Australian Government
Department of Defence

Defence Signals Directorate

Australasian Information Security Evaluation Program

Sufficiency of Security Measures (ALC_DVS.2) - CC V2.2

Common Evaluation Methodology

11 November 2005

Version 1.1

Amendment Record

Version	Date	Description
1.0	04/10/2005	Release
1.1	11 November 2005	Releasable to AISEFs

Table of Contents

1 Sufficiency of Security Measures (ALC_DVS.2) - CC V2.2

1.1 Objectives

1 The objective of this sub-activity is to determine whether the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised. Additionally, sufficiency of the measures as applied is intended be justified.

1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the development security documentation.

3 In addition, the evaluator may need to examine other deliverables to determine that the security controls are well-defined and followed. Specifically, the evaluator may need to examine the developer's configuration management documentation. Evidence that the procedures are being applied is also required.

1.3 Evaluator Actions

1.3.1 ALC_DVS.2.1E

ALC_DVS.2.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2-1 The evaluator ***shall examine*** the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.

4 The evaluator determines what is necessary by first referring to the ST for any information that may assist in the determination of necessary protection, especially the security objectives for the development environment.

5 If no explicit information is available from the ST the evaluator will need to make a determination of the necessary measures. In cases where the developer's measures are considered less than what is necessary, a clear justification should be provided for the assessment, based on a potential exploitable vulnerability.

6 The following types of security measures are considered by the evaluator when examining the documentation:

a) physical, for example physical access controls used to prevent unauthorised access to the TOE development environment (during normal working hours and at other times);

b) procedural, for example covering:

i) granting of access to the development environment or to specific parts of the environment such as development machines

ii) revocation of access rights when a person leaves the development team

iii) transfer of protected material out of the development environment and between different development sites in accordance with defined acceptance procedures

iv) admitting and escorting visitors to the development environment

v) roles and responsibilities in ensuring the continued application of security measures, and the detection of security breaches.

c) personnel, for example any controls or checks made to establish the trustworthiness of new development staff;

d) other security measures, for example the logical protections on any development machines.

7 The development security documentation should identify the locations at which development occurs, and describe the aspects of development performed, along with the security measures applied at each location and for transports between different locations. For example, development could occur at multiple facilities within a single building, multiple buildings at the same site, or at multiple sites. Transports of parts of the TOE or the unfinished TOE between different development sites are to be covered by the Development security (ALC_DVS), whereas the transport of the finished TOE to the user is dealt with in the Delivery (ADO_DEL).

8 Development includes such tasks as creating multiple copies (production) of the TOE, where applicable.

9 Whereas the CM capabilities (ACM_CAP) requirements are fixed, those for the Development security (ALC_DVS), mandating only necessary measures, are dependent on the nature of the TOE, and on information that may be provided in the ST. For example, the ST may identify a security objective for the development environment that requires the TOE to be developed by staff who have security clearance. The evaluators would then determine that such a policy had been applied under this sub-activity.

ALC_DVS.2-2 The evaluator ***shall examine*** the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.

10 These include the policies governing:

a) what information relating to the TOE development needs to be kept confidential, and which members of the development staff are allowed to access such material;

b) what material must be protected from unauthorised modification in order to preserve the integrity of the TOE, and which members of the development staff are allowed to modify such material.

11 The evaluator should determine that these policies are described in the development security documentation, that the security measures employed are consistent with the policies, and that they are complete.

12 It should be noted that configuration management procedures will help protect the integrity of the TOE and the evaluator should avoid overlap with the work-units conducted for the CM capabilities. For example, the CM documentation may describe the security procedures necessary for controlling the roles or individuals who should have access to the development environment and who may modify the TOE.

13 Whereas the CM capabilities (ACM_CAP) requirements are fixed, those for the Development security (ALC_DVS), mandating only necessary measures, are dependent on the nature of the TOE, and on information that may be provided in the ST. For example, the ST may identify a security objective for the development environment that requires the TOE to be developed by staff who have security clearance. The evaluators would then determine that such a policy had been applied under this sub-activity.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2-3 The evaluator ***shall check*** the development security documentation to determine that documentary evidence that would be produced as a result of application of the procedures has been generated.

14 Where documentary evidence is produced the evaluator inspects it to ensure compliance with procedures. Examples of the evidence produced may include entry logs and audit trails. The evaluator may choose to sample the evidence.

15 For guidance on sampling see CEM Annex B.2, Sampling.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

ALC_DVS.2-4 The evaluator ***shall examine*** the development security documentation to determine that an appropriate justification is given why the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

16 Since attacks on the TOE or its related information are assumed in different design and production stages, measures and procedures need to be implemented at an appropriate level necessary to prevent those attacks or to make them more difficult.

17 The concept of protection measures should be consistent, and the justification should include an analysis of how the measures are mutually supportive. All aspects of development and production on all the different sites with all roles involved up to delivery of the TOE should be analysed.

18 Justification may include an analysis of potential vulnerabilities taking the applied security measures into account.

19 There may be a convincing argument showing e.g.

a) that the technical measures and mechanisms of the developer's infrastructure are sufficient for keeping the appropriate security level (e.g. cryptographic mechanisms as well as physical protection mechanisms, properties of the CM system (cf. ACM_CAP);

b) that the system containing the implementation representation of the TOE (including concerning guidance documents) provides effective protection against logical attacks e.g. by "Trojan" code or viruses. It might be adequate, if the implementation representation is kept on an isolated system where only the software necessary to maintain it is installed and where no additional software is installed afterwards.

c) The appropriate organisational (procedural and personal) measures are unconditionally enforced.

1.3.2 ALC_DVS.2.2E

ALC_DVS.2.2E	The evaluator shall confirm that the security measures are being applied.

ALC_DVS.2-5 The evaluator ***shall examine*** the development security documentation and associated evidence to determine that the security measures are being applied.

20 This work unit requires the evaluator to determine that the security measures described in the development security documentation are being followed, such that the integrity of the TOE and the confidentiality of associated documentation is being adequately protected. For example, this could be determined by examination of the documentary evidence provided. Documentary evidence should be supplemented by visiting the development environment. A visit to the development environment will allow the evaluator to:

a) observe the application of security measures (e.g. physical measures);

b) examine documentary evidence of application of procedures;

c) interview development staff to check awareness of the development security policies and procedures, and their responsibilities.

21 A development site visit is a useful means of gaining confidence in the measures being used. Any decision not to make such a visit should be determined in consultation with the overseer.

22 For guidance on site visits see CEM Annex B.5, Site Visits.