3.2. The Chief Information Security Officer

Objective

3.2.1. The Chief Information Security Officer (CISO) sets the strategic direction for information security within their agency.

Context

Scope

3.2.2. This section covers the role of a CISO with respect to information security within an agency.

Appointing a CISO

3.2.3. The requirement to appoint a member of the Senior Executive Team or an equivalent management position, to the role of CISO does not require a new dedicated position be created in each agency.

3.2.4. The introduction of the CISO role and associated responsibilities is aimed at providing a more meaningful title for a subset of the security executive's responsibilities that relate to information security within their agency.

3.2.5. The CISO should bring accountability and credibility to information security management and appointees should be suitably qualified and experienced.

3.2.6. Where multiple roles are held by the CISO, conflicts of interest may occur particularly where operational imperatives conflict with security requirements. Good governance and assurance practices separates these roles. Where multiple roles are held by an individual, potential conflicts of interest should be clearly identified and a mechanism implemented to allow independent decision making in areas where conflict can occur.

PSR references

3.2.7. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV1, GOV3, GOV4, GOV8, INFOSEC1, INFOSEC2, INFOSEC4, PERSEC1, PERSEC2, PERSEC3, and PERSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements
PSR requirements sections	Self-assessment & reporting Protective security roles & responsibilities	Self-assessment and reporting | Protective Security Requirements Roles and responsibilities | Protective Security Requirements

Rationale & Controls

Requirement for a CISO

3.2.8.R.01. **Rationale**

The role of the CISO is based on industry and governance good practice, and relevant international standards, and has been introduced to ensure that information security is managed at the senior executive level within agencies. Without a CISO there is a risk that an agency may not be resourced to effectively manage information security.

3.2.8.R.02. **Rationale**

The CISO within an agency is responsible predominately for facilitating communications between security personnel, ICT personnel and business personnel to ensure alignment of business and security objectives within the agency.

3.2.8.R.03. **Rationale**

The CISO is also responsible for providing strategic level guidance for the agency security program and ensuring compliance with national policy, standards, regulations and legislation.

3.2.8.R.04. **Rationale**

Where multiple roles are held by the CISO, potential conflicts of interest should be identified and carefully managed so the agency is not disadvantaged.

3.2.8.R.05. **Rationale**

Conflicts of interest may also be apparent where the agency outsources the CISO function and that CISO deals with other vendors and organisations. In particular required availability, response times and related operational criteria should be identified and carefully managed to ensure the agency is not disadvantaged.

3.2.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:307]

The CISO MUST be:

- cleared for access to all classified information processed by the agency's systems, and
- able to be briefed into any compartmented information on the agency's systems.

3.2.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:308]

Agencies SHOULD appoint a person to the role of CISO or have the role undertaken by an existing person within the agency.

3.2.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:309]

The CISO role SHOULD be undertaken by a member of the Senior Executive Team or an equivalent management position.

3.2.8.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:310]

The CISO SHOULD be responsible for overseeing the management of security personnel within the agency.

3.2.8.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:311]

Where multiple roles are held by the CISO any potential conflicts of interest SHOULD be identified and carefully managed.

Responsibilities – Reporting

3.2.9.R.01. **Rationale**

As the CISO is responsible for the overall management of information security within an agency it is important that they report directly to the agency head on any information security issues.

3.2.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:314]

The CISO SHOULD report directly to the agency head on matters of information security within the agency.

Responsibilities – Security programs

3.2.10.R.01. **Rationale**

Without a comprehensive strategic level information security and security risk management program an agency will lack high-level direction on information security issues and may expose the agency to unnecessary risk.

3.2.10.R.02. **Rationale**

Working with system owners, assessors and accreditors will facilitate the determination of appropriate information security policies consistent with agency strategies, the requirements of the PSR and in particular the NZISM.

3.2.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:317]

The CISO SHOULD develop and maintain a comprehensive strategic level information security and security risk management program within the agency aimed at protecting the agency's official and classified information.

3.2.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:318]

The CISO SHOULD be responsible for the development of an information security communications plan.

3.2.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:319]

The CISO SHOULD create and facilitate the agency security risk management process.

