5.4. System Security Plans

Objective

5.4.1. System Security Plans (SSPs) specify the information security measures for systems.

Context

Scope

5.4.2. This section relates to the development of SSPs. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

5.4.3. Further information to be included in SSPs relating to specific functionality or technologies that could be implemented for a system can be found in the applicable areas of this manual.

Stakeholders

5.4.4. There can be many stakeholders involved in defining a SSP including representatives from the:

- project, who MUST deliver the capability (including contractors);
- owners of the information to be handled;
- system users for whom the capability is being developed;
- management audit authority;
- CISO, ITSM and system owners;
- system certifiers and accreditors;
- information management planning areas; and
- infrastructure management.

Rationale & Controls

Contents of System Security Plans (SSPs)

5.4.5.R.01. **Rationale**

The NZISM provides a list of controls that are potentially applicable to a system based on its classification, its functionality and the technology it is implementing. Agencies will need to determine which controls are in scope of the system and translate those controls to the SSP. These controls will then be assessed on their implementation and effectiveness during an information security assessment as part of the accreditation process.

5.4.5.R.02. **Rationale**

In performing accreditations against the latest baseline of this manual, agencies are ensuring that they are taking the most recent threat environment into consideration. GCSB continually monitors the threat environment and conducts research into the security impact of emerging trends. With each release of this manual, controls can be added, rescinded or modified depending on changes in the threat environment.

5.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:828]

Agencies MUST select controls from this manual to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP. Encryption Key Management requires specific consideration; refer to Chapter 17 – Cryptography.

5.4.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:829]

Agencies SHOULD use the latest baseline of this manual when developing, and updating, their SSPs as part of the certification, accreditation and reaccreditation of their systems.

5.4.5.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:831]

Agencies SHOULD include a Key Management Plan in the SSP.