation.

266. An organisation COULD monitor internal and external security environments for issues affecting the appropriate response to an incident and use this to inform improvements to responses

GOV 6.1.c Prepare and test your incident response readiness

267. An organisation SHOULD have a well-established security incident management plan for maintaining readiness and coordinating the response in the event of the major incident (See NCSC-Incident-Management-Be-Resilient-Be-Prepared guidance for more information and guidance on cyber-security related incidents):

    a. set of security actions and responses according to the incident scenario
    b. roles and responsibility matrix
    c. thresholds and procedures for leadership and other internal and external stakeholder notifications and escalations (including relevant government agencies)
    d. communication plan and message templates for notifying personnel
    e. interrelationships with changing threat levels, business continuity, and health and safety responses.

268. An organisation SHOULD conduct incident drills and exercises with its people to improve responses, policies, and processes.

GOV 6.2 Ensure that security incidents are detected and raised

269. When a security incident happens, an organisation needs to act quickly to reduce any impact and to recover as quickly as possible. Later it may also need to restore the confidence of any partners or clients affected by the incident.

GOV 6.2.a Require personnel to raise security incidents and make it easy for them to do so

270. An organisation MUST ensure that all personnel are required to raise security incidents, weaknesses, and threats as soon as possible.

271. An organisation MUST make it easy for staff to raise security incidents confidentially. This includes coverage in the organisation's security awareness training on:

    a. what a security incident is and when to report
    b. impacts of security incidents and why it is important to raise them
    c. consequences for not following security policies and procedures
    d. how to raise security incidents
    e. how to respond
    f. who to inform
    g. how the information will be dealt with (with sensitivity, confidentiality, and fairness).

272. An organisation COULD use collaboration tools and systems to ensure it is easy for people to understand how to report security concerns and actively engage in enhancing security measures.

GOV 6.2.b Establish mechanisms to quickly detect and respond to security incidents

273. An organisation SHOULD have mechanisms in place that ensure that it quickly detects potential security incidents including:

    a. Logging and monitoring of security related events
    b. Alerting of detected anomalous security events
    c. Automating security incident response where appropriate.

GOV 6.3 Record and assess security incidents

274. Recording security incidents gives valuable insights into an organisation's security environment and performance. For instance, repeated minor security incidents could be a symptom of poor personnel awareness and a need for more security awareness training.

GOV 6.3.a Implement methods for recording and assessing the impact of security incidents

275. An organisation MUST develop methods for recording and tracking incidents that suit your organisation's security environment and operations.

276. An organisation MUST assess the harm from any security incident to determine the impact on the organisation, New Zealand government, or other stakeholders.

277. An organisation SHOULD include the following information in security incident records:

    a. the time, date, and location
    b. the type of government resources involved
    c. a description of the incident's circumstances
    d. whether the incident was deliberate or accidental
    e. an assessment of the degree of compromise or harm
    f. a summary of immediate and long-term action you will take.

GOV 6.4 Report certain security incidents to relevant agencies

GOV 6.4.a Report certain security incidents to other agencies

278. An organisation MUST report to the appropriate agency any incidents of suspected:

    a. espionage (NZSIS, NZ Police, or both)
    b. sabotage (NZSIS, NZ Police, or both)
    c. acts of foreign interference (NZSIS)
    d. cyber-security attacks (NCSC)
    e. attacks on New Zealand's defence system (New Zealand Defence Force)
    f. politically motivated violence (NZSIS, NZ Police, or both)
    g. incitement to communal violence (NZSIS, NZ Police, or both)
    h. serious threats to New Zealand's border (NZ Customs Service, Immigration, and Ministry for Primary Industries).

279. As soon as possible, an organisation SHOULD first do an initial assessment of the harm and impact caused by the incident, then inform and follow advice of the relevant agency or agencies.

GOV 6.4.b Report security incidents involving holders of national security clearances

280. For national security clearance holders, an organisation MUST notify the New Zealand Security Intelligence Service (NZSIS) about:

    a. repeated minor security incidents
    b. major security incidents that relate to a person's suitability to hold a security clearance
    c. the outcome of any security investigation that relates to a person's suitability to hold a security clearance.

GOV 6.4.c Report certain cyber security incidents to the National Cyber Security Centre

281. An organisation MUST report certain information security incidents to the National Cyber Security Centre as set out in the NZISM. See NZISM Information Security Incidents for more information.

