CCIMB Interpretations-0407

平成 16 年 8 月

独立行政法人情報処理推進機構
セキュリティセンター
情報セキュリティ認証室

Index to CCIMB Interpretations

(as of 01 December 2003)

The following Interpretations to the *Common Criteria* have been approved and adopted by the Common Criteria Interpretations Management Board, which represents the schemes within Mutual Recognition.

Contents

Index of Final Interpretations

The following is a list of interpretations that have been approved by the CCIMB . They are listed in numerical order, each followed by the date it was approved .

- Interpretation 003 -- **Unique identification of configuration items in the configuration list** (11 February 2002)
- Interpretation 004 -- **ACM_SCP.*.1C requirements unclear** (12 November 2001)
- Interpretation 006 -- **Virtual machine description** (15 October 2000)
- Interpretation 008 -- **Augmented and Conformant overlap** (31 July 2001)
- Interpretation 009 -- **Definition of "Counter"** (13 April 2001)
- Interpretation 013 -- **Multiple SOF claims for multiple domains in a single TOE** (15 October 2000)
- Interpretation 016 -- **Objective for ADO_DEL** (11 February 2002)
- Interpretation 019 -- **Assurance Iterations** (11 February 2002)
- Interpretation 024 -- **Required evaluation evidence for commercial off the shelf (COTS) products** (16 February 2001)
- Interpretation 025 -- **Level of detail required for hardware descriptions** (31 July 2001)
- Interpretation 027 -- **Events and functions in AGD_ADM** (16 February 2001)
- Interpretation 031 -- **Obvious vulnerabilties** (25 October 2002)
- Interpretation 032 -- **Strength of Function Analysis in ASE_TSS** (15 October 2000)
- Interpretation 033 -- **Use of 'check' in part 3** (15 October 2000)
- Interpretation 037 -- **ACM on Product or TOE?** (16 February 2001)
- Interpretation 038 -- **Use of 'as a minimum' in C&P elements** (31 October 2003)
- Interpretation 043 -- **Meaning of "clearly stated" in APE/ASE_OBJ.1** (16 February 2001)

- Interpretation 049 -- **Threats met by environment** (16 February 2001)
- Interpretation 051 -- **Use of documentation without C & P elements** (25 October 2002)
- Interpretation 055 -- **Incorrect Component referenced in Part 2 Annexes, FPT_RCV** (15 October 2000)
- Interpretation 056 -- **When can the FPT_RCV dependency on FPT_TST be argued away?** (31 October 2003)
- Interpretation 058 -- **Confusion over refinement** (31 July 2001)
- Interpretation 062 -- **Confusion over source of flaw reports** (31 July 2001) -- INCORPORATED into ALC_FLR Supplement
- Interpretation 064 -- **Apparent higher standard for explicitly stated requirements** (16 February 2001)
- Interpretation 065 -- **No component to call out security function management** (31 July 2001)
- Interpretation 067 -- **Application notes missing in ST** (15 October 2000)
- Interpretation 069 -- **Informal Security Policy Model** (30 March 2001)
- Interpretation 074 -- **Duplicate Informative Text for ATE_COV.2-3 and ATE_DPT.1-3** (15 October 2000)
- Interpretation 075 -- **Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1** (15 October 2000)
- Interpretation 080 -- **APE_REQ.1-12 does not use "shall examine..to determine"** (15 October 2000)
- Interpretation 084 -- **Separate objectives for TOE and environment** (16 February 2001)
- Interpretation 085 -- **SOF Claims additional to the overall claim** (11 February 2002)
- Interpretation 092 -- **Release of the TOE** (31 July 2001) -- INCORPORATED into ALC_FLR Supplement
- Interpretation 094 -- **FLR Guidance Documents Missing** (31 July 2001) -- SUPERCEDED by ALC_FLR Supplement
- Interpretation 095 -- **ACM_CAP dependency on ACM_SCP** (16 February 2001)
- Interpretation 098 -- **Limitation of Refinement** (11 February 2002)
- Interpretation 103 -- **Association Of Access Control Attributes With Subjects And Objects** (15 July 2003)
- Interpretation 104 -- **Association of Information Flow Attributes with Subjects and Objects** (15 July 2003)
- Interpretation 111 -- **Settable Failure Limits are Permitted** (31 October 2003)
- Interpretation 116 -- **Indistinguishable work units for ADO_DEL** (31 July 2001)
- Interpretation 120 -- **Sampling of process expectations unclear** (12 November 2001)
- Interpretation 127 -- **TSS Work unit not at the right place** (25 October 2002)
- Interpretation 128 -- **Coverage of the delivery procedures** (15 November 2002)
- Interpretation 133 -- **Consistency analysis in AVA_MSU.2** (25 October 2002)
- Interpretation 138 -- **Iteration and narrowing of scope** (05 June 2002)
- Interpretation 140 -- **Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR** (15 July 2003)
- Interpretation 141 -- **Some Modifications to the Audit Trail Are Authorized** (15 July 2003)
- Interpretation 150 -- **A Completely Evaluated ST is not Required when TOE evaluation starts** (15 July 2003)
- Interpretation 151 -- **Security Attributes Include Attributes of Information and Resources** (31 October 2003)
- Interpretation 201 -- **"Other properties" specified by assignment** (31 October 2003)
- Interpretation 202 -- **Selecting One or More items in a selection operation and using "None" in an assignment** (26 August 2003)
- Interpretation 212 -- **Relationship between FPT_PHP and FMT_MOF** (31 October 2003)
- Interpretation 222 -- **Meaning and use of "normative" and "informative"?** (31 October 2003)

Final Interpretation for RI # 3 - Unique identification of configuration items in the configuration list

Date:	02 / 11 / 2002
Subject:	Unique identification of configuration items in the configuration list
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 8.2 (ACM_CAP)
CEM Reference:	

Issue:

Is it required that the configuration list uniquely identify all configuration items, including version numbers as appropriate? ACM_CAP.2.6C requires that the CM system uniquely identify all configuration items, but ACM_CAP.2.4C does not explicitly require that the configuration list itself uniquely identify each configuration item, including version numbers as appropriate.

Interpretation

The intent of ACM_CAP.2 is that the developer provides a unique reference for each version of a TOE configuration item that is submitted, whether draft or otherwise, as evaluation evidence. The configuration list need only contain the version of each configuration item that is specific to the TOE that is being evaluated, and as such the configuration items must be uniquely identified in the configuration list. However, for earlier drafts of configuration items that had been submitted by the developer as evaluation evidence, it is necessary for the evaluator to confirm that these drafts also possess unique identifiers in a manner that is consistent with the unique identification method that is described in the CM documentation.

Specific Changes

In the CC, the following new assurance element is added after ACM.CAP.2.3C, ACM.CAP.3.3C, ACM.CAP.4.3C, and ACM_CAP.5.3C:

> "The configuration list shall uniquely identify all configuration items that comprise the TOE."

In the CEM,

- A new action is inserted after paragraphs 659, 938 and work unit ACM_CAP.4-6, corresponding to the new element.
- The text of the current work units ACM_CAP.2-7, ACM_CAP.3-8 and ACM_CAP.4-9 (and their supporting guidance text) are moved below this new action.
- The text of the current work units ACM_CAP.2-7, ACM_CAP.3-8 and ACM_CAP.4-9 are replaced with the following:

> "The evaluator shall examine the configuration items to determine that they are identified in a way that is consistent with the CM documentation."

and the following guidance text:

> "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."

Final Interpretation for RI # 4 - ACM_SCP.*.1C requirements unclear

Date:	11 / 12 / 2001
Subject:	ACM_SCP.*.1C requirements unclear
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 8.3 (ACM_SCP)
CEM Reference:	CEM, Section 8.4.3 (ACM_SCP.2)

Issue:

ACM_SCP.*.1C requires that "design documentation" is tracked by the CM system. This term is not used elsewhere, and clearly does not map directly to ADV requirements (since it appears to exclude the implementation representation).

