5.1. Documentation Fundamentals

Objective

5.1.1. Information security documentation is produced for systems, to support and demonstrate good governance.

Context

Scope

5.1.2. This section is an overview of the information security documentation that each agency will need to develop. More specific information on each document can be found in subsequent sections of this chapter.

5.1.3. While this section describes a number of different but essential documents, it may be more advantageous and efficient to provide agency wide documentation for some elements (for example Physical Security) which can then be re-used for all agency systems.

5.1.4. Similarly some consolidation may be appropriate, for example, SOPs IRPs and EPs can easily be combined into a single document.

Note: For smaller agencies and smaller systems it is acceptable that all documentation elements are combined into a single document provided each documentation element is clearly identifiable.

Note: Agencies may choose to name the documentation in different terms. This is acceptable provided the required level of detail is captured. Naming conventions presented in the NZISM are not mandatory.

Information Security Documentation

5.1.5. Information Security Documentation requirements are summarised in the table below.

Title	Abbreviation	Reference
Information Security Policy (incorporates the vulnerability disclosure policy)	SecPol VDP	5.1.7 5.9
Systems Architecture	-	5.1.8
Security Risk Management Plan	SRMP	5.1.9
System Security Plan	SSP	5.1.10
Site Security Plan	SitePlan	8.2.7
Standard Operating Procedures	SOPs	5.1.11
Incident Response Plan	IRP	5.1.12
Emergency Procedures	EP	5.1.13
Independent Assurance reports for externally provided services	-	5.8

PSR references

5.1.6. Additional information on third party providers is provided in the PSR.

Reference	Title	Source
PSR Mandatory Requirements	GOV4, GOV5, INFOSEC1, INFOSEC2, PERSEC1, PERSEC2, PERSEC3 and PERSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Personnel security (PERSEC) | Protective Security Requirements

Rationale & Controls

Information Security Policy (SecPol)

5.1.7.R.01. **Rationale**

The SecPol is an essential part of information security documentation as it outlines the high-level policy objectives. The SecPol can form part of the overall agency security policy.

5.1.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:692]

Agencies MUST have a SecPol for their agency. The SecPol is usually sponsored by the Chief Executive and managed by the CISO or Chief Information Officer (CIO). The ITSM should be the custodian of the SecPol. The SecPol should include an acceptable use policy for any agency technology equipment, systems, resources and data.

Systems Architecture

5.1.8.R.01. **Rationale**

The systems architecture illustrates the design of the system (including any outsourced services), consistency with the SecPol and provides the basis for the Security Risk Management Plan (SRMP).

5.1.8.R.02. **Rationale**

In this context Systems Architecture includes Security Architecture.

5.1.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:696]

All systems MUST have a documented Systems Architecture.

Security Risk Management Plan (SRMP)

5.1.9.R.01. **Rationale**

The SRMP is considered to be a good practice approach to identifying and reducing identified security risks. Depending on the documentation framework chosen, multiple systems can refer to, or build upon, a single SRMP.

5.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:699]

Agencies MUST ensure that every system is covered by a Security Risk Management Plan, which includes identification of risk owners.

System Security Plan (SSP)

5.1.10.R.01. **Rationale**

The SSP describes the implementation and operation of controls within the system derived from the NZISM and the SRMP. Depending on the documentation framework chosen, some details common to multiple systems can be consolidated in a higher level SSP.

5.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:702]

Agencies MUST ensure that every system is covered by a SSP.

Standard Operating Procedures (SOPs)

5.1.11.R.01. **Rationale**

SOPs provide step-by-step guides to undertaking information security related tasks and processes. They provide assurance that tasks can be undertaken in a secure and repeatable manner, even by system users without strong technical knowledge of the system's mechanics. Depending on

the documentation framework chosen, some procedures common to multiple systems could be consolidated into a higher level SOP.

5.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:705]

Agencies MUST ensure that Standard Operating Procedures (SOPs) are developed for systems.

Incident Response Plan (IRP)

5.1.12.R.01. **Rationale**

The purpose of developing an IRP is to ensure that information security incidents are appropriately managed. In most situations the aim of the response will be to contain the incident and prevent the information security incident from escalating. The preservation of any evidence relating to the information security incident for criminal, forensic and process improvement purposes is also an important consideration.

5.1.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:708]

Agencies MUST develop an Incident Response Plan and supporting procedures.

5.1.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:709]

Agency personnel MUST be trained in and periodically exercise the Incident Response Plan.

