1.1. Understanding and using the NZISM

Objective

1.1.1. The New Zealand Information Security Manual details processes and controls essential for the protection of all New Zealand Government information and systems. Controls and processes representing good practice are also provided to enhance the baseline controls. Baseline controls are minimum acceptable levels of controls and are often described as "systems hygiene".

Context

Scope

1.1.2. The NZISM is intended for use by New Zealand Government departments, agencies and organisations. Crown entities, local government and private sector organisations are also encouraged to use the NZISM.

1.1.3. This section provides information on how to interpret the content and the layout of content within the NZISM.

1.1.4. Information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE or RESTRICTED is subject to a single set of controls in this NZISM. These are essential or minimum acceptable levels of controls (baseline controls) and have been consolidated into a single set for simplicity, effectiveness and efficiency.

1.1.5. All baseline controls will apply to all government systems, related services and information. In addition, information classified CONFIDENTIAL, SECRET or TOP SECRET has further controls specified in this NZISM.

1.1.6. Where the category "All Classifications" is used to define the scope of rationale and controls in the NZISM, it includes any information that is Official Information, UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET or any endorsements, releasability markings or other qualifications appended to these categories and classifications.

The purpose of this Manual

1.1.7. The purpose of the NZISM is to provide a set of essential or baseline controls and additional good and recommended practice controls for use by government agencies. The use or non-use of good practice controls MUST be based on an agency's assessment and determination of residual risk related to information security.

1.1.8. The NZISM is updated regularly. It is therefore important that agencies ensure that they are using the latest version of the NZISM.

Target audience

1.1.9. The target audience for the NZISM is primarily security personnel and practitioners within, or contracted to, an agency. This includes, but is not limited to:

- security executives;
- security and information assurance practitioners;
- IT Security Managers;
- Departmental Security Officers; and
- service providers.

Structure of this Manual

1.1.10. The NZISM seeks to present information in a consistent manner. There are a number of headings within each section, described below.

- Objective – the desired outcome when controls within a section are implemented.
- Context – the scope, applicability and any exceptions for a section.
- References – references to external sources of information that can assist in the interpretation or implementation of controls.
- Rationale & Controls
    - Rationale – the reasoning behind controls and compliance requirements.
    - Control – risk reduction measures with associated compliance requirements.

1.1.11. This section provides a summary of key structural elements of the NZISM. The detail of processes and controls is provided in subsequent chapters. It is important that reference is made to the detailed processes and controls in order to fully understand key risks and appropriate mitigations.

The New Zealand Government Security Classification System

1.1.12. The requirements for classification of government documents and information are based on the **Cabinet Committee Minute EXG (00) M 20/7** and **CAB (00) M42/4G(4)**. The Protective Security Requirements (PSR) INFOSEC2 require agencies to use the NZ Government Security Classification System and the NZISM for the classification, protective marking and handling of information assets. For more information on classification, protective marking and handling instructions, refer to the Protective Security Requirements, NZ Government Security Classification System.

Key definitions

Accreditation Authority

1.1.13. The Agency Head is generally the Accreditation Authority for that agency for all systems and related services up to and including those classified RESTRICTED. See also Chapter 3 – Roles and Responsibilities and Section 4.4 – Accreditation Framework.

1.1.14. Agency heads may choose to delegate this authority to a member of the agency's executive. The Agency Head remains accountable for ICT risks accepted and the information security of their agency.

1.1.15. In all cases the Accreditation Authority will be at least a senior agency executive who has an appropriate level of understanding of the security risks they are accepting on behalf of the agency.

1.1.16. For multi-national and multi-agency systems the Accreditation Authority is determined by a formal agreement between the parties involved. Consultation with the Office of the Government Chief Digital Officer (GCDO) may also be necessary.

1.1.17. For agencies with systems that process, store or communicate NZEO or information compartmented for national security reasons, the Director-General of the GCSB is the Accreditation Authority irrespective of the classification level of that information.

Certification and Accreditation Processes

1.1.18. Certification and accreditation of information systems is the fundamental governance process by which the risk owners and agency head derive assurance over the design, implementation and management of information systems and related services provided to or by government agencies. This process is described in detail in Chapter 4 – System Certification and Accreditation.

1.1.19. Certification and Accreditation are two distinct processes.

1.1.20. Certification is the formal assertion that an information system and related services comply with minimum standards and agreed design, including any security requirements.

