Australian Government
Department of Defence

# Defence Signals Directorate

## Australasian Information Security Evaluation Program

# Advanced Support (ACM_CAP.5) - CC V2.2

## *Common Evaluation Methodology*

**17 November 2006**

**Version 1.2**

# Amendment Record

| Version | Date | Description |
|---|---|---|
| 1.0 | 13 October 2005 | Released. |
| 1.1 | 11 November 2005 | Releasable to AISEFs. |
| 1.2 | 17 November 2006 | Fix re: ACM_CAP.5.4C thru ACM_CAP.5.19C |

# Table of Contents

# 1 Advanced Support (ACM_CAP.5)

## 1.1 Objectives

1 The objectives of this sub-activity are to determine whether the developer has clearly identified the TOE and its associated configuration items, and whether the ability to modify these items is properly controlled by automated tools, thus making the CM system less susceptible to human error or negligence.

## 1.2 Input

2 The evaluation evidence for this sub-activity is:

a) the ST;

b) the TOE suitable for testing;

c) the configuration management documentation; and

d) the developer CM system.

## 1.3 Evaluator Actions

### 1.3.1 ACM_CAP.5.1E

| **ACM_CAP.5.1C** | The reference for the TOE shall be unique to each version of the TOE. |
|---|---|

ACM_CAP.5-1 The evaluator ***shall check*** that the version of the TOE provided for evaluation is uniquely referenced.

3 The evaluator should use the developer's CM system to validate the uniqueness of the reference by checking the configuration list to ensure that the configuration items are uniquely identified. Evidence that the version provided for evaluation is uniquely referenced may be incomplete if only one version is examined during the evaluation, and the evaluator should look for a referencing system that is capable of supporting unique references (e.g. use of numbers, letters or dates). However, the absence of any reference will normally lead to a fail verdict against this requirement unless the evaluator is confident that the TOE can be uniquely identified.

4 The evaluator should seek to examine more than one version of the TOE (e.g. during rework following discovery of a vulnerability), to check that the two versions are referenced differently.

| **ACM_CAP.5.2C** The TOE shall be labelled with its reference. |
|---|

ACM_CAP.5-2 The evaluator ***shall check*** that the TOE provided for evaluation is labelled with its reference.

5 The evaluator should ensure that the TOE contains the unique reference which is stated in the ST. This could be achieved through labelled packaging or media, or by a label displayed by the operational TOE. This is to ensure that it would be possible for consumers to identify the TOE (e.g. at the point of purchase or use).

6 The TOE may provide a method by which it can be easily identified. For example, a software TOE may display its name and version number during the start up routine, or in response to a command line entry. A hardware or firmware TOE may be identified by a part number physically stamped on the TOE.

ACM_CAP.5-3 The evaluator ***shall check*** that the TOE references used are consistent.

7 If the TOE is labelled more than once then the labels have to be consistent. For example, it should be possible to relate any labelled guidance documentation supplied as part of the TOE to the evaluated operational TOE. This ensures that consumers can be confident that they have purchased the evaluated version of the TOE, that they have installed this version, and that they have the correct version of the guidance to operate the TOE in accordance with its ST.

8 The evaluator also verifies that the TOE reference is consistent with the ST.

| **ACM_CAP.5.3C** The CM documentation shall include a configuration list, a CM plan, an acceptance plan, **and integration procedures**. |
|---|

ACM_CAP.5-4 The evaluator ***shall check*** that the CM documentation provided includes a configuration list.

9 A configuration list identifies the items being maintained under configuration control.

ACM_CAP.5-5 The evaluator ***shall check*** that the CM documentation provided includes a CM Plan.

10 The CM plan needs not to be a connected document, but it is recommended that there is a single document that describes where the various parts of the CM plan can be found.

ACM_CAP.5-6 The evaluator ***shall check*** that the CM documentation provided includes an acceptance plan.

11 Acceptance procedures should include those developer roles or individuals responsible for the acceptance and the criteria to be used for acceptance. They should take into account all acceptance situations that may occur, in particular:

a) accepting an item into the CM system for the first time, in particular inclusion of software, firmware and hardware components from other manufacturers into the TOE (“integration”);

b) moving configuration items to the next life-cycle phase at each stage of the construction of the TOE (e.g. module, subsystem, system);

c) subsequent to transports between different development sites.

ACM_CAP.5-7 The evaluator ***shall check*** that the CM documentation provided includes integration procedures.

