4.4. Accreditation Framework

Objective

4.4.1. Accreditation is the formal authority for a system to operate, and an important element in fundamental information system governance. Accreditation requires risk identification and assessment, selection and implementation of baseline and other appropriate controls and the recognition and acceptance of residual risks relating to the operation of a system including any outsourced services such as Telecommunications or Cloud. Accreditation relies on the completion of system certification procedures.

Context

Scope

4.4.2. This section covers information on the accreditation framework for systems.

4.4.3. All types of government held information are covered, including Official Information and information subject to privacy requirements.

Rationale & Controls

Accreditation framework

4.4.4.R.01. **Rationale**

The development of an accreditation framework within the agency will ensure that accreditation activities are conducted in a repeatable and consistent manner across the agency and that consistency across government systems is maintained. This requirement is a fundamental part of a robust governance model and provides a sound process to demonstrate good governance of information systems.

4.4.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:595]

Agencies MUST develop an accreditation framework for their agency.

Accreditation

4.4.5.R.01. **Rationale**

Accreditation ensures that either sufficient security measures have been put in place to protect information that is processed, stored or communicated by the system or that deficiencies in such measures have been identified, assessed and acknowledged by an appropriate authority. As such, when systems are awarded accreditation the Accreditation Authority accepts that the residual security risks relating to the system are appropriate for the information that it processes, stores or communicates.

4.4.5.R.02. **Rationale**

Once systems have been accredited, conducting on-going monitoring activities will assist in assessing changes to its environment and operation and to determine the implications for the security risk profile and accreditation status of the system.

4.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:599]

Agencies MUST ensure that each of their systems is awarded accreditation.

4.4.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:600]

Agencies MUST ensure that all systems are awarded accreditation before they are used operationally.

4.4.5.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:601]

Agencies MUST ensure that all systems are awarded accreditation prior to connecting them to any other internal or external system.

4.4.5.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:602]

Agencies SHOULD ensure information security monitoring, logging and auditing is conducted on all accredited systems.

Determining authorities

4.4.6.R.01. **Rationale**

Determining the certification and accreditation authorities for multi-national and multi-agency systems via a formal agreement between the parties will ensure that the system owner has identified appropriate points of contact and that risk is appropriately managed. See Section 4.5 – Conducting Accreditations.

4.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:605]

For multi-national and multi-agency systems, the Certification and Accreditation Authorities SHOULD be determined by a formal agreement between the parties involved.

Notifying authorities

4.4.7.R.01. **Rationale**

In advising the certification and accreditation authorities of their intent to seek certification and accreditation for a system, the system owner can request information on the latest processes and requirements for their system.

4.4.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:608]

Prior to beginning the accreditation process the system owner SHOULD advise the certification and accreditation authorities of their intent to seek certification and accreditation for their system.

4.4.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:609]

Agencies SHOULD confirm governance arrangements with the certification authorities, and with the accreditation authorities.

Due diligence

4.4.8.R.01. **Rationale**

When an agency is connecting a system to another party they need to be aware of the security measures the other party has implemented to protect their information. More importantly, the agency needs to know where the other party may have varied from controls in this manual. This is vital where different classification systems are applied, such as in the use of multiple national classification systems.

4.4.8.R.02. **Rationale**

Methods that an agency may use to ensure that other agencies and third parties comply with the agency's information security expectations include:

- assurance and confirmation that the certification and accreditation process described in the NZISM is adhered to;
- conducting or utilising any third party reviewed assurance reports;
- conducting an accreditation of the system being connected to; and/or
- seeking a copy of existing accreditation deliverables in order to make their own accreditation determination.

4.4.8.R.03. **Rationale**

Ultimately, the agency MUST accept any security risks associated with connecting their system to the other party's system. This includes the risks of other party's system potentially being used as a platform to attack their system or "spilling" information requiring subsequent clean up processes.

4.4.8.R.04. **Rationale**

Special care MUST be taken for multi- national, multi-agency and All-of-Government systems.