1.1.21. *In all cases*, certification and the supporting documentation or summary of other evidence will be prepared by, or on behalf of, the host or lead agency. The certification is then provided to the Accreditation Authority.

1.1.22. Accreditation is the formal authority to operate an information system and related services, and requires the recognition and acceptance of associated risk and residual risks.

1.1.23. A waiver is NOT an exception (see below). A waiver is the formal acknowledgement that a particular compliance requirement of the NZISM cannot currently be met. A waiver is granted by the Accreditation Authority on the basis that full compliance with the NZISM is achieved or compensating controls are implemented within a time specified by the Accreditation Authority. Waivers are valid in the short term only and full accreditation cannot be granted until all conditions of the waiver have been met. The need for a waiver may occur when specified controls cannot be practically implemented because of technology, resource or other serious limitations. It is essential that risk is managed through the application of specified conditions.

1.1.24. An exception is NOT a waiver (see preceding paragraph). An exception is the formal acknowledgement that a requirement of the NZISM cannot be met and that a dispensation from the particular compliance requirement is granted by the Accreditation Authority. This exception is valid for the term of the Accreditation Certificate or some lesser time as determined by the Accreditation Authority. This may occur, for example, the system is to be in use for a very short time (usually measured in hours), or the requirement cannot be met and there is no viable alternative. It is essential that any consequential risk is acknowledged and appropriate measures are taken to manage any increased risk.

1.1.25. The requirements described above are **summarised** in the table below. Care MUST be taken when using this table as there are numerous endorsements, caveats and releasability instructions in the New Zealand Government Security Classification System that may change where the authority for accreditation lies.

Information Classification	MUST and MUST NOT controls	SHOULD and SHOULD NOT controls	Accreditation Authority
Information classified RESTRICTED and below, including UNCLASSIFIED and Official Information	Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high risk and mitigation is essential. If the control ***cannot*** be directly implemented, suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception from a specific requirement ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Control represents good and recommended practice. Non-use may be medium to high risk. Non-use of controls is formally recorded, compensating controls selected as required and residual risk acknowledged to be within the agency's risk appetite and formally agreed and signed off by the Accreditation Authority.	Agency Head/Chief Executive/Director General (or formal delegate)
All systems or services classified CONFIDENTIAL and above.	This is a baseline for any use of High Assurance Cryptographic Equipment (HACE) or the establishment of any compartments or the handling of any endorsed information (see below). The Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control ***cannot*** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception from a specific requirement ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	This is a baseline for any use of High Assurance Cryptographic Equipment (HACE) or the establishment of any compartments or the handling of any endorsed information (See below). Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority	Agency Head/Chief Executive/Director General (or formal delegate)
All use of High Assurance Cryptographic Equipment (HACE) **All systems or services with compartmented or caveated information classified CONFIDENTIAL and above.**	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Controls are baseline or "systems hygiene" controls and are essential for the secure use of a system or service. Non-use is high or very high risk and mitigation is essential. If the control ***cannot*** be directly implemented and suitable compensating controls MUST be selected to manage identified risks. The Accreditation Authority ***may*** grant a Waiver or Exception from a specific requirement ***if*** the level of residual risk is within the agency's risk appetite. Some baseline controls cannot be ***individually*** risk managed by agencies without jeopardising multi-agency, All-of-Government or international systems and related information.	Accreditation based on work conducted by the agency and authority to operate by the Agency Head. Control represents good and recommended practice. Non-use may be high risk Non-use of controls is formally recorded, compensating controls selected as required and residual risk formally acknowledged to be within the agency's risk appetite and agreed and signed off by the Accreditation Authority.	Director GCSB (or formal delegate)

"All Classifications" category

1.1.26. The "All Classifications" category is used to describe the applicability of controls for any information that is Official Information or protectively marked UNCLASSIFIED, IN-CONFIDENCE, SENSITIVE, RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET, including any caveats or releasability

endorsements associated with the respective document classification.

Compartmented Information

1.1.27. Compartmented information is information requiring special protection through separation or is "compartmented" from other information stored and processed by the agency.

Concept of Operations (ConOp) Document

1.1.28. Systems, operations, campaigns and other organisational activities are generally developed from an executive directive or organisational strategy. The ConOp is a document describing the characteristics of a proposed operation, process or system and how they may be employed to achieve particular objectives. It is used to communicate the essential features to all stakeholders and obtain agreement on objectives and methods. ConOps should be written in a non-technical language to facilitate agreement on understanding and knowledge and provide clarity of purpose. ConOp is a term widely used in the military, operational government agencies and other defence, military support and aerospace enterprises.