12 Integration procedures describe the steps that must be undertaken to construct the TOE from its software, firmware and hardware components, including any components provided from other manufacturers and should identify any test procedures to verify the correct assembly of the TOE.

**ACM_CAP.5.4C** The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.5-8 The evaluator ***shall examine*** the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

13 The minimum scope of configuration items to be covered in the configuration list is given by CM scope (ACM_SCP).

**ACM_CAP.5.5C** The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.5-9 The evaluator ***shall examine*** the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.

14 Procedures should describe how the status of each configuration item can be tracked throughout the life-cycle of the TOE. The procedures may be detailed in the CM plan or throughout the CM documentation. The information included should describe:

a) the method how each configuration item is uniquely identified, such that it is possible to track versions of the same configuration item;

b) the method how configuration items are assigned unique identifiers and how they are entered into the CM system;

c) the method to be used to identify superseded versions of a configuration item.

**ACM_CAP.5.6C** The CM system shall uniquely identify all configuration items.

ACM_CAP.5-10 The evaluator ***shall examine*** the configuration items to determine that they are identified in a way that is consistent with the CM documentation.

15 Assurance that the CM system uniquely identifies all configuration items is gained by examining the identifiers for the configuration items. For both configuration items that comprise the TOE, and drafts of configuration items that are submitted by the developer as evaluation evidence, the evaluator confirms that each configuration item possesses a unique identifier in a manner consistent with the unique identification method that is described in the CM documentation.

**ACM_CAP.5.7C** The CM plan shall describe how the CM system is used.

ACM_CAP.5-11 The evaluator ***shall examine*** the CM plan to determine that it describes how the CM system is used to maintain the integrity of the TOE configuration items.

16 The descriptions contained in a CM plan may include:

a) all activities performed in the TOE development environment that are subject to configuration management procedures (e.g. creation, modification or deletion of a configuration item);

b) the roles and responsibilities of individuals required to perform operations on individual configuration items (different roles may be identified for different types of configuration item (e.g. design documentation or source code));

c) the procedures that are used to ensure that only authorised individuals can make changes to configuration items;

d) the procedures that are used to ensure that concurrency problems do not occur as a result of simultaneous changes to configuration items;

e) the evidence that is generated as a result of application of the procedures. For example, for a change to a configuration item, the CM system might record a description of the change, accountability for the change, identification of all configuration items affected, status (e.g. pending or completed), and date and time of the change. This might be recorded in an audit trail of changes made or change control records;

f) the approach to version control and unique referencing of TOE versions (e.g. covering the release of patches in operating systems, and the subsequent detection of their application).

**ACM_CAP.5.8C** The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.5-12 The evaluator ***shall check*** the CM documentation to ascertain that it includes the CM system records identified by the CM plan.

17 The output produced by the CM system should provide the evidence that the evaluator needs to be confident that the CM plan is being applied, and also that all configuration items are being maintained by the CM system. Example output could include change control forms, or configuration item access approval forms.

ACM_CAP.5-13 The evaluator ***shall examine*** the evidence to determine that the CM system is being used as it is described in the CM plan.

18 The evaluator should select and examine a sample of evidence covering each type of CM-relevant operation that has been performed on a configuration item (e.g. creation, modification, deletion, reversion to an earlier version) to confirm that all operations of the CM system have been carried out in line with documented procedures. The evaluator confirms that the evidence includes all the information identified for that operation in the CM plan. Examination of the evidence may require access to a CM tool that is used. The evaluator may choose to sample the evidence.

19 For guidance on sampling see B.2.

20 Further confidence in the correct operation of the CM system and the effective maintenance of configuration items may be established by means of interview with selected development staff. In conducting such interviews, the evaluator should aim to gain a deeper understanding of how the CM system is used in practice as well as to confirm that the CM procedures are being applied as described in the CM documentation. Note that such interviews should complement rather than replace the examination of documentary evidence, and may not be necessary if the documentary evidence alone satisfies the requirement. However, given the wide scope of the CM plan it is possible that some aspects (e.g. roles and responsibilities) may not be clear from the CM plan and records alone. This is one case where clarification may be necessary through interviews.

21 It is expected that the evaluator will visit the development site in support of this activity.

22 For guidance on site visits see B.5.

**ACM_CAP.5.9C** The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.5-14 The evaluator ***shall check*** that the configuration items identified in the configuration list are being maintained by the CM system.

