6.3. Change Management

Objective

6.3.1. To ensure information security is an integral part of the change management process, it should be incorporated into the agency's IT maintenance governance and management activities.

Context

Scope

6.3.2. This section covers information on identifying and managing routine and urgent changes to systems.

Identifying the need for change

6.3.3. The need for change can be identified in various ways, including:

- system users identifying problems or enhancements;
- vendors notifying of upgrades to software or IT equipment;
- vendors notifying of the end of life to software or IT equipment;
- advances in technology in general;
- implementing new systems that necessitate changes to existing systems;
- identifying new tasks or functionality requiring updates or new systems;
- organisational change;
- business process or concept of operation change;
- standards evolution;
- government policy or Cabinet directives;
- threat or vulnerability identification and notifications received or issued; and
- other incidents or continuous improvement activities.

Types of system change

6.3.4. A proposed change to a system could involve:

- an upgrade to, or introduction of IT equipment;
- an upgrade to, or introduction of software;
- environment or infrastructure change; or
- major changes to access controls.

PSR references

6.3.5. 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

Change management

6.3.6.R.01. **Rationale**

A considered and accountable process requires consultation with all stakeholders before any changes are implemented. In the case of changes that will affect the security or accreditation status of a system, the Accreditation Authority is a key stakeholder and will need to be consulted and grant approval for the proposed changes.

6.3.6.R.02. **Rationale**

Change management processes are most likely to be bypassed or ignored when an urgent change needs to be made to a system. In these cases it is essential that the agency's change management process strongly enforces appropriate actions to be taken before and after an urgent change is implemented.

6.3.6.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1088]

Agencies MUST ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed;
- the proposed change is approved by the relevant authority;
- any proposed change that could impact the security or accreditation status of a system is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

6.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1089]

Agencies SHOULD ensure that for routine and urgent changes:

- the change management process, as defined in the relevant information security documentation, is followed;
- the proposed change is approved by the relevant authority;
- any proposed change that could impact the security of a system or accreditation status is submitted to the Accreditation Authority for approval; and
- all associated information security documentation is updated to reflect the change.

Change management process

6.3.7.R.01. **Rationale**

Uncontrolled changes pose risks to information systems as well as the potential to cause operational disruptions. A change management process is fundamental to ensure a considered and accountable approach with appropriate approvals. Furthermore, the change management process provides an opportunity for the security impact of the change to be considered and if necessary, reaccreditation processes initiated.

6.3.7.C.01. **Control System Classifications(s): Top Secret; Compliance: Must** [CID:1093]

An agency's change management process MUST define appropriate actions to be followed before and after urgent changes are implemented.

6.3.7.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1094]

An agency's change management process SHOULD define appropriate actions to be followed before and after urgent changes are implemented.

6.3.7.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1095]

Agencies SHOULD follow this change management process outline:

- produce a written change request;
- submit the change request to all stakeholders for approval;
- document the changes to be implemented;
- test the approved changes;
- notification to user of the change schedule and likely effect or outage;
- implement the approved changes after successful testing;
- update the relevant information security documentation including the SRMP, SSP and SOPs
- notify and educate system users of the changes that have been implemented as close as possible to the time the change is applied; and
- continually educate system users in regards to changes.

Changes impacting the security of a system

6.3.8.R.01. **Rationale**

The accreditation of a system accepts residual security risk relating to the operation of that system. Changes may impact the overall security risk for the system. It is essential that the Accreditation Authority is consulted and accepts the changes and any changes to risk.

6.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:1098]**

When a configuration change impacts the security of a system and is subsequently assessed as having changed the overall security risk for the system, the agency MUST reaccredit the system.