Information

1.1.29. The New Zealand Government requires information important to its functions, resources and classified equipment to be adequately safeguarded to protect public and national interests and to preserve personal privacy. Information is defined as any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation.

Information Asset

1.1.30. An information asset is any information or related equipment that has value to an agency or organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge.

Information Assurance (IA)

1.1.31. Confidence in the governance of information systems and that effective measures are implemented to manage, protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Security

1.1.32. Although sometimes described as cyber security, Information security is considered a higher level of abstraction than cyber security relating to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information".

1.1.33. A number of specialised security areas contribute to information security within government; these include: physical security, personnel security, communications security and information and communications technology (ICT) security along with their associated governance and assurance measures.

Information Systems

1.1.34. The resources and assets for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, and transmission of information. This includes necessary and related services provided as part of the information system, for example; Telecommunication or Cloud Services.

Information Systems Governance

1.1.35. An integral part of enterprise governance consists of the leadership and organisational structures and processes to ensure that the agency's information systems support and sustain the agency's and Government's strategies and objectives. Information Systems Governance is the responsibility of the Agency Head and the Executive team.

Secure Area

1.1.36. In the context of the NZISM a secure area is defined as any area, room, group of rooms, building or installation that processes, stores or communicates information classified CONFIDENTIAL, SECRET, TOP SECRET or any compartmented or caveated information at these classifications. A secure area may include a SCIF (see below). The physical security requirements for such areas are specified in the PSR Policy Framework - PHYSEC.

Security Posture

1.1.37. The Security Posture of an organisation describes and encapsulates the security status and overall approach to identification and management of

the security of an organisation's networks, information, systems, processes and personnel. It includes risk assessment, threat identification, technical and non-technical policies, procedures, controls and resources that safeguard the organisation from internal and external threats.

Sensitive Compartmented Information Facility (SCIF)

1.1.38. Any accredited area, room, or group of rooms, buildings, or installation where Sensitive Compartmented Information (SCI) is stored, used, discussed, processed or communicated. The Accreditation Authority for a SCIF is the Director GCSB or formal delegate.

System Owner

1.1.39. A System Owner is the **person** within an agency responsible for the information resource and for the maintenance of system accreditation. This may include such outsourced services such as telecommunications or cloud. Their responsibilities are described in more detail in Section 3.4 – System Owners.

Interpretation of controls

Controls language

1.1.40. The definition of controls in this manual is based on language as defined by the Internet Engineering Task Force (IETF)'s Request For Comment (RFC) 2119 to indicate differing degrees of compliance.

Applicability of controls

1.1.41. Whilst the NZISM provides controls for specific technologies, not all systems will use all of these technologies. When a system is developed, the agency will determine the appropriate scope of the system and which controls within this manual are applicable.

1.1.42. If a control within the NZISM is outside the scope of the system then non-compliance processes *do not apply*. However, if a control is within the scope of the system yet the agency chooses *not to implement* the control, then they are required to follow the non-compliance procedures as outlined below in order to provide appropriate governance and assurance.

1.1.43. The procedures and controls described in the NZISM are designed, not only to counter or prevent known common attacks, but also to protect from emerging threats.

Identification and Selection of controls

1.1.44. In all cases controls have been selected as the most effective means of mitigating identified risks and threats. Each control has been carefully researched and risk assessed against a wide range of factors, including useability, threat levels, likelihood, rapid technology changes, sustainability, effectiveness and cost.

Controls with a "MUST" or "MUST NOT" requirement

1.1.45. A control with a "MUST" or "MUST NOT" requirement indicates that use, or non-use, of the control is essential in order to effectively manage the identified risk, unless the control is demonstrably not relevant to the respective system. These controls are baseline controls, sometimes described as systems hygiene controls.

1.1.46. The rationale for non-use of baseline controls MUST be clearly demonstrated to the Accreditation Authority as part of the certification process, before approval for exceptions is granted. MUST and MUST NOT controls take precedence over SHOULD and SHOULD NOT controls.

Controls with a "SHOULD" or "SHOULD NOT" requirement

1.1.47. A control with a "SHOULD" or "SHOULD NOT" requirement indicates that use, or non-use, of the control is considered good and recommended practice. Valid reasons for not implementing a control could exist, including:

a. A control is not relevant in the agency;
b. A system or ICT capability does not exist in the agency; or
c. A process or control(s) of equal strength has been substituted.