23 The CM system employed by the developer should maintain the integrity of the TOE. The evaluator should check that for each type of configuration item (e.g. high-level design or source code modules) contained in the configuration list there are examples of the evidence generated by the procedures described in the CM plan. In this case, the approach to sampling will depend upon the level of granularity used in the CM system to control CM items. Where, for example, 10,000 source code modules are identified in the configuration list, a different sampling strategy should be applied compared to the case in which there are only 5, or even 1. The emphasis of this activity should be on ensuring that the CM system is being operated correctly, rather than on the detection of any minor error.

24 For guidance on sampling see B.2.

**ACM_CAP.5.10C** The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.5-15 The evaluator ***shall examine*** the CM access control measures described in the CM plan to determine that they are effective in preventing unauthorised access to the configuration items.

25 The evaluator may use a number of methods to determine that the CM access control measures are effective. For example, the evaluator may exercise the access control measures to ensure that the procedures could not be bypassed.

26 The evaluator may use the outputs generated by the CM system procedures and already examined as part of the work unit ACM_CAP.5-13. The evaluator may also witness a demonstration of the CM system to ensure that the access control measures employed are operating effectively.

27 The developer will have provided automated access control measures as part of the CM system and as such their suitability may be verified under the ACM_AUT.x component.

**ACM_CAP.5.11C** The CM system shall support the generation of the TOE.

ACM_CAP.5-16 The evaluator ***shall check*** the CM documentation for procedures for supporting the generation of the TOE.

28 In this work unit the term "generation" applies to those processes adopted by the developer to progress the TOE from implementation to a state acceptable for delivery to the end customer.

29 The evaluator verifies the existence of generation support procedures within the CM documentation. The generation support procedures provided by the developer may be automated, and as such their existence may be verified under the ACM_AUT.x sub activity.

ACM_CAP.5-17 The evaluator ***shall examine*** the TOE generation procedures to determine that they are effective in helping to ensure that the correct configuration items are used to generate the TOE.

30 The evaluator determines that by following the generation support procedures the version of the TOE expected by the customer (i.e. as described in the TOE ST and consisting of the correct configuration items) would be generated and delivered for installation at the customer site. For example, in a software TOE this may include checking that the procedures ensure that all source files and related libraries are included in the compiled object code.

31 The evaluator should bear in mind that the CM system need not necessarily possess the capability to generate the TOE, but should provide support for the process that will help reduce the probability of human error.

**ACM_CAP.5.12C** The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

ACM_CAP.5-18 The evaluator ***shall examine*** the acceptance procedures to determine that they describe the acceptance criteria to be applied to newly created or modified configuration items.

32 An acceptance plan describes the procedures that are to be used to ensure that the constituent parts of the TOE are of adequate quality prior to incorporation into the TOE. The acceptance plan should identify the acceptance procedures to be applied:

a) at each stage of the construction of the TOE (e.g. module, integration, system);

b) to the acceptance of software, firmware and hardware components;

c) to the acceptance of previously evaluated components.

33 The description of the acceptance criteria may include identification of:

a) developer roles or individuals responsible for accepting such configuration items;

b) any acceptance criteria to be applied before the configuration items are accepted (e.g. successful document review, or successful testing in the case of software, firmware or hardware).

**ACM_CAP.5.13C The integration procedures shall describe how the CM system is applied in the TOE manufacturing process.**

ACM_CAP.5-19 The evaluator ***shall examine*** the integration procedures to determine that they are effective in ensuring that a TOE is generated that reflects its implementation representation.

34 The integration procedures should describe which tools have to be used to produce the final TOE from the implementation representation in a clearly defined way. The conventions, directives, or other necessary constructs are described under ALC_TAT.

35 The evaluator determines that by following the integration procedures the correct configuration items would be used to generate the TOE. For example, in a software TOE this may include checking that the automated production procedures ensure that all source files and related libraries are included in the compiled object code. Moreover, the procedures should ensure that compiler options and comparable other options are defined uniquely.

36 The customer can then be confident that the version of the TOE delivered for installation is derived from the implementation representation in an unambiguous way and implements the SFRs as described in the ST.

37 The evaluator should bear in mind that the CM system need not necessarily possess the capability to produce the TOE, but should provide support for the process that will help reduce the probability of human error. The integration procedures should identify how the CM system is applied in such a process.

**ACM_CAP.5.14C The CM system shall require that the person responsible for accepting a configuration item into CM is not the person who developed it.**

ACM_CAP.5-20 The evaluator ***shall examine*** the CM system to determine that it ensures that the person responsible for accepting a configuration item is not the person who developed it.

38 The acceptance procedures describe who is responsible for accepting a configuration item. From these descriptions, the evaluator should be able to determine that the person who developed a configuration item is in no case responsible for its acceptance.