Interpretation

ACM_SCP is interpreted as intending to extend the requirements of ACM_CAP to additional items, not to impose additional CM capabilities (i.e. the requirement to 'track').

ACM_SCP.1.1C requires that the following must be included in the list of configuration items: the implementation representation and the evaluation evidence required by the assurance components in the ST.

Specific Changes

In CC Part 3, the following changes are made:

- The following is inserted after paragraph 257 (last application note for ACM_CAP):

  > ACM_CAP identifies the CM requirements to be imposed on all items identified in the configuration item list. Other than the TOE itself, ACM_CAP leaves the contents of the configuration item list to the discretion of the developer. (ACM_SCP can be used to identify specific items that must be included in the configuration item list, and hence covered by CM.)

- Paragraphs 274 and 275 (Objectives for ACM_SCP) are replaced with:

  > The objective of this family is to require items to be included as configuration items and hence placed under the CM requirements of ACM_CAP. Applying configuration management to these additional items provides additional assurance that the integrity of TOE is maintained.

- Paragraph 276 (Component levelling for ACM_SCP) is replaced with:

  > The components in this family are levelled on the basis of which of the following are required to be included as configuration items: implementation representation; the evaluation evidence required by the assurance components in the ST; security flaws; and development tools and related information.

- Immediately before paragraph 277, the following is inserted as the new first paragraph of the application notes for ACM_SCP:

  While ACM_CAP mandates a list of configuration items and that each item on this list be under CM, other than the TOE itself, ACM_CAP leaves the contents of the configuration item list to the discretion of the developer. ACM_SCP narrows this discretion by identifying items that must be included in the configuration item list, and hence come under the CM requirements of ACM_CAP.

- Paragraphs 277, 279, and 280 (application notes for ACM_SCP) are changed as follows:

  "tracked by the CM system" is replaced by "included in the list of configuration items"

- Paragraph 278 (second application note for ACM_SCP) is replaced with:

  ACM_SCP.1.1C also introduces the requirement that the evaluation evidence required by the other assurance components in the ST be included in the list of configuration items.

- Paragraphs 281, 282, and 284 (first objective for ACM_SCP.1, ACM_SCP.2, and ACM_SCP.3) are each replaced with:

  A CM system can control changes only to those items that have been placed under CM (i.e., the configuration items identified in the configuration item list). Placing the TOE implementation and the evaluation evidence required by the other assurance components in the ST under CM provides assurance that they have been modified in a controlled manner with proper authorisations.

- Paragraphs 283 and 285 (second objective for ACM_SCP.2 and ACM_SCP.3) are changed as follows:

  "The ability to track security flaws under CM ensures" is replaced with "Placing security flaws under CM ensures"

- ACM_SCP.*.1D is changed to:

  ACM_SCP.*.1D The developer shall provide a list of configuration items for the TOE.

- ACM_SCP.*.1C is changed to:

  ACM_SCP.1.1C **The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.**

  ACM_SCP.2.1C The list of configuration items shall include the following: implementation representation; **security flaws**; and the evaluation evidence required by the assurance components in the ST.

  ACM_SCP.3.1C The list of configuration items shall include the following: implementation representation; security flaws; **development tools and related information**; and the evaluation evidence required by the assurance components in the ST.

- ACM_SCP.*.2C is deleted.

In the CEM, the following changes are made:

- Paragraphs 953 and 1327 (input for ACM_SCP.1 and ACM_SCP.2 sub-activities respectively) are each changed to:

  "configuration management documentation" is changed to "configuration item list"

- Work units 3:ACM_SCP.1-1 and 4:ACM_SCP.2-1 are each replaced by:

  The evaluator ***shall check*** that the configuration item list includes the set of items required by the CC.

- Paragraphs 955 (guidance for work units 3:ACM_SCP.1-1) is replaced with:

  The list includes thefollowing:

  a) the TOE implementation representation (i.e., the components or subsystems that compose the TOE). For a software-only TOE, the implementation representation may consist solely of source code; for a TOE that includes a hardware platform, the implementation representation may refer to a combination of software, firmware and a description of the hardware.

  b) the evaluation evidence required by the assurance components in the ST.

- Paragraph 1329 (guidance for work unit 4:ACM_SCP.2-1) is replaced with:

  The list includes the following:

  a) the TOE implementation representation (i.e., the components or subsystems that compose the TOE). For a software-only TOE, the implementation representation may consist solely of source code; for a TOE that includes a hardware platform, the implementation representation may refer to a combination of software, firmware and a description of the hardware.

  b) the evaluation evidence required by the assurance components in the ST.

  c) the documentation used to record details of reported security flaws associated with the implementation (e.g., problem status reports derived from a developer's problem database).

- Work units 3:ACM_SCP.1-2 and 4:ACM_SCP.2-2 and their associated guidance are deleted.

Final Interpretation for RI # 6 - Virtual machine description

Date:	10/15/2000
Subject:	Virtual machine description
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 10.2 (ADV_HLD)
CEM Reference:	

Issue:

The reference to underlying hardware, firmware and software in ADV_HLD.*.5C is unclear. It is assumed that the information required by this element concerns the virtual machine on which the TOE runs (if any), rather than mechanisms contained within the TOE (which is covered elsewhere in the component). As such it could be considered a requirement on information about the IT environment.

Interpretation

The phrase “underlying hardware, firmware and software” is interpreted to mean “information required by ADV_HLD.*.5C concerning the virtual machine on which the TOE runs (if any), rather than mechanisms contained within the TOE (which is covered elsewhere in the component), and as such it is a requirement on information about the IT environment”.

Specific Changes

CEM: Already addressed in CEM part 2 version 1.0

CC: Add a new application note after paragraph 328.

"In ADV_HLD.*.5C the phrase "underlying hardware, firmware and/or software" concerns the virtual machine on which the TOE runs (if any), rather than mechanisms contained within the TOE (which are covered elsewhere in the component). As such it is a requirement on information about the IT environment."

Final Interpretation for RI # 8 - Augmented and Conformant overlap

Date:	07/31/2001
Subject:	Augmented and Conformant overlap
CC Part #1 Reference:	CC Part 1, Section 5.4
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 4.4.3 (ASE_INT.1)

Issue:

The notion of assurance packages, without any evaluation requirements for packages, has caused the definitions of "augmented" and "conformant" to become merged. An assurance package is effectively the same as an assurance package plus other assurance components, since the content of an assurance package is arbitrary.

Interpretation

An assurance package is not so much "arbitrary" as "not pre-defined". One defined assurance package can be augmented and the resulting set of assurance requirements could be defined as a new assurance package. To clarify this issue, and to make the results of evaluations more clear to potential consumers, the CC is interpreted as detailed in the specific change below.

Specific Changes

To address this interpretation, the following changes are made to CC v2.1, Part 1:

- The following sentence is added to the end of paragraph 175 in CC v2.1 Part 1:

  The results of evaluation shall also include a "Conformance Result".

- The title of CC Part 1, section/Clause 5.4 is changed to "Conformance results".
- The following text replaces CC Part 1, section/Clause 5.4:

  The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

  The conformance result consists of one of the following:

  Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

  Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

  plus one of the following:

  Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance

requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

To address this interpretation, the following change is made to CEM Part 2 v1.0:

- Paragraphs 335 through 340 are replaced by the following:

The evaluator determines that the CC conformance claim contains either Part 3 conformant or Part 3 extended.

If Part 3 extended is claimed and the assurance requirements package includes assurance requirements in Part 3, the evaluator determines that the CC conformance claim states which assurance requirements that are in Part 3 are claimed.

If Package Name conformant is claimed, the evaluator determines that the CC conformance claim states which package is claimed.

