6.1. Information Security Reviews

Objective

6.1.1. Information security reviews maintain the security of agency systems and detect gaps and deficiencies.

Context

Scope

6.1.2. This section covers information on conducting reviews of any agency's information security posture and security implementation.

Information security reviews

6.1.3. An information security review:

- identifies any changes to the business requirements or concept of operation for the subject of the review;
- identifies any changes to the security risks faced by the subject of the review;
- assesses the effectiveness of the existing counter-measures;
- validates the implementation of controls and counter-measures; and
- reports on any changes necessary to maintain an effective security posture.

6.1.4. An information security review can be scoped to cover anything from a single system to an entire agency's systems.

References

6.1.5. Additional information relating to system auditing is contained in:

Reference	Title	Publisher	Source
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 security, cybersecurity and privacy protection — 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

PSR references

6.1.6. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements
PSR requirements sections	Self-assessment & reporting Protective security measures	Self-assessment and reporting | Protective Security Requirements Complying with the Protective Security Requirements | Protective Security Requirements

Rationale & Controls

Conducting information security reviews

6.1.7.R.01. **Rationale**

Annual reviews of an agency's information security posture can assist with ensuring that agencies are responding to the latest threats, environmental changes and that systems are properly configured in accordance with any changes to information security documentation and guidance.

6.1.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1040]

Agencies SHOULD undertake and document information security reviews of their systems at least annually.

Managing Conflicts of Interest

6.1.8.R.01. **Rationale**

Reviews may be undertaken by personnel independent of the target of evaluation or by an independent third party to ensure that there is no (perceived or actual) conflict of interest and that an information security review is undertaken in an objective manner.

6.1.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1043]

Agencies SHOULD have information security reviews conducted by personnel independent to the target of the review or by an independent third party.

Focus of information security reviews

6.1.9.R.01. **Rationale**

Incidents, significant changes or an aggregation of minor changes may require a security review to determine and support any necessary changes and to demonstrate good systems governance. An agency may choose to undertake an information security review:

- as a result of a specific information security incident;
- because a change to a system or its environment that significantly impacts on the agreed and implemented system architecture and information security policy; or
- as part of a regular scheduled review.

6.1.9.R.02. **Rationale**

In order to review risk, an information security review should analyse the threat environment and the highest classification of information that is stored, processed or communicated by that system.

6.1.9.R.03. **Rationale**

Depending on the scope and subject of the information security review, agencies may gather information on areas including:

- agency priorities, business requirements and/or concept of operations;
- threat data;

- risk likelihood and consequence estimates;
- effectiveness of existing counter-measures;
- other possible counter-measures;
- changes to standards, policies and guidelines;
- recommended good practices; and
- significant system incidents and changes.

6.1.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1048]

Agencies SHOULD review the components detailed in the table below. Agencies SHOULD also ensure that any adjustments and changes as a result of any vulnerability analysis are consistent with the vulnerability disclosure policy.

Component	Review
Information security documentation	The SecPol, Systems Architecture, SRMPs, SSPs, SitePlan, SOPs, the VDP, the IRP, and any third party assurance reports.
Dispensations	Prior to the identified expiry date.
Operating environment	When an identified threat emerges or changes, an agency gains or loses a function or the operation of functions are moved to a new physical environment.
Procedures	After an information security incident or test exercise.
System security	Items that could affect the security of the system on a regular basis.
Threats	Changes in threat environment and risk profile.
NZISM	Changes to baseline or other controls, any new controls and guidance.