1.1.48. While some cases may require a simple record of fact, agencies must recognise that non-use of any control, without due consideration, may increase residual risk for the agency. This residual risk needs to be agreed and acknowledged by the Accreditation Authority. In particular an agency should pose the following questions:

a. Is the agency willing to accept additional risk?
b. Have any implications for All-of-Government systems been considered?
c. If, so, what is the justification?

1.1.49. A formal auditable record of this consideration and decision is required as part of the IA governance and assurance processes within an agency.

Non-compliance

1.1.50. Non-compliance is a risk to the agency and may also pose risks to other agencies and organisations. Good governance requires these risks are clearly articulated, measures are implemented to manage and reduce the identified risks to acceptable levels, that the Accreditation Authority is fully briefed, acknowledges any residual and additional risk and approves the measures to reduce risk.

1.1.51. In some circumstances, full compliance with the NZISM may not be possible, for example some legacy systems may not support the configuration of particular controls. In such circumstances, a risk assessment should clearly identify *compensating* controls to reduce risks to an acceptable level. Acceptance of risk or residual risk, without due consideration is NOT adequate or acceptable.

1.1.52. It is recognised that agencies may not be able to immediately implement all controls described in the NZISM due to resource, budgetary, capability or other constraints. Good practice risk management processes will acknowledge this and prepare a timeline and process by which the agency can implement all appropriate controls described in the NZISM.

1.1.53. Simply acknowledging risks and not providing the means to implement controls *does not* represent effective risk management.

1.1.54. Where multiple controls are not relevant or an agency chooses not to implement multiple controls within the NZISM the system owner may choose to logically group and consolidate controls when following the processes for non-compliance.

Rationale Statements

1.1.55. A short rationale is provided with each group of controls. It is intended that this rationale is read in conjunction with the relevant controls in order to provide context and guidance.

Risk management

Risk Management Standards

1.1.56. For security risk management to be of true value to an agency it MUST relate to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization (ISO).

1.1.57. The International Organization for Standardization has published an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2018 - Risk Management - Guidelines. Refer to the tables below for additional reference materials.

The NZISM and Risk Management

1.1.58. The NZISM encapsulates good and recommended best-practice in managing technology risks and mitigating or minimising threat to New Zealand government information systems.

1.1.59. Because there is a broad range of systems across government and the age and technological sophistication of these systems varies widely, there is no single governance, assurance, risk or controls model that will accommodate all agencies information and technology security needs.

1.1.60. The NZISM contains guidance on governance and assurance processes and technological controls based on comprehensive risk and threat assessments, research and environmental monitoring.

1.1.61. The NZISM encourages agencies to take a similar risk-based approach to information security. This approach enables the flexibility to allow agencies to conduct their business and maintain resilience in the face of a changing threat environment, while recognising the essential requirements and guidance provided by the NZISM.

References

1.1.62. **Key Standards**

Reference	Title	Publisher	Source
NZISM	**New Zealand Information Security Manual**	GCSB	https://nzism.gcsb.govt.nz/
PSR	**Protective Security Requirements**	NZSIS	https://protectivesecurity.govt.nz
ISO/IEC 27000:2018	**Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary (fifth edition)**	ISO	https://www.iso.org/standard/73906.html
CNSS Instruction No. 4009 6 April 2015	**National Information Assurance (IA) Glossary, (US)**	Committee on National Security Systems (CNSS)	https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf [PDF, 1.04 MB]
NISTIR 7298 Revision 3, July 2019	**Glossary of Key Information Security Terms**	NIST	https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