GOV 6.4.d Report security incidents involving Cabinet material to the Cabinet Office

282. An organisation MUST report suspected security incidents involving Cabinet material to the Cabinet Office in the Department of the Prime Minister and Cabinet.

283. The Cabinet Manual covers the security and handling of Cabinet documents.

GOV 6.4.e Report criminal incidents to law enforcement bodies

284. Where the incident may be a criminal offence, an organisation MUST report to the NZ Police for advice.

GOV 6.4.f Include these details when you report major security incidents

285. When reporting suspected major security incidents, an organisation MUST provide these details:

    a. the date and time of the incident, or when it was reported or discovered
    b. location
    c. brief details
    d. what may have been compromised (and the type and Business Impact Level (BIL), if relevant)
    e. the names of those involved in the incident if you know
    f. the name and contact details of the agency for follow-up
    g. an initial assessment of the harm or damage
    h. what action you have already taken.

286. Once a major incident has been reported, an organisation MUST report any updates and changes to the situation to the reported agency.

287. The reporting organisation is responsible for circulating information about incidents within their own organisation.

GOV 6.5 Investigate, respond to, and manage security incidents

GOV 6.5.a Investigate security incidents

288. A security incident can result in a security investigation, disciplinary action under a code

of conduct, and/or criminal investigation. An organisation MUST consider the timing and extent of which security incident information can be shared, and who with. Early engagement with HR/legal advice is essential.

289. Not all security incidents need to be investigated. Initial screening may identify security incidents that are not suitable for further investigation (e.g. minor and self-reported.) Where further investigation may be required, guidance can be sought from supporting agencies – the New Zealand Police, NZSIS, GCSB, New Zealand Defence Force, or other relevant agencies.

290. The purpose of a security investigation is to establish what has happened, what caused the incident, and how far it compromised or threatened the security of people, information, or assets. It is not to make or influence the decisions on any action to be taken.

291. A security investigation can result in a security outcome, disciplinary action under a code of conduct, and/or criminal investigation. An organisation MUST consider the timing and extent of which security incident information can be shared. Early engagement with HR is essential.

292. A security investigation SHOULD focus on establishing:

    a. the nature of the incident
    b. how the incident occurred (including the root cause)
    c. what circumstances led to the incident (including any trend analysis undertaken)
    d. who was involved
    e. the degree of damage to organisational and national security interests
    f. procedures needed to prevent a similar event or reduce its likelihood.

293. When undertaking any investigation and action against an employee, an organisation MUST follow a fair process, act in good faith, and use natural justice principles. This includes not jumping to conclusions before going through the process. Refer to Employment Investigations on Employment.govt.nz for more information.

294. An organisation COULD ensure that major security incident investigations are independently reviewed to confirm the investigation has been handled appropriately and fairly.

GOV 6.5.b Take interim measures while investigations are underway

295. In some circumstances it will be appropriate to take interim security measures while an investigation is underway. What is appropriate will be different in every case.

296. In applying interim measures an organisation MUST balance the need to protect its people, information, or assets with its employment obligations of natural justice. Early engagement with HR is essential to ensure this balance is achieved.

297. An organisation's interim measures MUST be justifiable and proportional to the concern held, and appropriately directed to protect any people, information, or assets potentially at risk.

298. An organisation SHOULD consider interim measures such as:

    a. conducting an audit of relevant information

b. monitoring computer usage
c. monitoring building access
d. limiting computer access
e. removing computer access
f. limiting after-hours access to place of work
g. removing access to a place of work (following decision to suspend having followed due process).

299. If relevant, an organisation SHOULD tell affected employees what interim measures are being taken, particularly where the employees remain in the workplace. Clearly explain:

a. What security measures are being taken
b. The measures are interim while the security investigation is ongoing
c. The interim measures do not signal predetermination.

GOV 6.5.c When appropriate, involve others in security investigations

300. When security incidents involve people, information, or assets from another organisation, an organisation SHOULD work with that organisation to investigate the incident. The other organisation may have operational security requirements, and it may be more appropriate for the originating or responsible organisation to investigate the incident. Apply the 'need-to-know' principle.

301. If an incident requires more than one type of investigation, an organisation SHOULD work with the other agency(ies) to determine priorities and an investigative approach.

GOV 6.6 Learn from security incidents

GOV 6.6.a Monitor and measure incident management effectiveness

302. An organisation SHOULD have processes for monitoring and measuring the types, volumes, and costs of security incidents. Use the information to:

a. identify recurring or high-impact problems
b. check whether you need more or better measures to limit problems
c. review the security policy.