If Package Name augmented is claimed, the evaluator determines that the CC conformance claim states which package is claimed and which augmentations to that package are claimed.

If PP conformant is claimed, the evaluator determines that the CC conformance claim states to which PP or PPs conformance is claimed.

Final Interpretation for RI # 9 - Definition of Counter

Date:	04 / 13 / 2001
Subject:	Definition of Counter
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 1
CEM Reference:	

Issue:

The definition of *counter* is inaccurate. Strictly speaking, an objective cannot counter a threat; an objective is a statement of what is needed to counter a threat.

Interpretation

Objectives are merely statements of goals. They do not counter threats solely by their existence; it is when objectives are realised that the threat is mitigated.

Specific Changes

CC Part 3, Paragraph 75 is replaced with:

> **Counter** (verb) - This term is typically used in the context that the impact of a particular threat is mitigated but not necessarily eradicated.

Final Interpretation for RI # 13 - Multiple SOF claims for multiple domains in a single TOE

Date:	10 / 15 / 2000
Subject:	Multiple SOF claims for multiple domains in a single TOE
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 5.6 (ASE_REQ) CC Part 3, Section 14.3 (AVA_SOF)
CEM Reference:	

Issue:

The CC implies that a single minimum SOF claim should be made for the TOE. This is inadequate for TOEs that operate in multiple domains.

Interpretation

It is acceptable to define a PP or ST for a TOE that operates in multiple domains with a minimum SOF level claim for each domain. The CC is interpreted as detailed in the specific change below. The CEM addresses this issue in paragraphs 236, 237, 425 and 426.

Specific Changes

A new paragraph is added after paragraph 157 (APE_REQ) and paragraph 178 (ASE_REQ):

> The CC recognises the validity of multiple SOF domains within a given TOE. A SOF domain is a subset of the TOE (logical or physical) for which a specific functional strength level is appropriate, in the context of the intended environment. This allows for a TOE with some functionality having a higher minimum strength requirement than other functionality. For a TOE with multiple SOF domains, the phrase "minimum strength of function" is used to indicate the set that contains the minimum strength of function for each domain, identified by domain. Additionally, the requirements rationale must consider the SOF level for each domain in light of how that that domain impacts meeting the security objectives.

Final Interpretation for RI # 16 - Objective for ADO_DEL

Date:	02 / 11 / 2002
Subject:	Objective for ADO_DEL
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 9.1 (ADO_DEL)
CEM Reference:	CEM, Section 6.5.1 (ADO_DEL.1)

Issue:

The CC objective statement in ADO_DEL refers only to protection of the integrity of the TOE, and yet the components use the more general term security. For some TOEs confidentiality and availability may be an issue for delivery, and it may be argued that there is no current assurance component to specify this.

Interpretation

The objective for ADO_DEL is to maintain the security (e.g. confidentiality, integrity, availability) of the TOE during distribution. The technical measures introduced in ADO_DEL.2 and ADO_DEL.3 are required to address integrity issues only.

Specific Changes

In CC Part 3, the following changes are made:

The objectives statement for ADO_DEL (CC Part 3 paragraph 289) is replaced with:

> The requirements for delivery call for system control and distribution facilities and procedures that detail the measures necessary to provide assurance that the security of the TOE is maintained during distribution of the TOE. For a valid distribution of the TOE, the procedures used for the distribution of the TOE address the threats identified in the PP/ST relating to the security of the TOE during delivery.

The words "detect and prevent modifications to" in CC Part 3 Paragraph 290 are replaced with "maintain security of".

The following is included as an application note after CC Part 3 paragraph 290:

> These procedures could consider issues such as:

- ensuring the TOE received by the consumer corresponds precisely to the TOE Master copy;
- avoiding/detecting any tampering with the actual version of the TOE;
- preventing submission of a false version of the TOE;
- avoiding unwanted knowledge of distribution of the TOE to the consumer;
- avoiding/detecting the TOE being intercepted during delivery; and
- avoiding the TOE being delayed or stopped during distribution.

> Although the procedures consider protection of the TOE in all aspects (integrity, confidentiality, availability), the technical measures introduced in ADO_DEL.2 and ADO_DEL.3 are required to address integrity issues only.

In the CEM, the following changes are made:

The objectives statement for ADO_DEL.1 (CEM para 664 and 960) is replaced with:

> The objective of this sub-activity is to determine whether the delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user's site.

The objectives statement for ADO_DEL.2 (CEM para 1334) is replaced with:

> The objective of this sub-activity is to determine whether the delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site.

The term "integrity" is replaced with "security of the TOE" in CEM paragraphs 668, 964 and 1338.

CEM Paragraphs 669, 965 and 1339 are replaced with:

> The emphasis in the delivery documentation is likely to be on measures related to integrity, as technical measures are required to be applied to maintain integrity during the TOE delivery. However, confidentiality and availability of the delivery will be of concern in the delivery of some TOEs; procedures relating to these aspects of the secure delivery should also be discussed in the procedures.

Final Interpretation for RI # 19 - Assurance Iterations

Date:	02 / 11 / 2002
Subject:	Assurance Iterations
CC Part #1 Reference:	CC Part 1, Section 4.4.1
CC Part #2 Reference:	CC Part 2, Section 2.1.4
CC Part #3 Reference:	CC Part 3, Section 2.1.4
CEM Reference:	

Issue:

Are iterations allowed in assurance components (see CC Part 3, section 2.1.4 (paragraph 56))? CC Part 1, section 4.4.1.3 (paragraph 148) specifically permits it.

Interpretation

Iteration is permitted for assurance components, particularly in instances where assurance elements within these components have undergone refinement. The same operations that are applicable to Part 2 functional components are also applicable to Part 3 assurance components. In addition, at the present time none of the Part 3 assurance components contain explicit assignment or selection operations. However, this does not preclude Part 3 assurance components from containing assignment or selection operations in the future.

Specific Changes

The following changes are made to the CC:

- CC Part 2 section 2.1.4 is deleted.
- CC Part 3 paragraph 56 is deleted.
- In CC Part 1, paragraph 148 is replaced with the following text:

> CC functional and assurance components may be used exactly as defined in the CC, or they may be tailored through the use of permitted operations in order to meet a security objective. When an element within a component undergoes a refinement, the PP/ST author shall clearly identify that such a refinement has been performed. The PP/ST author must also be

careful that the dependency needs of other requirements that depend on this requirement are satisfied. The permitted operations are selected from the following set:

Iteration: allows a component to be used more than once with varying operations;

Assignment: allows the specification of parameters;

Selection: allows the specification of one or more items from a list; and

Refinement: allows the addition of details.

Iteration

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component to cover each aspect is permitted.

While iteration is referred to at the level of a requirement component, it is not always necessary to repeat the full text of each of the iterations of the component, if doing so

would result in some elements within the component being repeated multiple times with no changes. It is permissible in the PP or ST to repeat only those requirement elements that are being changed each time, whether by refinement, or by the completion of assignment or selection operations. (See Refinement for further guidance on iterating refined requirements).

Assignment

Some components have elements that contain parameters that enable the PP/ST author to specify a set of values for incorporation into the PP or ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter.

Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

Selection

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

Refinement

For all components, the PP/ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details.

In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

- A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the PP/ST;

- In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement;

however, the sum of the iterations must together meet the entire scope of the original requirement;

- The refined requirement does not extend the scope of the original requirement; and

- The refined requirement does not alter the list of dependences of the original requirement.

Some examples of valid refinements are:

1) Any change that is only editorial, such as changes to enhance the readability of a completed assignment or to address grammatical correctness.

2) A change that does not alter the scope of the requirement due to the context in which it is used in the PP/ST. For example, changing a requirement that stated "TOE

users" to "TOE telnet users" would be a valid refinement where the only users of the TOE are telnet users.

