Information security guidance for

Project Managers

This guide is for project managers working on ICT projects that need to meet New Zealand Government Information Security standards, regulations, and policies.

These requirements may include, but are not limited to:

- The New Zealand Information Security Manual (NZISM)
- The Protective Security Requirements (PSR)
- Public Records Act 2005
- Official Information Act 1982
- Electronic Transactions Act 2002
- Privacy Act 1993

Agencies responsible for these standards and policies include:

- Government Communications Security Bureau (GCSB);
- National Cyber Security Centre (NCSC);
- Government Chief Digital Officer (GCDO), Department of Internal Affairs (DIA);
- Government Chief Digital Steward (GCDS); Statistics New Zealand;
- Government Chief Privacy Officer (GCPO); Department of Internal Affairs (DIA);
- New Zealand Security Intelligence Service (NZSIS)

Each of these agencies has a different mandate and interest in ICT arrangements. Each can also provide advice and guidance on compliance with their particular areas of interest.

Project lifecycle

Traditional project lifecycles have various stages, each of which has critical implications for information security. These stages also correspond to various points in the INFOSEC lifecycle.[1]

Initiation

- Requires the identification and articulation of a business need.
- Is the ideal point to begin work to understand and assess the information associated with the business and the proposed project.

Planning

- Is the opportunity to formally determine milestones, dependencies, and deliverables.
- Should involve risk assessment, research of relevant standards, and setting out delivery requirements.
- Includes practical design of layered information security measures.
- Requires acceptance of design and sign off on planning.

Execution

- Involves the practical implementation of information security measures.
- Should ensure secure supply chains throughout.
- Validates and tests information security measures.
- Monitors any changes in scope and technology. Revise assessment of risks, relevant standards, and delivery requirements as necessary.

Closure

- Examines information received through monitoring and evaluation measures.
- Reviews and assesses project success.
- Finalises reporting.

Feedback on policies and standards:

If you have feedback on standards, policies, or guidance that GCSB is responsible for please email us at info@ncsc.govt.nz.

If you have feedback on the NZISM specifically please email ism@gcsb.govt.nz

[1] Further on INFOSEC at https://www.protectivesecurity.govt.nz/information-security/