1.1.63. **Additional Guidance**

Reference	Title	Publisher	Source
Approved Products			
ISO/IEC 15408-1:2009	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	ISO	https://www.iso.org/standard/50341.html
ISO/IEC 15408-2:2008	Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components	ISO	https://www.iso.org/standard/46414.html
ISO/IEC 15408-3:2008	Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components	ISO	https://www.iso.org/standard/46413.html
	AISEP Evaluated Products List	ASD	https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-evaluated-products
	Other Evaluated Products Lists	NSA NCSC UK CSEC Common Criteria	https://nsa.gov https://ncsc.gov.uk/ https://cse-cst.gc.ca https://commoncriteriaportal.org/products
Archiving of information			
	Public Records Act 2005 (as amended)	Archives New Zealand Parliamentary Counsel Office	https://archives.govt.nz https://legislation.govt.nz/
	Archives, Culture, and Heritage Reform Act 2000 (as amended)	Parliamentary Counsel Office	https://legislation.govt.nz/
Business continuity			
ISO 22301:2019	Security and Resilience - Business Continuity Management Systems - Requirements	ISO	https://www.iso.org/standard/75106.html
Cable security			
NZCSS 400	New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	CONFIDENTIAL document available on application to authorised personnel
Cryptographic Security			
NZCSP 301	New Zealand Communications Security Policy No 301 (Document classified RESTRICTED)	GCSB	RESTRICTED document available on application to authorised personnel
Emanation security			
NZCSS 400	New Zealand Communications Security Standard No 400 (Document classified CONFIDENTIAL)	GCSB	CONDFIDENTIAL document available on application to authorised personnel
Information classification			
	Protective Security Requirements (New Zealand Government Security Classification System Handling Requirements for protectively marked information and equipment)	NZSIS	https://protectivesecurity.govt.nz
Information security management			
ISO/IEC 27001:2013	Information technology — Security techniques — Information security management systems — Requirements	ISO	https://www.iso.org/standard/54534.html

ISO/IEC 27002:2022	Information security, cybersecurity, and privacy protection — Information security controls	ISO	https://www.iso.org/standard/75652.html
ISO/IEC 270xx series	Other standards and guidelines in the ISO/IEC 270xx series, as appropriate	ISO	https://www.iso.org/standards.html
Key management – commercial grade			
ISO/IEC 11770	ISO/IEC 11770 Parts 1-6: Information Technology – Security Techniques – Key Management	IS0	https://www.iso.org/standards.html
Management of electronic records that may be used as evidence			
ISO/IEC 27037:2012	Information Technology – Security Techniques - Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence	ISO	https://www.iso.org/standard/44381.html
Personnel security			
PSR	Protective Security Requirements	NZSIS	https://protectivesecurity.govt.nz/personnel-security/
Physical security			
PSR	Protective Security Requirements	NZSIS	https://protectivesecurity.govt.nz/physical-security/
Privacy requirements			
	Privacy Act 2020	Office of The Privacy Commissioner Parliamentary Counsel Office	https://privacy.org.nz https://legislation.govt.nz/
	Privacy advice, guidance and tools to help government agencies improve their privacy capability and maturity.	GCPO	https://digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/
Risk management			
ISO 31000:2018	Risk Management -- Guidelines	ISO	https://www.iso.org/standard/65694.html
ISO/IEC 27005:2018	Information technology — Security techniques — Information security risk management	ISO	https://www.iso.org/standard/75281.html
HB 436:2013	Risk Management Guidelines (Companion to withdrawn standard ISO 31000:2009)	Standards NZ	https://standards.govt.nz
ISO Guide 73:2009	Risk Management – Vocabulary – Guidelines for use in Standards	ISO	https://www.iso.org/standard/44651.html
NIST SP 800-30 rev. 1	Guide for conducting Risk Assessments	NIST	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [PDF, 807 KB]
Security Management			
HB 167:2006	Security Risk Management	Standards NZ	https://standards.govt.nz
Security And Intelligence Legislation			
	Intelligence and Security Act 2017	Parliamentary Counsel Office	https://legislation.govt.nz/
	Telecommunications (Interception Capability and Security) Act 2013 (as amended)	Parliamentary Counsel Office	https://legislation.govt.nz/

Rationale & Controls

Non-compliance

1.1.64.R.01.

Rationale

Controls for classified systems and information within the NZISM with a "MUST" or "MUST NOT" compliance requirement **cannot** be effectively *individually* risk managed by agencies without jeopardising their own, multi-agency or All-of-Government information assurance.

1.1.64.R.02. **Rationale**

Controls within the NZISM with a "SHOULD" and "SHOULD NOT" requirement may be risk managed by agencies. As the individual control security risk for non-compliance is not as high as those controls with a 'MUST' or 'MUST NOT' requirement, the Accreditation Authority can consider the justification for the acceptance of risks, consider any mitigations then acknowledge and accept any residual risks.

1.1.64.R.03. **Rationale**

Deviations from the procedures and controls in the NZISM may represent risks in themselves. It is important that governance and assurance is supported by evidence, especially where deviations from the procedures and controls in the NZISM are accepted. In this case a formal approval or signoff by the Accreditation Authority is essential. Ultimately, the Agency Head remains accountable for the ICT risks and information security of their agency.