Emergency Procedures (EP)

5.1.13.R.01. **Rationale**

Classified information and systems are secured if a building emergency or evacuation is required.

5.1.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:712]

Agencies SHOULD document procedures relating to securing classified information and systems when required to evacuate a facility in the event of an emergency.

Developing content

5.1.14.R.01. **Rationale**

Ensuring personnel developing information security documentation are sufficiently knowledgeable of information security issues and business requirements will assist in achieving the most useful and accurate set of documentation.

5.1.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:715]

Agencies SHOULD ensure that information security documentation is developed by personnel with a good understanding of policy requirements, the subject matter, essential processes and the agency's business and operations

Documentation content

5.1.15.R.01. **Rationale**

As the SRMP, Systems Architecture, SSP, SOPs and IRP are developed as a documentation suite for a system it is essential that they are logically connected and consistent within themselves and with other agency systems. Furthermore, each documentation suite developed for a system will need to be consistent with the agency's overarching SecPol.

5.1.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:718]

Agencies SHOULD ensure that their SRMP, Systems Architecture, SSP, SOPs and IRP are logically connected and consistent for each system, other agency systems and with the agency's SecPol.

Documentation framework

5.1.16.R.01. **Rationale**

The implementation of an overarching information security document framework ensures that all documentation is accounted for, complete and maintained appropriately. Furthermore, it can be used to describe linkages between documents, especially when higher level documents are used to avoid repetition of information in lower level documents.

5.1.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:721]

Agencies SHOULD create and maintain an overarching document describing the agency's documentation framework, including a complete listing of all information security documentation that shows a document hierarchy and defines how each document is related to the other.

5.1.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:722]

Where an agency lacks an existing, well-defined documentation framework, they SHOULD use the document names defined in this manual.

Documentation Consistency

5.1.17.R.01. **Rationale**

Consistency in approach, terminology and documentation simplifies the use and interpretation of documentation for different systems and agencies.

5.1.17.R.02. **Rationale**

Factors which should be taken into account when determining the classification of systems documentation include:

- Highest classification of information stored, processed or communicated over that system;
- Sensitivity including existence of the facility;
- Inclusion of vulnerability information, security mechanisms or special processing capability in the systems documentation;
- Potential data aggregation;
- Risk and threat levels; and
- Scope and use of the system.

5.1.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:726]

Where an agency uses alternative documentation names to those defined within this manual for their information security documentation they SHOULD convert the documentation names to those used in this manual.

Documentation Classification

5.1.18.R.01. **Rationale**

Systems documentation will usually reflect the importance or sensitivity of particular systems.

5.1.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:729]

Agencies MUST ensure that their SecPol, SRMP, SSP, SOPs and IRP are appropriately classified.

Outsourcing development of content

5.1.19.R.01. **Rationale**

Agencies outsourcing the development of information security documentation need to be aware of the contents of the documentation produced. As such, they will still need to review and control the documentation contents to make sure it is appropriate and meets their requirements.

5.1.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:732]

When information security documentation development is outsourced, agencies SHOULD:

- review the documents for suitability;
- retain control over the content; and
- ensure that all policy requirements are met.

Obtaining formal sign-off

5.1.20.R.01. **Rationale**

Without appropriate sign-off of information security documentation within an agency, the security personnel will have a reduced ability to ensure appropriate security procedures are selected and implemented. Having sign-off at an appropriate level assists in reducing this security risk as well as ensuring that senior management is aware of information security issues and security risks to the agency's business.

5.1.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:735]

All information security documentation SHOULD be formally approved and signed off by a person with an appropriate level of seniority and authority.

5.1.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:736]

Agencies SHOULD ensure that:

- all high-level information security documentation is approved by the CISO and the agency head or their delegate; and
- all system-specific documents are reviewed by the ITSM and approved by the system owner.

Documentation Maintenance

5.1.21.R.01. **Rationale**

The threat environment and agencies' businesses are dynamic. If an agency fails to keep their information security documentation up to date to reflect the changing environment, they do not have a means of ascertaining that their security measures and processes continue to be effective.

5.1.21.R.02. **Rationale**

Changes to risk and technology may dictate a reprioritisation of resources in order to maximise the effectiveness of security measures and processes.

5.1.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:767]

Agencies SHOULD develop a regular schedule for reviewing all information security documentation.

5.1.21.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:768]

Agencies SHOULD ensure that information security documentation is reviewed:

- at least annually; or
- in response to significant changes in the environment, business or system; and
- with the date of the most recent review being recorded on each document.