5.3. Security Risk Management Plans

Objective

5.3.1. Security Risk Management Plans (SRMP) identify security risks and appropriate treatment measures for systems.

Context

Scope

5.3.2. This section relates to the development of SRMPs, focusing on risks associated with the security of systems. Information relating to other mandatory documentation can be found in Section 5.1 - Documentation Fundamentals.

5.3.3. SRMPs may be developed on a functional basis, systems basis or project basis. For example, where physical elements will apply to all systems is use within that agency, a single SRMP covering all physical elements is acceptable. Generally each system will require a separate SRMP.

5.3.4. The agency's risk identification and assessment process should include:

- How risks are found, recognised and described; and
- How sources of possible risks are to be considered.

References

5.3.5. Information on the development of SRMPs can be found in:

Reference	Title	Publisher	Source
HB 436:2013	**Risk management guidelines - Companion to AS/NZS ISO 31000:2009**	Standards NZ	https://standards.govt.nz/
ISO 22301:2019	**Business Continuity**	ISO	https://www.iso.org/standard/75106.html
ISO 31000:2018	**Risk Management - Guidelines**	ISO	https://www.iso.org/standard/65694.html
IEC 31010:2019	**Risk Management – Risk Assessment Techniques**	ISO	https://www.iso.org/standard/72140.html
ISO Guide 73:2009	**Risk Management - Vocabulary**	ISO	https://www.iso.org/standard/44651.html
ISO 19011:2018	**Guidelines for auditing management systems**	ISO	https://www.iso.org/standard/70017.html
ISO/IEC 27000:2018	**Information technology - Security techniques - Information security management systems - Overview and vocabulary**	ISO	https://www.iso.org/standard/73906.html
ISO/IEC 27001:2013	**Information technology - Security techniques - Information security management systems - Requirements**	ISO	https://www.iso.org/standard/54534.html
ISO/IEC 27005:2018	**Information Security Risk Management**	ISO	https://www.iso.org/standard/75281.html
ISO/IEC 27006:2015	**Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems**	ISO	https://www.iso.org/standard/62313.html
ISO/IEC 27007:2020	**Information technology - Security techniques - Guidelines for information security management systems auditing**	ISO	https://www.iso.org/standard/77802.html
ISO/IEC TS 27008:2019	**Information technology - Security techniques - Guidelines for the assessment of information security controls**	ISO	https://www.iso.org/standard/67397.html
ISO/IEC 27017:2015	**Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services**	ISO	https://www.iso.org/standard/43757.html
ISO/IEC 27018:2019	**Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors**	ISO	https://www.iso.org/standard/76559.html

Rationale & Controls

Agency and system specific security risks

5.3.6.R.01. **Rationale**

While a baseline of security risks with associated levels of security risk and corresponding risk treatments are provided in this manual, agencies will almost certainly have variations to those considered during the security risk assessment. Such variations could be in the form of differing risk sources and threats, assets and vulnerabilities, or exposure and severity. In such cases an agency will need to follow its own risk management procedures to determine its risk appetite and associated risk acceptance, risk avoidance and risk tolerance thresholds. Risk owners must be identified.

5.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:802]

Agencies SHOULD determine agency and system specific security risks that could warrant additional controls to those specified in this manual.

Contents of SRMPs

5.3.7.R.01. **Rationale**

Risks within an agency cannot be managed if they are not known, and if they are known, failing to treat or accept them is also a failure of risk management. For this reason SRMPs consist of two components, a security risk assessment and a corresponding treatment strategy.

5.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:805]

The Security Risk Management Plan SHOULD contain a security risk assessment and a corresponding treatment strategy.

Agency risk management

5.3.8.R.01. **Rationale**

If an agency fails to incorporate SRMPs for systems into their wider agency risk management plan then the agency will be unable to manage risks in a coordinated and consistent manner across the agency.

5.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:808]

Agencies SHOULD incorporate their SRMP into their wider agency risk management plan.

Risk Management standards

5.3.9.R.01. **Rationale**

For security risk management to be of true value to an agency there must be direct relevance to the specific circumstances of an agency and its systems, as well as being based on an industry recognised approach or risk management guidelines. For example, guidelines and standards produced by Standards New Zealand and the International Organization for Standardization.

The Protective Security Requirements requires that agencies adopt risk management approaches in accordance with ISO 31000:2018. Refer to PSR governance requirement GOV2.

5.3.9.R.02. **Rationale**

The International Organization for Standardization has developed an international risk management standard, including principles and guidelines on implementation, outlined in ISO 31000:2018, Risk Management – Guidelines. The terms and definitions for this standard can be found in ISO/IEC 31073:2022, Risk Management – Vocabulary. The ISO/IEC 2700x series of standards also provides guidance.

5.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:812]

Agencies SHOULD develop their SRMP in accordance with international standards for risk management.