4.4.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:615]

Where an agency's system exchanges information with a third-party system, the agency MUST ensure that the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification or privacy requirements of their information and that the third party is authorised to receive that information.

4.4.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:616]

An agency MUST ensure that a third party is aware of the agency's information security expectations and national security requirements by defining expectations in documentation that includes, but is not limited to:

- contract provisions;
- a memorandum of understanding;
- non-disclosure agreements.

4.4.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:617]

An agency MUST ensure that a third party complies with the agency's information security expectations through a formal process providing assurance to agency management that the operation of information security within the third party meets, and continues to meet, these expectations.

4.4.8.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:618]

Agencies SHOULD review accreditation deliverables when determining whether the receiving party has appropriate measures in place to provide a level of protection commensurate with the classification of their information.

Processing restrictions

4.4.9.R.01. **Rationale**

When security is applied to systems, protective measures are put in place based on the highest classification that will be processed, stored or communicated by the system. As such, any classified information placed on the system above the level for which it has been accredited will receive an inappropriate level of protection and could be exposed to a greater risk of compromise.

4.4.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:621]

Agencies MUST NOT allow a system to process, store or communicate classified information above the classification for which the system has received accreditation.

Accrediting systems bearing a compartment marking

4.4.10.R.01. **Rationale**

When processing compartmented information on a system, agencies need to ensure that the system has received accreditation.

4.4.10.R.02. **Rationale**

Compartments are invariably established for the additional protection of information of National security significance, over and above the protection provided by the primary classification. It is extremely unlikely that such compartments would be established at a classification below CONFIDENTIAL.

4.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:624]

A system that processes, stores or communicates compartmented information MUST be accredited by the GCSB.

Requirement for New Zealand control

4.4.11.R.01. **Rationale**

NZEO systems process, store and communicate information that is particularly sensitive to the government of New Zealand. When agencies are dealing with New Zealand Eyes Only (NZEO) information they need to be aware of the requirement for a New Zealand national to remain in control of the system and information at all times. It is, therefore, essential that control of such systems is maintained by New Zealand citizens working for the government of New Zealand.

4.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:627]

Agencies MUST ensure that systems processing, storing or communicating NZEO information remain under the control of a New Zealand national working for the New Zealand government, at all times.

Reaccreditation

4.4.12.R.01. **Rationale**

Agencies should reaccredit their systems at least every two years; however, they can exercise an additional one year's grace if they follow the procedures in this manual for non-compliance with a 'SHOULD' requirement, namely conducting a comprehensive security risk assessment, obtaining sign-off by senior management and formal acceptance of residual risk.

4.4.12.R.02. **Rationale**

Accreditations should be commenced at least six months before due date to allow sufficient time for the certification and accreditations processes to be completed. Once three years has elapsed between accreditations, the authority to operate the system (the accreditation) will lapse and the agency will need to either reaccredit the system or request a dispensation to operate without accreditation. It should be noted that operating a system without accreditation is considered extremely risky. This will be exacerbated when multiple agency or All-of-Government systems are involved.

4.4.12.R.03. **Rationale**

Additional reasons for conducting reaccreditation activities could include:

- changes in the agency's information security policies or security posture;
- detection of new or emerging threats to agency systems;
- the discovery that controls are not operating as effectively as planned;
- a major information security incident; and
- a significant change to systems, configuration or concept of operation for the accredited system.

4.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:632]

Agencies MUST ensure that the period between accreditations of each of their systems does not exceed three years.

4.4.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:633]

Agencies MUST notify associated agencies where multiple agencies are connected to agency systems operating with expired accreditations.

4.4.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:634]

Agencies MUST notify the Government Chief Digital Officer (GCDO) where All-of-Government systems are connected to agency systems operating with expired accreditations.

4.4.12.C.04. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:635]

Agencies MUST NOT operate a system without accreditation or with a lapsed accreditation unless the accreditation authority has granted a dispensation.

4.4.12.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:636]

Agencies SHOULD ensure that the period between accreditations of each of their systems does not exceed two years.