3) A change that provides information on allowable approaches to implementation without extending the scope of the requirement. An example of a valid refinement is changing a requirement from "provide the capability to verify" to "provide the capability to verify by implementing cryptographic checksums". The change places restrictions on the nature of the mechanism to be used in implementing an existing requirement, and does not extend the scope of the original.

In CC Part 1, paragraph 199 a) and a) 1) are replaced with the following text:

This part of the PP defines the detailed IT security requirements that shall be satisfied by the TOE or its environment. The IT security requirements shall be stated as follows:

a) Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of **TOE security requirements** shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. The TOE security requirements shall be stated as follows:

1) The statement of **TOE security functional requirements** should define the functional requirements for the TOE as functional components drawn from Part 2 where

applicable.

Where AVA_SOF.1 is included in the TOE security assurance requirements (e.g. EAL2 and higher), the statement of TOE security functional requirements shall include a minimum strength level for the TOE security functions realised by a probabilistic or permutational mechanism (e.g. a password or hash function). All such functions shall meet this minimum level. The level shall be one of the following: SOF-basic, SOF-medium, SOF-high. The selection of the level shall be consistent with the identified security objectives for the TOE. Optionally, specific strength of function metrics may be defined for selected functional requirements, in order to meet certain security objectives for the TOE.

As part of the strength of TOE security functions evaluation (AVA_SOF.1), it will be assessed whether the strength claims made for individual TOE security functions and the overall minimum strength level are met by the TOE.

In CC Part 1, paragraph 215 a) and a) 1) are replaced with the following text:

This part of the ST defines the detailed IT security requirements that shall be satisfied by the TOE or its environment. The IT security requirements shall be stated as follows:

a) Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of **TOE security requirements** shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. The TOE security requirements shall be stated as follows:

1) The statement of **TOE security functional requirements** should define the functional requirements for the TOE as functional components drawn from Part 2 where applicable.

Where AVA_SOF.1 is included in the TOE security assurance requirements (e.g. EAL2 and higher), the statement of TOE security functional requirements shall include a minimum strength level for the TOE security functions realised by a probabilistic or permutational mechanism (e.g. a password or hash function). All such functions shall meet this minimum level. The level shall be one of the following: SOF-basic, SOF-medium, SOF-high. The selection of the level shall be consistent with the identified security objectives for the TOE. Optionally, specific strength of function metrics may be defined for selected functional requirements, in order to meet certain security objectives for the TOE.

As part of the strength of TOE security functions evaluation (AVA_SOF.1), it will be assessed whether the strength claims made for individual TOE security functions and the overall minimum strength level are met by the TOE.

The following changes are made to the CEM:

- The second sentence of paragraph 220 is reworded as follows:

"That is, the PP can contain IT security requirement statements that include uncompleted operations for assignment or selection."

- Paragraphs 221 and 222 are replaced by the following:

> "The permitted operations for CC Part 2 and Part 3 components are assignment, iteration, selection and refinement. The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components."

- Paragraphs 410 and 411 are replaced by the following:

> The permitted operations for CC Part 2 and Part 3 components are assignment, iteration, selection and refinement. The assignment and selection operations are permitted only where specifically indicated in a component. Iteration and refinement are permitted for all components.

Final Interpretation for RI # 24 - COTS product in TOE providing security

Date:	01 / 16 / 2001
Subject:	COTS product in TOE providing security
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 8.6 (ADV) CEM, Section 8.4 (ACM)

Issue:

A TOE includes another developer's product that provides security functionality. What evaluation evidence is required in order for the product to be included in the evaluated TOE? At issue is the developer's capability to provide sufficient configuration management (ACM), development (ADV) and vulnerability analysis (AVA) evidence for those products where the developer does not have access to proprietary information.

Interpretation

The assurance requirements apply to the entire TOE (including those products that are not under the direct control of the developer) and the relevant information must be available to the evaluator to perform the required analysis and testing.

Specific Changes

The following text is appended to the end of paragraph 34 of CEM Part 2:

> Since the assurance requirements apply to the entire TOE, evaluation evidence pertaining to all products that are part of the TOE is made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the products that are part of the TOE. For example, if a high-level design is required, then the ADV_HLD requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place (for example, ACM_CAP and ADO_DEL) will also apply to the entire TOE (including any product from another developer).

Final Interpretation for RI # 25 - Level of detail required for hardware descriptions

Date:	07/31/2001
Subject:	Level of detail required for hardware descriptions
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Annex B.6.2 CEM, Annex B.6.3

Issue:

What level of detail must be provided about the hardware and firmware of a TOE comprising vendor developed software and generic "PC" firmware/hardware? Is it sufficient to identify the TOE hardware components by their "generic" identities (e.g. Pentium-based PC, 10-Base-T Network Interface Card, SCSI disk drive)? Or is it necessary instead to specify the precise specification of each component of an evaluated configuration (e.g. Intel P5-233Mhz, Intel Starfire 2-revision 6.2 motherboard, 16Mb of 70ns EDO RAM, 3Com 3C509 NICS, Quantum Fireball 4.3 SCSI disk drive, Adaptec 2940W SCSI adapter)?

Interpretation

The hardware and firmware portions of a TOE must be described at the same level of detail as the software portions of the TOE.

In identifying the TOE as required for ASE_INT and the ETR, the level of hardware identification is determined by the impact that the hardware features have upon the security functions and assurances being claimed. The TOE identification must be as detailed as necessary to capture all security relevant information.

In describing the TSF as required by components in the ADV class, the hardware features that provide the security being claimed are described in terms of how they provide those features.

Specific Changes

- The following paragraph is inserted into section B.6.2 of the CEM after para 1817:

  > This evaluated configuration is identified in sufficient detail to differentiate hardware included in the evaluated configuration from hardware that is not included in the evaluated configuration, though it might be available as part of the product upon which the TOE is based. This identification makes it apparent to potential customers what product must be purchased, and what configuration options must be used, in order for the TOE to run securely.

- The following paragraph is inserted into section B.6.3 of the CEM after para 1818:

  > The hardware portions of the TSF are described at a level of detail commensurate with the assurance requirements related to the relevant development documentation (functional specification, high-level design, low-level design) and the testing documentation. The level of hardware identification is determined by the impact that the hardware features have upon the security functions and assurances being claimed.

Final Interpretation for RI # 27 - Events and actions

Date:	02 / 16 / 2001
Subject:	Events and actions
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 11.1 (AGD_ADM)
CEM Reference:	

Issue:

AGD_ADM.1.6C states:

> The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.1C stipulates that administrator functions must be defined. Is an event (AGD_ADM.1.6C) the same as a function (AGD_ADM.1.1C) or something different?

Interpretation

Security-relevant events and administrative functions are not identical.

Specific Changes

The following application note is added to AGD_ADM after paragraph 375:

> AGD_ADM.1.6C requires that the administrator guidance describe the appropriate administrator's reactions to all security-relevant events. Although many security-relevant events are the result of performing administrative functions, this need not always be the case (e.g. the audit log fills up, an intrusion is detected). Furthermore, a security-relevant event may happen as a result of a specific chain of administrator functions or, conversely, several security-relevant events may be triggered by one function.

Revised Final Interpretation for RI # 31 - Obvious vulnerabilties

Date:	10 / 25 / 2002
Subject:	Obvious vulnerabilties
Revision:	1
Reason for revision:	Interpretation should be captured in the document so information is not lost
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 14.4 (AVA_VLA)
CEM Reference:	CEM, Section 6.9.2 (AVA_VLA.1) CEM, Section 7.10.3 (AVA_VLA.1) CEM, Section 8.10.3 (AVA_VLA.2)

Issue:

AVA_VLA.1 requires the developer to identify and test for obvious vulnerabilities, and for evaluators to verify the adequacy of the set of identified vulnerabilities and perform penetration testing to ensure that all obvious vulnerabilities have been addressed. The CC defines 'obvious vulnerabilities'. However, information in the public domain is highly dynamic. Thus, it is conceivable (even likely) for new vulnerabilities to appear between the time that the TOE is frozen and the time that evaluators complete the Evaluation Technical Report. This leads to two obvious questions:

1) At what point in the evaluation should monitoring of the public domain for new 'obvious vulnerabilities' cease?

