PSR | Protective Security Requirements

National Cyber Security Centre

# Chief Information Security Officer

## Ensures information security within an organisation is managed at the executive level

As the Chief Information Security Officer (CISO), you will have a good knowledge and understanding of information technology and its associated security risks.

The CISO position may be:

- an individual role assigned at a senior level
- part of a portfolio
- outsourced to a third party virtual Chief Information Security Officer (vCISO)

The CISO is one of many key security roles within an organisation including CSO, and COMSO. As the CISO, it is important you have a direct line to senior and executive leaders to provide free and frank advice. An organisation's executive will always retain responsibility to accept residual risk.

## Key responsibilities

Strengthening information security capability and culture will enable your organisation to function more effectively and better manage risk.

Security is everyone's responsibility — but as the CISO, you have additional responsibilities:

- Develop and maintain a strategic information security programme
- Ensure that your organisation complies with the relevant standards and regulations for information security as well as government and internal policies
- Facilitate communication between security, information technology, and business teams to ensure security objectives are aligned
- Oversee the creation and ongoing implementation of an information security awareness and training programme
- Provide strategic level information security guidance for your organisation, including projects and operations
- Ensure external information security resources and vendors are well managed
- Identify acceptable levels of risk across the organisation and ensure risk is calculated consistently across your organisation
- Work with teams in your organisation to help them understand their information security risks and ensure these risks are owned and managed
- Contribute to disaster recovery policies and standards within your organisation to ensure business-critical assets and services are supported, and that your information remains secure in the event of a disaster

## Working with the Government Chief Information Security Officer

The Government Chief Information Security Officer (GCISO) has an important relationship with organisation CISOs.

The GCISO provides advice, support, and guidance through a range of channels including the New Zealand Information Security Manual (NZISM) and the National Cyber Security Centre (NCSC).

### New Zealand Information Security Manual

New Zealand Government's risk-based manual on information assurance and information systems security. It explains processes and defines risk treatments (controls) essential for protecting New Zealand Government information systems and communications.

Setup a generic email (eg ciso@*yourorg*.govt.nz) for your CISO and send it to gciso@gcsb.govt.nz to receive information security updates

## CISO in action: a case study

Your organisation uses on-premise assets for data storage and processing that can no longer support its requirements. Consequently, the organisation has decided to migrate to cloud services for its critical operations.

- Your job as the CISO is to ensure the migration is secure, compliant, and doesn't expose the organisation to unnecessary risk.

To do this, you:

☑ identify business-critical assets

☑ establish a risk management framework that connects cyber security with your agency's overall risk appetite and business operations

☑ understand the potential impact of a breach on your organisation's business goals

☑ prioritise security measures accordingly.

All systems must go through a certification process that involves providing evidence that due consideration has been given to risk and security.

As the Certification Authority, you are responsible for providing a recommendation to the Accreditation Authority on whether to accept residual risk associated with the operation of the system.

Frameworks such as CSF, NIST, ISO27001, or CIS Controls will help guide your policies and practices, and ensure compliance with industry standards.

March 2025 1.0

**ncsc.govt.nz**
info@ncsc.govt.nz

**protectivesecurity.govt.nz**
psr@protectivesecurity.govt.nz