Information Security Lifecycle

Understand

Understand the information you need to protect, it's value to your organisation and the business impact of loss or compromise to inform your security requirements.

You should understand how the information will be used, shared and stored both in your organisation or by your providers / partners. You also need to consider your confidentiality, integrity, privacy and legislative requirements..

Assess

Assess the risks to your information, and supporting ICT systems, to enable you to identify security measures to reduce those risks to an acceptable level.

You need to identify the security threats and vulnerabilities relevant to your information. Analysing your existing security measures and the likelihood and impact of each risk will let you evaluate where further action is required.

Design

Design fit-for-purpose security measures that are proportionate to the risks identified and in line with your organisation's risk appetite.

Consider relevant standards (e.g. NZISM). Make sure you consider third party suppliers and the role they play. Factor security requirements into your business continuity / disaster recovery requirements

Accept the security design
The responsible executive (normally the CISO) accepts that the proposed security design is fit for purpose.

Implement

Implement the agreed security measures including policies, processes, procedures and technical security controls.

Retire

When your information, and supporting ICT systems, are no longer required they need to be archived/ destroyed/repurposed or disposed in an appropriately secure way.

Make sure you consider appropriate legislation including the Public Records Act and the Archives Act.

Validate

Validate that the risk mitigations and security controls identified in your design have been correctly implemented and are fit-for- purpose.

For ICT systems this requires a formal certification and accreditation process that includes independent technical validation.

Certification
The CISO, or other delegate, accepts that due consideration has been paid to risk, security, functionality and business requirements.

Respond
Identify and respond to security incidents or breaches. See "Incident Management" Infographic.

Review

Undertake regular reviews to ensure your security measures remain fit-for-purpose. Identify changes in your information use, your organisation or the threat environment. Use this information to inform improvements.

Operate & Maintain

Staying secure requires going activity to keep up to date with evolving security threats, vulnerabilities and mitigations. Make sure your security controls are kept up to date and remain fit for purpose.

Go Live

Accreditation
The agency head, or their delegate, gives approval to operate and accepts any residual risks

PSR | Protective Security Requirements

www.protectivesecurity.govt.nz/information