2) What obligation does the vendor have to address vulnerabilities, not addressed by the ST or the TOE?

Interpretation

Concerning question 1, the point at which monitoring should cease is a national scheme issue and therefore outside the scope of a Common Criteria Interpretation. It may be the case that this issue will be dealt with more directly in the context of mutual recognition.

Concerning question 2, all vulnerabilities found in the time frame defined by the scheme (see answer to question 1) that affect the TOE's ability to meet the stated requirements or counter the stated threats must be addressed either directly by TOE or through appropriate statements in the intended environment. Any other vulnerabilities are outside the scope of the evaluation and need not be addressed.

Specific Changes

In the CEM, the following paragraph is inserted after paragraphs 899, 1255, and 1722.

Information in the public domain is highly dynamic. Therefore, it is possible that new vulnerabilities are reported in the public domain between the time the developer performs the vulnerability analysis and the time that the evaluation is completed. The point at which monitoring of the public domain information ceases is an evaluation authority issue; therefore guidance and agreement should be sought from the evaluation authority.

Final Interpretation for RI # 32 - Strength of Function Analysis in ASE_TSS

Date:	10 / 15 / 2000
Subject:	Strength of Function Analysis in ASE_TSS
CC Part #1 Reference:	CC Part 1, Annex C
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 5.8 (ASE_TSS)
CEM Reference:	

Issue:

There appears to be an inconsistency between CC Part 1 (paragraph 217) and CC Part 3 (ASE_TSS.1.10.C) as to whether a strength of function analysis has to be provided in the ST.

Interpretation

The intent was not that an analysis of strength of TOE security function be required in an ST.

Specific Changes

CC Part 1, paragraph 217a)3) where it states:

> "A strength of TOE security function analysis shall be provided for all these functions."
>
> is replaced with:
>
> "A strength of TOE security function claim shall be provided for each of these functions."

The following sentence is deleted:

> "The evidence provided about the strength of function shall be sufficient to allow the evaluators to make their independent assessment and to confirm that the strength claims are adequate and correct"

Final Interpretation for RI # 33 - CC use of "Check"

Date:	10/15/2000
Subject:	CC use of "Check"
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 16.4 (AMA_SIA)
CEM Reference:	

Issue:

In AMA_SIA.*.2E the verb "check" is used. However, the evaluator action described indicates that confirm would be appropriate. Since this is the only use of "check" in CC part 3, the definition in 2.4 can be removed.

Interpretation

"Check" was used in error in AMA_SIA and "check" should be removed from section 2.4 of CC Part 3.

Specific Changes

The use of "check" in AMA_SIA.1.2E and AMA_SIA.2.2E is replaced with "confirm" and paragraph 70 of CC Part 3 is deleted.

Final Interpretation for RI # 37 - ACM on Product or TOE?

Date:	02 / 16 / 2001
Subject:	ACM on Product or TOE?
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 2.6.1 ACM
CEM Reference:	

Issue:

The ACM requirements appear to have been written with the assumption that the TOE is an entire product. When the TOE is a subset of a product, does ACM apply to the whole product?

When the sponsor of an evaluation is not the developer, does ACM apply (1) only up to the point at which the sponsor receives the TOE or (2) through the end of the evaluation?

Interpretation

The ACM requirements cover the TOE and information related to the TOE. If the TOE is a subset of an product, then only that part of the product which is the TOE need be covered by the ACM requirements.

The ACM requirements require that CM be in place and in use prior to the end of the evaluation.

Specific Changes

The following application notes are added to the “Objectives” section of CC Part 3, section 8.9 (CM capabilities (ACM_CAP)) after current paragraph 250:

> In the case where the TOE is a subset of a product, the ACM requirements apply only to the TOE configuration items, not to the product as a whole. While it is desired that CM be applied from the early design stages and continue into the future, ACM requires that CM be in place and in use prior to the end of the evaluation.

Final Interpretation for RI # 038 - Use of 'as a minimum' in C&P elements

Date:	October 31, 2003
Subject:	Use of 'as a minimum' in C&P elements
CC Part #1 Reference:	CC Part 1, Annex C.2.7
CC Part #2 Reference:	CC Part 2, Annex E.1 (FCS_CKM)
CC Part #3 Reference:	CC Part 3, Section 4.1 (APE_DES) CC Part 3, Section 8.2 (ACM_CAP) CC Part 3, Section 8.3 (ACM_SCP)
CEM Reference:	CEM v1.0, Section 7.4.2 (ACM_SCP.1) CEM v1.0, Section 8.4.3 (ACM_SCP.2)

Issue:

The CC occasionally uses the phrase 'as a minimum' in content and presentation of evidence elements. In using this phrase the CC explicitly allows the developer to provide additional information. Where this phrase is not used, does the CC imply that the developer is not allowed to provide additional information?

Interpretation

The CC allows the developer to provide additional information to that explicitly required. Therefore, the phrase 'as a minimum' is unnecessary.

Specific Changes

The following change is made to CC v2.1, Part 1:

- The phrase 'as a minimum' is deleted from paragraph 217

The following change is made to CC v2.1, Part 2:

- The first sentence of paragraph 696 is deleted. The paragraph becomes:

  > The inclusion of other stages is dependent on the key management strategy being implemented, as the TOE need not be involved in all of the key life-cycle (e.g. the TOE may only generate and distribute cryptographic keys).

The following changes are made to CC v2.1, Part 3:

- The phrase 'as a minimum' is deleted from the following elements in CC Part 3:
  APE_DES.1.1C
  ASE_DES.1.1C
  ACM_CAP.5.16C
  ACM_SCP.*.1C
  AMA_AMP.1.11C

- In CC Part 3, section 15.3.2, paragraph 549:

"As a minimum, TOE components are required to be categorised as either TSP-enforcing or non-TSP-enforcing."

is changed to:

"TOE component categorisation must indicate whether the component is TSP-enforcing or non-TSP-enforcing."

- In CC Part 3, AMA_CAT.1.1C:

"as a minimum, TOE components must be categorised as one of TSP-enforcing or non-TSP-enforcing."

is changed to:

"TOE component categorisation must indicate whether the component is TSP-enforcing or non-TSP-enforcing."

The following change is made to the CEM v1.0:

- The phrase "as a minimum" is deleted from paragraphs 952 and 1326.
- Each first line of paragraphs 955 and 1329 is changed to: "The list should include at least the following:"

Rationale

This interpretation removes the instances of 'as a minimum' as that is the phrase referenced. Other uses of similar phrases, such as 'at a minimum' and 'minimum requirements' are under consideration and will be handled under a separate intepretation in the future.

Final Interpretation for RI # 43 - Meaning of "clearly stated" in APE/ASE_OBJ.1

Date:	02/16/2001
Subject:	Meaning of "clearly stated" in APE/ASE_OBJ.1
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 4.4 (APE_OBJ) CC Part 3, Section 5.4 (ASE_OBJ)
CEM Reference:	

Issue:

ASE_OBJ.1.2C and ASE_OBJ.1.3C state that “The security objectives [...] shall be clearly stated [...]”. This seems superfluous with the coherency requirement in ASE_OBJ.1.2E.

Interpretation

Use of the term "clearly stated" in ASE_OBJ.1.2/3C and APE_OBJ.1.2/3C is essentially a duplication of the requirement for coherence in ASE_OBJ.1.2E and APE_OBJ.1.2E, and the term should be ignored.

Specific Changes

The words “clearly stated and” are deleted from APE_OBJ.1.2C, APE_OBJ.1.3C, ASE_OBJ.1.2C and ASE_OBJ.1.3C.