GOV 6.6.b Conduct post-incident reviews when appropriate

303. An organisation MUST take corrective action in response to relevant incidents and put an improvement plan in place (e.g., conducting additional training or updating policies and procedures).

304. An organisation SHOULD establish when security incidents are subject to post-incident review to assess the effectiveness of incident management and response. This should include:

a. Conducting root cause analysis when appropriate
b. Reporting to security governance body on security incidents, the measures taken to remedy them, and outcomes from the actions taken
c. Confirming that all incidents were raised appropriately and followed good incident management processes
d. Incorporating findings into incident management plans, policies, and procedures

including addressing gaps in security culture, awareness, and training.

GOV 6.6.c Research incident management best practices and security trends

305. An organisation COULD conduct ongoing research into measures for preventing and managing incidents as part of its continuous improvement programme. This includes engaging with external experts.

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.

306. Be prepared to increase heightened security levels in emergencies or situations of increasing security risks.

307. Security alert levels communicate information about the security measures an organisation uses to reduce risks in emergency situations and other times of heightened risk. Alert levels also allow an organisation to scale its security measures, so they are appropriate to the type of incident and can change easily as risks increase or decrease.

GOV 7.1 Identify sources of risk for heightened security alert levels

308. Sources of security risks fall into three main categories:

    a. Event – an important happening or incident that affects the organisation's ability to function. Examples include a weather event such as a storm or an emergency event, such as an earthquake.
    b. Threat – a declared intent and capability to inflict harm on your people, information, or property. Examples include a cyber-threat or terrorism threat.
    c. Activity – an action by one or more people likely to have a negative impact on security. Examples include a protest activity, occupation, attempted occupation, or filming near the organisation's premises.

GOV 7.1.a Use internal and external sources of information to inform response planning

309. An organisation MUST be ready to respond to emergency and increased security risk situations by developing alert levels as identified as part of GOV2 (Take a risk-based approach) and GOV3 (prepare for business continuity.)

310. In developing alerts levels and plans for increasing and responding to heightened security alert levels, an organisation MUST seek information on risks from internal sources including:

    a. Security plans, risk assessments and risk management plan maintained as part of GOV2
    b. Business continuity plans developed as part of GOV3
    c. Post security incident reviews prepared as part of GOV6
    d. Security governance reports provided as part of GOV1, INFOSEC, PHYSEC, and PERSEC.

311. In developing alert levels and plans, an organisation SHOULD seek information on risks from external sources including any organisations it works, partners, or co locates with. Determine whether in such arrangements the other organisations have unique risk factors and how might they affect and integrate into the security alert response plans. Other examples of external sources of information include:

    a. National Emergency Management Agency (NEMA)

b. National terrorism threat level and associated assessment advice
c. Police, MetService, and Civil Defence advisories
d. National Cyber Security Centre (NCSC)
e. media reports.

GOV 7.2 Develop alert levels

312. Developing alert levels helps an organisation to apply security measures quickly before or during an incident. A quick response can increase the ability to protect people, information, and assets.

GOV 7.2.a Establish alert levels that address all types of emergency and security alerts

313. The number of alert levels to use depends on your operating environment and expected changes in your risk sources. Essential factors to consider are the nature of the organisation, the types of facilities it uses, its operational role, and its known risk levels. See **Security Governance Appendix C: Developing alert levels guidance** for more information.

314. An organisation MUST take an 'all hazards' approach to developing alert levels. That means including all types of threats from all sources, so you can generate a balanced response. Physical and environmental threats may have the same, or greater, impact on your organisation's ability to function as traditional security threats.

GOV 7.3 Plan your response during heightened security alerts

GOV 7.3.a Determine your security measures at different alert levels

315. An organisation MUST use its assessment of risk sources and operational requirements for each facility to work out which security measures are needed for each alert level. Several generic measures might be suitable at each alert level. For examples, see 'Operational security measures for alert levels'.

316. An organisation SHOULD work with local area managers and consult with its risk managers to develop procedures for each facility and risk source.

317. An organisation SHOULD aim for a balanced approach in designing security measures for alert levels:

a. Over-protection is costly, inefficient, and can be an obstacle. Over-protection is often caused by personal interpretation of the level of harm possible from a risk source or not having enough alert levels to allow staged escalation of measures appropriate to the increase in risk.
b. Under-protection can affect personal safety, and the security of your information and assets.