3.2.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7084]

The CISO SHOULD work with system owners, system certifiers and system accreditors to determine appropriate information security policies for their systems and ensure consistency with the Protective Security Requirements (PSR) and in particular the relevant NZISM components.

Responsibilities – Ensuring compliance

3.2.11.R.01. **Rationale**

Without having a person responsible for ensuring compliance with the information security policies and standards within the agency, security measures of the agency are unlikely to meet minimum government requirements and may expose the agency to unnecessary risk.

3.2.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:322]

The CISO SHOULD be responsible for establishing mechanisms and programs to ensure compliance with the information security policies and standards within the agency.

3.2.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:323]

The CISO SHOULD be responsible for ensuring agency compliance with the NZISM through facilitating a continuous program of certification and accreditation of all agency systems.

3.2.11.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:324]

The CISO SHOULD be responsible for the implementation of information security measurement metrics and key performance indicators within the agency.

Responsibilities – Coordinating security

3.2.12.R.01. **Rationale**

One of the core roles of the CISO is to ensure appropriate communication between business and information security teams within their agency. This includes interpreting information security concepts and language into business concepts and language as well as ensuring that business teams consult with information security teams to determine appropriate security measures when planning new business projects for the agency.

3.2.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:327]

The CISO SHOULD facilitate information security and business alignment and communication through an information security steering committee or advisory board which meets formally and on a regular basis, and comprises key business and ICT executives.

3.2.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:328]

The CISO SHOULD be responsible for coordinating information security and security risk management projects between business and information security teams.

3.2.12.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:329]

The CISO SHOULD work with business teams to facilitate security risk analysis and security risk management processes, including the identification of acceptable levels of risk consistently across the agency.

Responsibilities – Working with ICT projects

3.2.13.R.01. **Rationale**

As the CISO is responsible for the development of the strategic level information security program within an agency they are best placed to advise ICT projects on the strategic direction of information security within the agency.

3.2.13.R.02. **Rationale**

As the CISO is responsible for the overall management of information security within an agency, they are best placed to recommend to the accreditation authority the acceptance of residual security risks associated with the operation of agency systems.

3.2.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:333]

The CISO SHOULD provide strategic level guidance for agency ICT projects and operations.

3.2.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:334]

The CISO SHOULD liaise with agency technology architecture teams to ensure alignment between security and agency architectures.

Responsibilities – Working with vendors

3.2.14.R.01. **Rationale**

Having the CISO coordinate the use of external information security resources will ensure that a consistent approach is being applied across the agency.

3.2.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:337]

The CISO SHOULD coordinate the use of external information security resources to the agency including contracting and managing the resources.

Responsibilities – Budgeting

3.2.15.R.01. **Rationale**

Controlling the information security budget will ensure that the CISO has sufficient access to funding to support information security projects and initiatives.

3.2.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:341]

The CISO SHOULD be responsible for controlling the information security budget.

Responsibilities – Information security incidents

3.2.16.R.01. **Rationale**

To ensure that the CISO is able to accurately report to the Agency Head on information security issues within their agency, it is important that they remain fully aware of all information security incidents within their agency.

3.2.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:345]

The CISO SHOULD be fully aware of all information security incidents within the agency.

Responsibilities – Disaster recovery

3.2.17.R.01. **Rationale**

Restoring business-critical services to an operational state after a disaster is an important function of business continuity. As such it will need high level support from the CISO.

3.2.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:348]

The CISO SHOULD coordinate the development of disaster recovery policies and standards within the agency to ensure that business-critical services are supported appropriately and that information security is maintained in the event of a disaster.

Responsibilities – Training

3.2.18.R.01. **Rationale**

To ensure personnel within an agency are actively contributing to the information security posture of the agency, an information security awareness and training program will need to be developed. As the CISO is responsible for information security within the agency they will need to oversee the development and operation of the program.

3.2.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:351]

The CISO SHOULD be responsible for overseeing the development and operation of information security awareness and training programs within the agency.

Responsibilities – Providing security knowledge

3.2.19.R.01.

Rationale

The CISO is not expected to be a technical expert on all information security matters; however, knowledge of national and international standards and good practice will assist in communicating with technical experts within their agency on information security matters

3.2.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:354]

The CISO SHOULD provide authoritative security advice and have familiarity with a range of national and international standards and good practice.