Final Interpretation for RI # 49 - Threats met by environment

Date:	02/16/2001
Subject:	Threats met by environment
CC Part #1 Reference:	CC Part 1, Annex B.2.5 CC Part 1, Annex C.2.5
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 4.4 (APE_OBJ) CC Part 3, Section 5.4 (ASE_OBJ)
CEM Reference:	

Issue:

CC Part 1 B.2.5 and C.2.5 state that:

> security objectives for the environment shall be clearly stated and traced back to aspects of identified threats not completely countered by the TOE [...].

In the case where the PP/ST environment contains only threats, and no OSPs or assumptions, is it allowed for a security objective for the environment to counter a threat by itself, or should it always do so in conjunction with one or more security objectives for the TOE?

Interpretation

CC Part 1 paras 196 b) and 212 b) state:

> A description of threats shall include all threats against which specific protection within the TOE or its environment is required.

This statement is interpreted to permit the inclusion of threats countered entirely by measures within the environment. The CC is interpreted as detailed in the specific changes below.

Specific Changes

The following text is inserted in CC Part 1, paras 198 and 214, after the third sentence:

> A threat may be countered by one or more objectives for the TOE, one or more objectives for the environment, or a combination of these.

The following text is inserted as a new para after paras 172 and 355 in the CEM:

A threat may therefore be addressed entirely by one or more objectives for the environment. An extreme case would be where there are no security objectives for the TOE. Whilst this remains a valid use of the PP / ST construct, a TOE for which all threats and OSPs are addressed by the environment would be of questionable utility, as for such a TOE there would be no security functional requirements for the TOE. Certification / validation of such a TOE is a scheme issue.

Revised Final Interpretation for RI # 51 - Use of documentation without C & P elements.

Date:	10/25/2002
Subject:	Use of documentation without C & P elements.
Revision:	1
Reason for revision:	Changes in CC Part 3 required corresponding CEM changes
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 9.2 (ADO_IGS) CC Part 3, Section 14.4 (AVA_VLA)
CEM Reference:	CEM, Section 6.9.2 (AVA_VLA.1) CEM, Section 7.10.3 (AVA_VLA.1) CEM, Section 8.10.3 (AVA_VLA.2)

Issue:

There are two instances where the CC does not expand on which documentation must meet the content and presentation requirements: ADO_IGS and AVA_VLA. Do these refer to the same documentation in the developer action elements?

Interpretation

The content and presentation elements of ADO_IGS and AVA_VLA families apply to the documentation identified in the developer action elements of these families.

Specific Changes

The following changes are made to CC Part 3:

ADO_IGS.*.1C is replaced with:

> **The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.**

ADO_IGS.2.2C is replaced with:

> **The installation, generation and start-up documentation shall describe procedures capable of creating a log containing the generation options used to generate the TOE in such a way that it is possible to determine exactly how and when the TOE was generated.**

The developer action elements for AVA_VLA.* are replaced with:

> **AVA_VLA.*.1D The developer shall perform a vulnerability analysis.AVA_VLA.*.2D The developer shall provide vulnerability analysis documentation.**

The content and presentation elements for AVA_VLA.1 are replaced with:

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2C The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

The content and presentation elements for AVA_VLA.2 are replaced with:

AVA_VLA.2.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for **ways** in which a user can violate the TSP.

AVA_VLA.2.2C The vulnerability analysis documentation shall describe the disposition of **identified** vulnerabilities.

AVA_VLA.2.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.2.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

The content and presentation elements for AVA_VLA.3 are replaced with:

AVA_VLA.3.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.3.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.3.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.3.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.3.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

The content and presentation elements for AVA_VLA.4 are replaced with:

AVA_VLA.4.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2C The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3C The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4C The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks. AVA_VLA.4.5C The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6C The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

The following changes are made to the CEM:

The reference to AVA_VLA.1.1C just below the section heading 6.9.2.4.1 is replaced with :

AVA_VLA.1.1C, AVA_VLA.1.2C and AVA_VLA.1.3C.

The reference to AVA_VLA.1.1C just below the section heading 7.10.3.4.1 is replaced with :

AVA_VLA.1.1C, AVA_VLA.1.2C and AVA_VLA.1.3C.

The reference to AVA_VLA.2.1C and AVA_VLA.2.2C just below the section heading 8.10.3.4.1 is replaced with :

AVA_VLA.2.1C, AVA_VLA.2.2C, AVA_VLA.2.3C and AVA_VLA.2.4C.

Final Interpretation for RI # 55 - Incorrect Component referenced in Part 2 Annexes, FPT_RCV

Date:	10/15/2000
Subject:	Incorrect Component referenced in Part 2 Annexes, FPT_RCV
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, Annex J.8 (FPT_RCV)
CC Part #3 Reference:	
CEM Reference:	

Issue:

The following text is found in the User Notes for FPT_RCV: "...the dependency from FPT_FLS.1 to ADV_SPM.1 can be argued away." This appears to be a cut-and-paste error from the User Application Notes for FPT_FLS.1.1.

Interpretation

This is a cut and paste error. The text should refer to each component from FPT_RCV, rather than to FPT_FLS.1.

Specific Changes

The final sentence of paragraph 1236 in CC Part 2 is reworded as follows:

> "If the developer provided a clear definition of the secure state and the reason why it should be considered secure, the dependency from each of the components in FPT_RCV to ADV_SPM.1 can be argued away."

Final Interpretation for RI # 056 - When can the FPT_RCV dependency on FPT_TST be argued away?

Date:	October 31, 2003
Subject:	When can the FPT_RCV dependency on FPT_TST be argued away?
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FPT_RCV CC Part 2, FPT_TST CC Part 2, Annex J (FPT)
CC Part #3 Reference:	
CEM Reference:	

Issue:

Each of the components within the FPT_RCV family has dependencies on FPT_TST.1. While it is clearly useful for the TOE to be able to test itself to ensure that it has successfully recovered from an error, it is unclear when it might be possible to argue away this dependency.

CCIMB deliberations also identified the need to provide flexibility in defining TOE capabilities for recovery and self-test in these families.

Interpretation

There is a need for additional flexibility of expression within the FPT_RCV and FPT_TST families. There is no need for a dependency between FPT_RCV and FPT_TST. The components of FPT_RCV and FPT_TST are changed to include additional operations, and additional guidance of the applicability of the dependency from FPT_RCV components to FPT_TST.1 has been provided in Annex J.

Specific Changes

The CC v2.1 Part 2 is changed as follows:

- The dependencies of FPT_RCV components on FPT_TST.1 are removed.
- The following text is appended to para 1235:
  "It is likely that the use of one of these families will be required to support the adoption of FPT_RCV. This is to ensure that the TOE will be able to detect when recovery is required.
- The following new FPT elements replace those currently existing:

  FPT_RCV.1.1 **After [assignment: list of failures/service discontinuities] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided**.

  FPT_RCV.2.1 **When automated recovery from** [assignment: list of failures / service discontinuities] **is not possible,** the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

  FPT_RCV.3.1 When automated recovery from [assignment: list of failures / service discontinuities] is not

possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_TST.1.1 **The TSF shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]] to demonstrate the correct operation of [selection: [assignment: parts of TSF], the TSF].**

FPT_TST.1.2 **The TSF shall provide authorised users with the capability to verify the integrity of [selection: [assignment: parts of TSF data], TSF data].**

- The following text is added following para 1233:

  There are different interactions between FPT_RCV and FPT_TST components to be considered when selecting FPT_RCV:

  The need for trusted recovery may be indicated through the results of TSF self-testing, where the results of the self-tests indicate that the TSF is in an insecure state and return to a secure state or entrance in maintenance mode is required.