**ACM_CAP.5.15C The CM system shall clearly identify the configuration items that comprise the TSF.**

ACM_CAP.5-21 The evaluator ***shall examine*** the CM system to determine that it clearly identifies the configuration items that comprise the TSF.

39 The CM documentation should describe how the CM system identifies the configuration items that comprise the TSF. The evaluator should select a sample of configuration items covering each type of items, particularly containing TSF and non-TSF items, and check that they are correctly classified by the CM system.

**ACM_CAP.5.16C The CM system shall support the audit of all modifications to the TOE, including the originator, date, and time in the audit trail.**

ACM_CAP.5-22 The evaluator ***shall examine*** the CM system to determine that it supports the audit of all modifications to the TOE by automated means, including as a minimum the originator, date, and time in the audit trail.

40 The evaluator should inspect a sample of audit trails and check, if they contain the minimum information. For guidance on sampling see B.2.

**ACM_CAP.5.17C The CM system shall be able to identify the master copy of all material used to generate the TOE.**

ACM_CAP.5-23 The evaluator ***shall examine*** the CM system to determine that it is able to identify the master copy of all material used to generate the TOE.

41 The CM documentation should describe how the CM system identifies the master copies of the implementation representation from which the TOE is generated. The evaluator should select a sample of the parts used to produce the TOE and should apply the CM system to verify that it identifies the corresponding implementation representations in the correct version.

**ACM_CAP.5.18C The CM documentation shall demonstrate that the use of the CM system, together with the development security measures, allow only authorised changes to be made to the TOE.**

ACM_CAP.5-24 The evaluator ***shall examine*** the CM documentation to determine that use of the CM system, together with the development security measures, allow only authorised changes to be made to the TOE.

42 The evaluator will have already examined the acceptance procedures employed within the CM system in ACM_CAP.5-6. The evaluator uses this information together with:

a) the evidence provided for the ALC_DVS sub activity;

b) the roles and responsibilities of individuals required to perform operations on individual configuration items (different roles may be identified for different types of configuration items (e.g. design documentation or source code))

c) change management procedures; and

d) the procedures that are used to ensure that only authorised individuals can make changes to configuration items.

43 The evaluator analyses the CM documentation to establish that the documented procedures do not include any inconsistencies or omissions that would allow for unauthorised changes to be made to the TOE configuration items.

44 The evaluator should verify their analysis by sampling the CM system audit trail and change records against the defined roles to verify that only those individuals with authorisation to make changes to a configuration item have effected those changes. For guidance on sampling see B.2.

**ACM_CAP.5.19C The CM documentation shall demonstrate that the use of the integration procedures ensures that the generation of the TOE is correctly performed in an authorised manner.**

ACM_CAP.5-25 The evaluator shall examine the integration procedures to determine that they demonstrated the correct generation of all parts of the TOE was initiated and carried out in an authorised manner.

45 The evaluator will have already examined the integration procedures employed within the CM system in ACM_CAP.5-19. The evaluator analyses this information with an emphasis on correct authorisation.

46 The evaluator should verify their analysis by sampling the CM system audit trail and TOE generation logs to verify correct authorisation. For guidance on sampling see B.2.

**ACM_CAP.5.20C The CM documentation shall demonstrate that the CM system is sufficient to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.**

ACM_CAP.5-26 The evaluator shall examine the CM documentation to determine that it demonstrated that the CM system is sufficient to ensure that the person responsible for accepting a configuration item into CM is not the person who developed it.

47 The evaluator will have already examined the acceptance procedures employed within the CM system in ACM_CAP.5-6. The evaluator uses this information together with:

a) the roles and responsibilities of individuals required to perform operations on individual configuration items (different roles may be identified for different types of configuration items (e.g. design documentation or source code))

48 The evaluator analyses the CM documentation to establish that the documented procedures do not include any inconsistencies or omissions that would allow for a developer of a configuration item to accept the item into the CM system.

49 The evaluator should verify their analysis by sampling the CM system audit trail and configuration items against the defined roles to verify that the developer of a configuration item has not also been the individual who has accepted the item into the CM system. For guidance on sampling see B.2.

**ACM_CAP.5.21C The CM documentation shall justify that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.**

ACM_CAP.5-27 The evaluator ***shall examine*** the CM documentation to determine that it justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.

50 The CM documentation should make it sufficiently clear that by following the acceptance procedures only parts of adequate quality are incorporated into the TOE.