1.2. Applicability, Authority and Compliance

Objective

1.2.1. Agencies understand and follow the requirements of the New Zealand Information Security Manual (NZISM). Protection of government information and systems is a core accountability.

Context

Scope

1.2.2. The NZISM provides guidance and specific ICT controls that form part of a suite of requirements produced by GCSB relating to information security. Its role is to promote a consistent approach to information assurance and information security across all New Zealand Government agencies. It is based on security risk assessments for any information that is processed, stored or communicated by government systems with corresponding risk treatments (control sets) to reduce the level of security risk to an acceptable level.

Applicability

1.2.3. The NZISM applies to information and systems operated by, or on behalf of:

- New Zealand Government departments, agencies and organisations as listed in:
  - Parts 1 and 2 of Schedule 1 to the Ombudsmen Act 1975 (as amended); and
  - Schedule 1 to the Official Information Act 1982.
- any other organisations that have entered into a formal Agreement with the New Zealand Government to have access to classified information.

Authority

1.2.4. The Intelligence and Security Act 2017 provides that one of the functions of the GCSB is to co-operate with, and provide advice and assistance to, any public authority whether in New Zealand or overseas, or to any other entity authorised by the Minister responsible for the GCSB on any matters relating to the protections, security and integrity of communications; and information structures of importance to the Government of New Zealand. The NZISM is one aspect of the GCSB's advice and assistance to government agencies on information security.

1.2.5. This function furthers the objective of the GCSB to contribute to:

- The national security of New Zealand; and
- The international relations and well-being of New Zealand; and
- The economic well-being of New Zealand.

1.2.6. The NZISM is intended to structure and assist the implementation of government policy that requires departments and agencies to protect the privacy, integrity and confidentiality of the information they collect, process, store and archive. While these overarching requirements are mandatory for departments and agencies, compliance with the NZISM is not required as a matter of law. The controls in the NZISM could be made binding on departments and agencies, either by legislation, or Cabinet direction.

1.2.7. The Protective Security Requirements Framework provides a specific authority and mandate through a Cabinet Directive **CAB MIN (14) 39/38.**

1.2.8. The NZISM is published by the Government Chief Information Security Officer (GCISO). See 2.1.20 for more information about the GCISO. The GCISO mandate:

- confirms the GCISO's ability to set information security standards for GCISO mandated agencies;
- clarifies the expectation for the GCISO to set assurance activities, and develop assurance methodologies, to meet standards and guidelines;
- confirms GCISO access to information security investment information (along with joint System Leads for Data and Digital) from GCISO mandated agencies, including baseline spending; and
- confirms the expectation of the GCISO to provide investment advice and guidance to the government on cyber security matters for the public sector.

1.2.9. Agencies mandated under the GCISO authority are those set out as mandated agencies in the Protective Security Requirements.

Compliance by smaller agencies

1.2.10. As smaller agencies may not always have sufficient staffing or budgets to comply with all the requirements of the NZISM, they may choose to consolidate their resources with another larger host agency to undertake a joint approach.

1.2.11. In such circumstances smaller agencies may choose to either operate on systems fully hosted by another agency using their information security policies and information security resources or share information security resources to jointly develop information security policies and systems for use by both agencies. The requirements within the NZISM can be interpreted as either relating to the host agency or to both agencies, depending on the approach taken.

1.2.10. In situations where agencies choose a joint approach to compliance, especially when an agency agrees to fully host another agency, the agency heads may choose to seek a memorandum of understanding regarding their information security responsibilities.

Legislation and other government policy

1.2.13. Agencies should rely on their own inquiries. While the NZISM does contain examples of relevant legislation (see table 1.1.63), there is no comprehensive consideration of legislation.

1.2.14. All controls within the NZISM may be used as the basis for internal and external annual audit programmes, any review or investigation by the Controller and Auditor-General or referenced for assurance purposes by the Government Chief Digital Officer (GCDO).

Rationale & Controls

Compliance

1.2.15.R.01. **Rationale**

In complying with the latest version of the NZISM agencies awareness of the current threat environment for government systems and the associated acceptable level of security risk is vital. Furthermore, if a system is designed to an out-dated standard, agencies may need additional effort to obtain accreditation for their systems.

1.2.15.R.02. **Rationale**

GCSB continuously monitors technology developments in order to identify business risks, technology risks and security threats. If a significant risk is identified, research may be undertaken, additional controls identified and implementation timeframes specified.

1.2.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:177]

Agencies undertaking system design activities for in-house or out-sourced projects MUST use the latest version of the NZISM for information security requirements.

1.2.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:178]

When GCSB makes a determination that newly introduced standard, policy or guideline within the NZISM, or any additional information security policy, is of particular importance, agencies MUST comply with any new specified requirements and implementation timeframes.