GOV 7.3.b Develop a plan for changing security alert levels

318. Developing a plan will help refine alert levels and associated security measures.

319. An organisation MUST establish a plan, criteria, and process for increasing security alert levels. This includes the criteria and process for returning to normal alert levels after a heightened event has concluded.

320. An organisation SHOULD consult the different business areas in your organisation when developing the plan for changing security alert levels.

321. An organisation SHOULD ensure that plans for moving up to heightened security alert levels are integrated and coordinated with other business continuity and emergency prevention and response plans, such as for fire, bomb threat, hazardous chemical spill, power failure, evacuation, or civil defence emergency.

322. An organisation SHOULD ensure that its plans are flexible to manage changing circumstances in real time.

GOV 7.4 Monitor the risk environment and change alert level when necessary

GOV 7.4.a Change alert levels when necessary

323. An organisation MUST be able to respond during emergencies or heightened security risk events and change (increase or decrease) the alert level to match any changes in risks.

324. An organisation MUST clearly and appropriately communicate all changes in alert level to its people, so that they know what has changed and what to do.

325. In considering how to communicate changes in alert levels and organisation SHOULD consider audiences, messages, methods, and responsibilities appropriately. Work with your communications team for expert advice.

GOV 7.4.b Debrief after changing alert levels

326. A debrief can be helpful for improving your response. An organisation SHOULD consider debriefing after changing alert levels covering:

    a. why the alert level change was initiated
    b. how the alert level change was initiated
    c. what activity and actions were undertaken for the alert level change
    d. what and where, if any, improvements could be made to alert level procedures and communications.

GOV 7.5 Review and update your processes

GOV 7.5.a Practice, review, and improve alert response processes

327. An organisation MUST practise and review the activation procedures for alert levels and the security measures for each level, to identify any gaps and update its plan.

328. An organisation SHOULD review its alert level processes:

    a. at least every two years
    b. when it takes on new projects
    c. as the risk environment changes
    d. after a significant incident that affects its ability to operate.

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 two years, or sooner if changes in the threat or operating environment make it necessary.

329. Ongoing improvement in protective security requires a cycle of assessing and managing risks in an ever-changing environment. By using a self-assessment cycle, the organisation can:

    a. identify needs for security measures
    b. evaluate the effectiveness of existing protective security practices
    c. prioritise and plan the focus areas and actions to take to improve protective security and effectively manage its security risks
    d. report back to Government on current capability and improvement plans.

GOV 8.1 Monitor and measure your protective security performance

330. An organisation MUST regularly monitor the performance of its protective security measures and plan, and report to its security governance body. The frequency and mechanisms for monitoring and reporting will depend on the level of risk that the organisation faces as defined in the organisation's security policies. See also GOV 2.3.d (Embed, measure, and improve security) for more information.

331. An organisation MUST monitor security practices to ensure they are generally repeatable, and results show that they are consistently followed within the organisation.

332. To measure the performance of its protective security plan and achievement of its goals, an organisation SHOULD:

    a. establish and monitor key performance indicators
    b. review historic performance information and act on any findings, trends, and lessons learnt
    c. promote good security behaviours.

333. An organisation COULD use continuous monitoring and spot checks to detect and prevent breakdowns in its security measures. This monitoring could be supported by automation in key high-risk areas.

334. An organisation COULD use performance indicators to inform both continuous improvement and real-time responses.

335. An organisation COULD ensure that its continuous improvement programme includes continuous monitoring and control with active contribution and management by relevant experts and service providers.

336. An organisation COULD ensure that protective security measures go beyond the enterprise to include all touch points with customers, partners, and suppliers.

GOV 8.2 Assess your protective security capability

337. An organisation MUST self-assess its protective security capability at least annually.

338. An organisation MUST assess how its capability maturity has changed as a result of changes in the environment such as when:

    a. key personnel have left the organisation
    b. technology has changed
    c. threat environment has changed
    d. resources assignments have changed.

339. An organisation MUST gather and use evidence in its assessment that demonstrates how well their security policies, processes, and measures achieve the objectives set out in the PSR to manage the risks that the organisation faces.

340. An organisation MUST ensure performance against security policies and procedures can be verified and are occasionally verified (audited).

341. An organisation SHOULD consider use of the following evidence types when assessing its capability (see PSR Evidence & Moderation Guide for detailed examples):

    a. risk management plan, threat assessments, and risk reporting
    b. documentation of policies, processes, and procedures
    c. compliance with policies, processes, and procedures
    d. security programme deliverables
    e. security incidents including infringements and breaches
    f. changes in security personnel and responsibilities
    g. security performance measures and reports
    h. personnel training, awareness programmes, and engagement surveys.