1.1.64.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:127]

System owners seeking a dispensation for non-compliance with any baseline controls in the NZISM MUST be granted a dispensation by their Accreditation Authority. Where High Assurance Cryptographic Systems (HACS) are implemented, the Accreditation Authority will be the Director-General GCSB or a formal delegate.

Justification for non-compliance

1.1.65.R.01. **Rationale**

Without sufficient justification and consideration of security risks by the system owner when seeking a dispensation, the agency head or their authorised delegate will lack the appropriate range of information to the make an informed decision on whether to accept the security risk and grant the dispensation or not.

1.1.65.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:131]

System owners seeking a dispensation for non-compliance with baseline controls MUST complete an agency risk assessment which documents:

- the reason(s) for not being able to comply with this manual;
- the effect on any of their own, multi-agency or All-of-Government system;
- the alternative mitigation measure(s) to be implemented;
- The strength and applicability of the alternative mitigations;
- an assessment of the residual security risk(s); and
- a date by which to review the decision.

Consultation on non-compliance

1.1.66.R.01. **Rationale**

When an agency stores information on their systems that belongs to a foreign government they have an obligation to inform and seek agreement from that third party when they do not apply all appropriate controls in the NZISM. These third parties will place reliance on the application of controls from the NZISM. If the agency fails to implement all appropriate controls, the third party will be unaware that their information may have been placed at a heightened risk of compromise. As such, the third party is denied the opportunity to consider their own additional risk mitigation measures for their information in light of the agency's desire to risk manage controls from the NZISM.

1.1.66.R.02. **Rationale**

Most New Zealand Government agencies will store or processes information on their systems that originates from another New Zealand Government Agency. The use of the NZ Government Security Classification System, and implementation of its attendant handling instructions, provides assurance to the originating agency that the information is adequately safeguarded.

1.1.66.R.03. **Rationale**

Additional controls, not described or specified in the NZISM, are welcomed as a means of improving and strengthening security of information systems, provided there are no obvious conflicts or contradictions with the controls in the NZISM. A comprehensive risk assessment of the additional controls is a valuable means of determining the effectiveness of additional controls.

1.1.66.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:137]

If a system processes, stores or communicates classified information from another agency, that agency MUST be consulted before a decision to be non-compliant with the NZ Government Security Classification System is made.

1.1.66.C.02.

Control System Classifications(s): All Classifications; Compliance: Must [CID:138]

If a system processes, stores or communicates classified information from a foreign government, that government MUST be consulted before a decision to be non-compliant with NZISM controls is made.

All-of-Government Systems

1.1.67.R.01. **Rationale**

All-of-Government systems, because they are connected to multiple agencies, have the potential to cause significant and widespread disruption should system failures, cyber-attacks or other incidents occur.

1.1.67.R.02. **Rationale**

Any deviation from the baseline controls specified in the NZISM MUST be carefully considered and their implication and risk for all government systems understood and agreed by all interested parties.

1.1.67.R.03. **Rationale**

Interested parties may include the lead agency, the Government CIO and key service providers, such as with cloud services.

1.1.67.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:143]

If a system processes, stores or communicates data and information with multiple agencies or forms part of an All-of-Government system, interested parties MUST be formally consulted before non-compliance with any baseline controls.

Reviewing non-compliance

1.1.68.R.01. **Rationale**

As part of the process of providing justification for a dispensation to the Accreditation Authority, an assessment of the degree of compliance, identification of areas of non-compliance and determination of residual security risk is undertaken by the agency or lead agency. This assessment is based on the risk environment at the time the dispensation is sought. As the risk environment will continue to evolve over time it is important that agencies revisit the assessment on an annual basis and update it according to the current risk environment, and if necessary reverse any decisions to grant a dispensation if the security risk is no longer of an acceptable level.

1.1.68.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:146]

Agencies SHOULD review decisions to be non-compliant with any controls at least annually.

Recording non-compliance

1.1.69.R.01. **Rationale**

Without appropriate records of decisions to risk manage controls from the NZISM, agencies have no record of the status of information security within their agency. Furthermore, a lack of such records will hinder any governance, compliance or auditing activities that may be conducted.

1.1.69.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:151]

Agencies MUST retain a copy and maintain a record of the supporting risk assessment and decisions to be non-compliant with any baseline controls from the NZISM.

1.1.69.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:152]

Where good and recommended practice controls are NOT implemented, agencies MUST record and formally recognise that non-use of any controls without due consideration may increase residual risk for the agency. This residual risk MUST be agreed and acknowledged by the Accreditation Authority.