  A failure, as discussed above, may be identified by an administrator. Either the administrator may perform the actions to return the TOE to a secure state and then invoke TSF self-tests to confirm that the secure state has been achieved. Or, the TSF self-tests may be invoked to complete the recovery process.

  A combination of a. and b. above, where the need for trusted recovery is indicated through the results of TSF self-testing, the administrator performs the actions to return the TOE to a secure state and then invokes TSF self-tests to confirm that the secure state has been achieved.

  Self tests detect a failure / service discontinuity, then either automated recovery or entrance to a maintenance mode.

- The following text is appended to para 1235:
  "It is likely that the use of one of these families will be required to support the adoption of FPT_RCV. This is to ensure that the TOE will be able to detect when recovery is required."

- The following text is added following para 1236:
  "Following recovery, it may be necessary to confirm that the secure state has been achieved through self-testing of the TSF. However, if the recovery is performed in a manner such that only a secure state can be achieved, else recovery fails, then the dependency to the FPT_TST.1 TSF self-test component may be argued away."

- The following text is added following para 1239:

  Operations
  Assignment:
  For FPT_RCV.1.1 the PP/ST author should specify the list of failures or service discontinuities (e.g. power failure, audit storage exhaustion, any failure or discontinuity) following which the TOE will enter a maintenance mode.

- The following text is inserted immediately before para 1245: "**For FPT_RCV.2.1 the PP/ST author should specify the list of failures or service discontinuities (e.g. power failure, audit storage exhaustion) following which the TOE will need to enter a maintenance mode.**"

- The following text is inserted immediately before para 1251: "**For FPT_RCV.3.1 the PP/ST author should specify the list of failures or service discontinuities (e.g. power failure, audit storage exhaustion) following which the TOE will need to**

enter a maintenance mode."

- The following text is appended to para 1300:

  In FPT_TST.1.1 the PP/ST author should specify whether the self tests are to be carried out to demonstrate the correct operation of the entire TSF, or of only specified parts of TSF.

  In FPT_TST.1.2 the PP/ST author should specify whether data integrity is to be verified for all TSF data, or only for selected data.

- The following text is appended to para 1301:

  In FPT_TST.1.1 the PP/ST author should, if selected, specify the list of parts of the TSF that will be subject to TSF self-testing.

  In FPT_TST.1.2 the PP/ST author should, if selected, specify the list of TSF data that will be verified for integrity.

Rationale
Investigation identified a lack of flexibility in these components. It may be the case that only part of the TSF needs to be tested in order to support recovery, in which case the SFR FPT_TST.1 is not met. Rather than restricting the response to this request to just provide the clarification to CC Part 2 Annex J regarding the relationship between FPT_RCV and FPT_TST, the additional issues have been addressed.

CC Part 2 Annex J provides some clarification of the relationship between FPT_RCV and FPT_TST. From this it is clear that FPT_RCV addresses recovery from "generally anticipated system failures", such as power interruptions, hardware failures or failure due to administrator error. Such failures are characterised as being easy to detect, and the emphasis is on how recovery to a secure state is achieved. In FPT_TST the emphasis is placed on testing to check for conformance to the specification of the TSF, searching for those failures that might not otherwise be evident.

It is assumed that the inclusion of a dependency of FPT_RCV on FPT_TST was to ensure that, following a system interruption, the TSF should confirm that it is operating correctly through a suite of tests. This would appear to be a flawed argument, since FPT_RCV does not require this approach. The dependency appears to impose an approach to implementing FPT_RCV, rather than identify a necessary precondition. This is particularly true of FPT_RCV.1, where the TOE need only enter a maintenance mode, and recovery requires manual intervention. The two sets of functionality are in fact separate, and the dependency should be removed.

Additional issues fixed:
FPT_TST requires a complete set of tests to ensure correct operation of the TSF. There is no operation to choose what tests are done. Therefore a situation such as this, where only certain very specific failures need to be checked for, may lead to a burdensome testing requirement if the dependency is to be satisfied. It is also the case that FPT_RCV.1 requires entry to a maintenance mode after any failure or discontinuity The dependency on FPT_TST.1 arises on the grounds that recovery is not possible without detection of a failure state through self-testing. This is true, but it may not demand the thorough testing called up by TST. It could, for example, be accomplished through a simple check for a flag being set. The need is therefore identified for additional flexibility of expression within the FPT_RCV and FPT_TST components.

Previously the list of failures / service discontinuities was not required in both RCV.2.1 and RCV.3.1, as it was viewed that were just the complement of those failures / service discontinuities listed in RCV.2.2 and RCV.3.2. This meant that the complete list of failures / service discontinuities was not explicitly specified anywhere, although all possibilities had to be addressed by the implementation of this requirement. The update now allows for the specification of the specific failures / service discontinuities that are to be considered in the implementation of this requirement, making it clear which events are considered.

It was previously necessary in FPT_RCV.1 for the TSF shall enter a maintenance mode for all failures / service discontinuities. However, this Interpretation has indicated that this is not always the case - that there are (valid) requirements for recovery from a particular subset of failures.

Final Interpretation for RI # 58 - Confusion over refinement

Date:	07/31/2001
Subject:	Confusion over refinement
CC Part #1 Reference:	CC Part 1, Annex B.2.6 CC Part 1, Annex C.2.6
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	

Issue:

With respect to requirements already identified as applying to the IT environment, is changing "The TSF shall" to "The IT environment shall" a refinement or an extension?

Interpretation

With respect to requirements already identified as applying to the IT environment, changing "The TSF shall" to "The IT environment shall" is a refinement.

Specific Changes

CC Part 1, subclause B.2.6 paragraph 199b) is changed to:

> The optional statement of **security requirements for the IT environment** shall identify the IT security requirements that are to be met by the IT environment of the TOE. The requirements in this part of the PP may be drawn from CC Part 2 and Part 3 and, if so, should be rephrased to clearly indicate that the IT environment, not the TOE, must meet the requirement. Such rephrasing is a special case of refinement and not subject to the assessment requirements associated with modified CC components. If the TOE has no asserted dependencies on the IT environment, this part of the PP may be omitted.

CC Part 1, subclause C.2.6 paragraph 215b) is changed to:

> The optional statement of **security requirements for the IT environment** shall identify the IT security requirements that are to be met by the IT environment of the TOE. The requirements in this part of the ST may be drawn from CC Part 2 and Part 3 and if so should be rephrased to clearly indicate that the IT environment, not the TOE, must meet the requirement. Such rephrasing is a special case of refinement and not subject to the assessment requirements associated with modified CC components. If the TOE has no asserted dependencies on the IT environment, this part of the ST may be omitted.

CC Part 2, paragraph 1 is changed to:

> Security functional components, as defined in this CC Part 2, are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) or the IT environment of the TOE and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Final Interpretation for RI # 62 - Confusion over source of flaw reports

Date:	07/31/2001
Subject:	Confusion over source of flaw reports
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 12.2 (ALC_FLR)
CEM Reference:	

Issue:

ALC_FLR.*.2D requires accepting and acting upon 'user' reports. The user community is only one of several potential sources for flaw reports that should be addressed. Examples of other sources include academia, computer emergency response teams, and intelligence organisations.

Interpretation

The term *user reports* is not restricted to those reports received directly from TOE users; reports from other sources cannot be ignored simply because they are not TOE users.

Specific Changes

A new second sentence is inserted into paragraph 391 of CC Part 3 v2.1. The new paragraph 391 reads:

> The flaw remediation procedures should describe the methods for dealing with all types of flaws encountered. These flaws may be reported by the developer, by users of the TOE, or by other parties with familiarity with the TOE. Some flaws may not be reparable immediately. There may be some occasions where a flaw cannot be fixed and other (e.g. procedural) measures must be taken. The documentation provided should cover the procedures for providing the operational sites with fixes, and providing information on flaws where fixes are delayed (and what to do in the interim) or when fixes are not possible.

