12.2. Product Installation and Configuration

Objective

12.2.1. Evaluated products use evaluated configurations.

Context

Scope

12.2.2. This section covers information on installing and configuring products providing security functionality. It does not provide information on the installation and configuration of general products or physical security products.

Evaluated configuration

12.2.3. A product is considered to be operating in its evaluated configuration if:

- functionality is used that was within the scope of the evaluation and implemented in the specified manner;
- only patches that have been assessed through a formal assurance continuity process have been applied; and
- the environment complies with assumptions or organisational security policies stated in the product's security target or similar document.

Unevaluated configuration

12.2.4. A product is considered to be operating in an unevaluated configuration when it does not meet the requirements of an evaluated configuration.

Rationale & Controls

Installation and configuration of evaluated products

12.2.5.R.01. **Rationale**

An evaluation of products provides assurance that the product will work as expected with a clearly defined set of constraints. These constraints, defined by the scope of the evaluation, generally consist of what security functionality can be used, and how the products are configured and operated.

12.2.5.R.02. **Rationale**

Using an evaluated product in manner which it was not intended could result in the introduction of new threats and vulnerabilities that were not considered by the initial evaluation.

12.2.5.R.03. **Rationale**

For products evaluated under the Common Criteria and ITSEC, information is available from the developer in the product's installation, generation and startup documentation. Further information is also available in the security target and certification report.

12.2.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3387]

Agencies MUST ensure that high assurance products and HACE are installed, configured, operated and administered in accordance with all product specific policy.

12.2.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3389]

Agencies SHOULD install, configure, operate and administer evaluated products in accordance with available documentation resulting from the product's evaluation.

Use of evaluated products in unevaluated configurations

12.2.6.R.01. **Rationale**

To ensure that a product will still provide the assurance desired by the agency when used in a manner for which it was not intended, a security risk

assessment MUST be conducted upon the altered configuration. The further that a product deviates from its evaluated configuration, the less assurance can be gained from the evaluation.

12.2.6.R.02. **Rationale**

Given the potential threat vectors and the value of the classified information being protected, high assurance products and HACE MUST be configured in accordance with the GCSB's guidelines.

12.2.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must [CID:3401]**

Agencies wishing to use a product in an unevaluated configuration MUST undertake a security risk assessment including:

- the necessity of the unevaluated configuration;
- testing of the unevaluated configuration; and
- the environment in which the unevaluated product is to be used.

12.2.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not [CID:3404]**

High assurance products and HACE MUST NOT be used in unevaluated configurations.