342. An organisation SHOULD involve others in the assessment representing various parts of the organisation, from executives to specialists and take them on the journey and use it as learning process that provides a good forum for balancing needs and priorities.

343. An organisation SHOULD use the PSR provided self-assessment tools, providing answers that best represents the organisation's current capability as demonstrated in the evidence gathered. See PSR self-assessment tool for more information.

344. An organisation COULD conduct effectiveness audits and use the findings to inform improvements.

GOV 8.3 Set your protective security goals for improvement

345. As part of GOV2, an organisation MUST understand its inherent security risks before establishing its security capability improvement goals. This will ensure that its protective security plan is right for the organisation. See PSR Threat and Risk Guidance for more information.

346. An organisation MUST use information from multiple sources to inform decisions and

planning that has been evaluated for relevance and reliability.

347. An organisation SHOULD set its goals for capability maturity in line with its risk exposure and risk tolerance. Consider the following points:

    a. The PSR provided self-assessment tool is designed to help organisations to identify and prioritise the gaps between inherent risk and current capability.
    b. Set goals that are realistic with what can be accomplished.
    c. Organisations face different types and levels of security risk, so targets need to reflect the specific strategic goals and priorities. One size does not fit all.
    d. For organisations new to the PSR framework, their goals will be quite different to organisations who have been on the protective security journey for multiple years. See **Security Governance Appendix D: PS-CMM improvement goals for organisations new to PSR**.

348. An organisation SHOULD periodically review and use historic performance information to inform where improvements should be made.

349. An organisation SHOULD have an annual proactive protective security programme that is planned, tracked and well managed and governed as well as resourced to maintain capability and maturity.

350. An organisation COULD ensure that protective security performance measures (goals) are set and aligned to organisational strategy and business goals.

351. An organisation COULD ensure security is a strategic issue for the organisation and protective security skills are continuously updated to ensure knowledge remains current.

352. An organisation COULD support continuous improvement programmes with real-time performance data and automated response mechanisms.

GOV 8.4 Provide assurance of your protective security capability and goals

353. An organisation MUST have an assurance process that provides its leaders and security governance body with confidence that:

    a. capability self-assessment is accurate
    b. capability gaps are known
    c. risk response measures and security plans are effective
    d. goals are appropriate to address its specific risks.

354. An organisation SHOULD use its risk and assurance function to provide internal or external independent and objective assurance on the accuracy of its PSR capability self-assessment and plans (e.g. conduct an effectiveness audit or independent moderation of protective security self-assessment results). See PSR Moderation Framework for more information.

355. The organisation SHOULD use independent oversight and assurance expertise to:

    a. confirm protective security performance;
    b. independently assess effectiveness of security measures;
    c. give expert advice and guidance to security personnel; and

d. provide assurance to the organisation head, security leaders, and security governance body that the right investments are being made to address protective security priorities.

356. An organisation COULD regularly audit the implementation and effectiveness of its security risk measures that are not subject to continuous monitoring.

357. An organisation COULD have a governance or audit committee provide independent oversight of the effectiveness and efficiency of its security plan.

GOV 8.5 Report on your protective security capability and improvement plans

358. An organisation MUST report regularly to its Chief Executive and security governance body on its security capability, goals, and plans.

359. Organisations mandated by Cabinet MUST report to the PSR Unit of the NZSIS, on their protective security capability and compliance with the mandatory requirements of the PSR. This reporting confirms that the organisation has:

a. undertaken an assessment against the protective security requirements
b. gathered the evidence to support the assessment
c. undertaken an independent assurance process to verify its findings and any moderation results
d. assessed where the organisation is at risk and set appropriate protective security goals to address its risks
e. established an effective plan to reach its goals and maintain the appropriate level of protective security capability based on its risk profile.

360. In the report submitted to PSR, an organisation MUST provide in detail:

a. Evidence that the capability / measure is in place and effective (e.g., how confirmed its effectiveness)
b. Risks, issues, and barriers experienced during the reporting period including security incidents, changes in personnel, and new threats or risks identified
c. Plans for improvement and risk response measures where capability is not sufficient to address the risk
d. Where residual risk has been accepted
e. Whether alternative measures are in place to address the specific risk that were not identified in the PSR. This will inform potential future PSR policy framework improvements.

361. Regular security reporting COULD be provided to senior leaders that supports strategic oversight and decisions to support a secure and effective workforce.