6.2. Vulnerability Analysis

Objective

6.2.1. Exploitable information system weaknesses can be identified by vulnerability analyses and inform assessments and controls selection.

Context

Scope

6.2.2. This section covers information on conducting vulnerability assessments on systems as part of the suite of good IT governance activities.

Changes as a result of a vulnerability analysis

6.2.3. It is important that normal change management processes are followed where changes are necessary in order to address security risks identified in a vulnerability analysis.

Rationale & Controls

Vulnerability analysis strategy

6.2.4.R.01. **Rationale**

Vulnerabilities may be unintentionally introduced and new vulnerabilities are constantly identified, presenting ongoing risks to information systems security.

6.2.4.R.02. **Rationale**

While agencies are encouraged to monitor the public domain for information related to vulnerabilities that could affect their systems, they should not remain complacent if no specific vulnerabilities relating to deployed products are disclosed.

6.2.4.R.03. **Rationale**

In some cases, vulnerabilities can be introduced as a result of poor information security practices or as an unintended consequence of activities within an agency. As such, even if no new public domain vulnerabilities in deployed products have been disclosed, there is still value to be gained from regular vulnerability analysis activities.

6.2.4.R.04. **Rationale**

Furthermore, monitoring vulnerabilities, conducting analysis and being aware of industry and product changes and advances, including NZISM requirements, provides an awareness of other changes which may adversely impact the security risk profile of the agency's systems.

6.2.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1063]

Agencies SHOULD implement a vulnerability analysis strategy by:

- monitoring public domain information about new vulnerabilities in operating systems and application software;
- considering the use of automated tools to perform vulnerability assessments on systems in a controlled manner;
- running manual checks against system configurations to ensure that only allowed services are active and that disallowed services are prevented;
- using security checklists for operating systems and common applications; and
- examining any significant incidents on the agency's systems.

Conducting vulnerability assessments

6.2.5.R.01. **Rationale**

A baseline or known point of origin is the basis of any comparison and allows measurement of changes and improvements when further information security monitoring activities are conducted.

6.2.5.C.01.

Control System Classifications(s): All Classifications; Compliance: Should [CID:1066]

Agencies SHOULD conduct vulnerability assessments in order to establish a baseline. This SHOULD be done:

- before a system is first used;
- after any significant incident;
- after a significant change to the system;
- after changes to standards, policies and guidelines;
- when specified by an ITSM or system owner.

Resolving vulnerabilities

6.2.6.R.01. **Rationale**

Vulnerabilities may occur as a result of poorly designed or implemented information security practices, accidental activities or malicious activities, and not just as the result of a technical issue.

6.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1069]

Agencies SHOULD analyse and treat all vulnerabilities and subsequent security risks to their systems identified during a vulnerability assessment.