Additionally, the use of the term *user reports* in requirements ALC_FLR.2.2D and ALC_FLR.3.2D is changed to *all reports*. The resulting rewording is:

> The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

Final Interpretation for RI # 64 - Apparent higher standard for explicitly stated requirements

Date:	02/16/2001
Subject:	Apparent higher standard for explicitly stated requirements
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 4.6 (APE_SRE) CC Part 3, Section 5.7 (ASE_SRE)
CEM Reference:	

Issue:

APE/ASE_SRE.1.5C requires measurable, objective requirements that can be systematically demonstrated. However, by the very nature of security requirements, it is not always possible to produce fully measurable and objective requirements that can be subjected to a systematic demonstration.

Interpretation

The existing CC functional and assurance requirements are to be used as models of compliance with the requirements of this family.

Specific Changes

This new paragraph is added to the application notes of the APE_SRE family following CC Part 3 paragraph 164:

> The elements APE_SRE.1.5C and APE_SRE.1.6C require that the explicitly stated IT security requirements shall be measurable and objective as well as clearly and unambiguously expressed. The existing CC functional and assurance requirements are to be used as models for compliance with these requirements.

This new paragraph is added to the application notes of the ASE_SRE family following CC Part 3 paragraph 185:

> The elements ASE_SRE.1.5C and ASE_SRE.1.6C require that the explicitly stated IT security requirements shall be measurable and objective as well as clearly and unambiguously expressed. The existing CC functional and assurance requirements are to be used as models for compliance with these requirements.

The following paragraph is appended to these CEM work-units: APE_SRE.1-5 after paragraph 281, APE_SRE.1-6 after the work unit, ASE_SRE.1-5 after paragraph 470, and ASE_SRE.1-6 after the work unit:

> The existing CC functional and assurance requirements are to be used as models for compliance with this requirement.

Final Interpretation for RI # 65 - No component to call out security function management

Date:	07/31/2001
Subject:	No component to call out security function management
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, Class FMT
CC Part #3 Reference:	
CEM Reference:	

Issue:

The CC words for the FMT class specify restrictions on roles that may perform security management functions, but fail to provide explicit requirements that the TSF provide the security management functions upon which the restrictions apply. A common argument is that restricting the functions implicitly requires that they be provided.

Interpretation

A new family is added to the FMT Class in CC Part 2 that allows specification of management functions to be provided by the TOE.

Specific Changes

To address this interpretation, the following changes are made to CC Part 2:

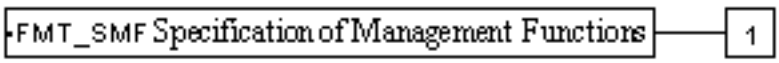
The following family is added to Clause 8, Class FMT:

8.x Specification of Management Functions (FMT_SMF)

Family Behaviour

This family allows the specification of the management functions to be provided by the TOE. Management functions provide TSFI that allow administrators to define the parameters that control the operation of security-related aspects of the TOE, such as data protection attributes, TOE protection attributes, audit attributes, and identification and authentication attributes. Management functions also include those functions performed by an operator to ensure continued operation of the TOE, such as backup and recovery. This family works in conjunction with the other components in the FMT class: the component in this family calls out the management functions, and other families in FMT restrict the ability to use these management functions.

Component Levelling



FMT_SMF.1 Specification of Management Functions requires that the TSF provide specific management functions.

Management: FMT_SMF.1

There are no management activities foreseen for this component.

Audit: FMT_SMF.1

The following events should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Use of the management functions.

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: ***[assignment: list of security management functions to be provided by the TSF].***

Dependencies: No Dependencies

The following subclause is added to Annex H, Security Management:

H.x Specification of Management Functions (FMT_SMF)

This family allows the specification of the management functions to be provided by the TOE. Each security management function that is listed in fulfilling the assignment is either security attribute management, TSF data management, or security function management.

FMT_SMF.1 Specification of Management Functions

This component specifies the management functions to be provided.

Application Note

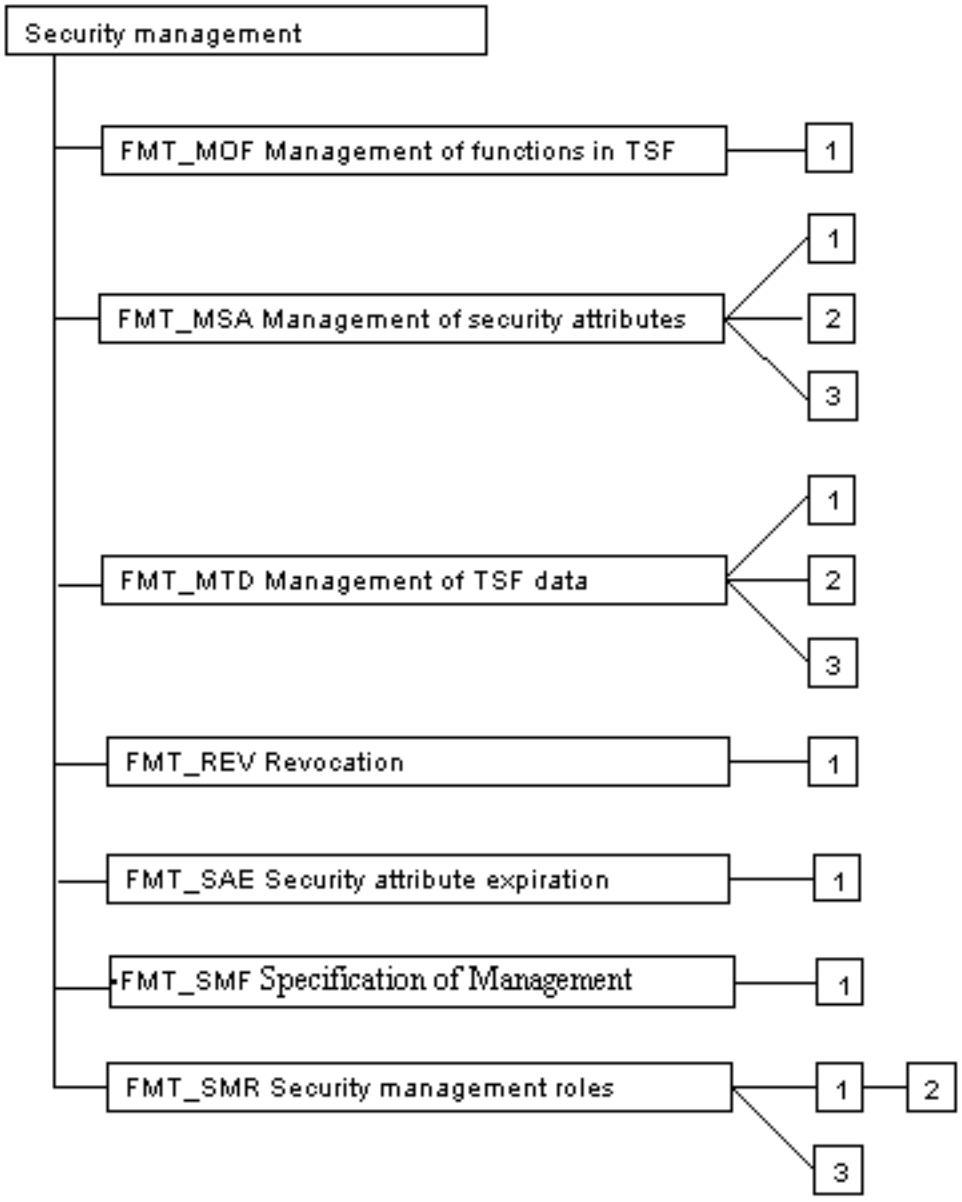
PP/ST authors should consult the “Management” sections for components included in their PP/ST to provide a basis for the management functions to be listed via this component.

Operations

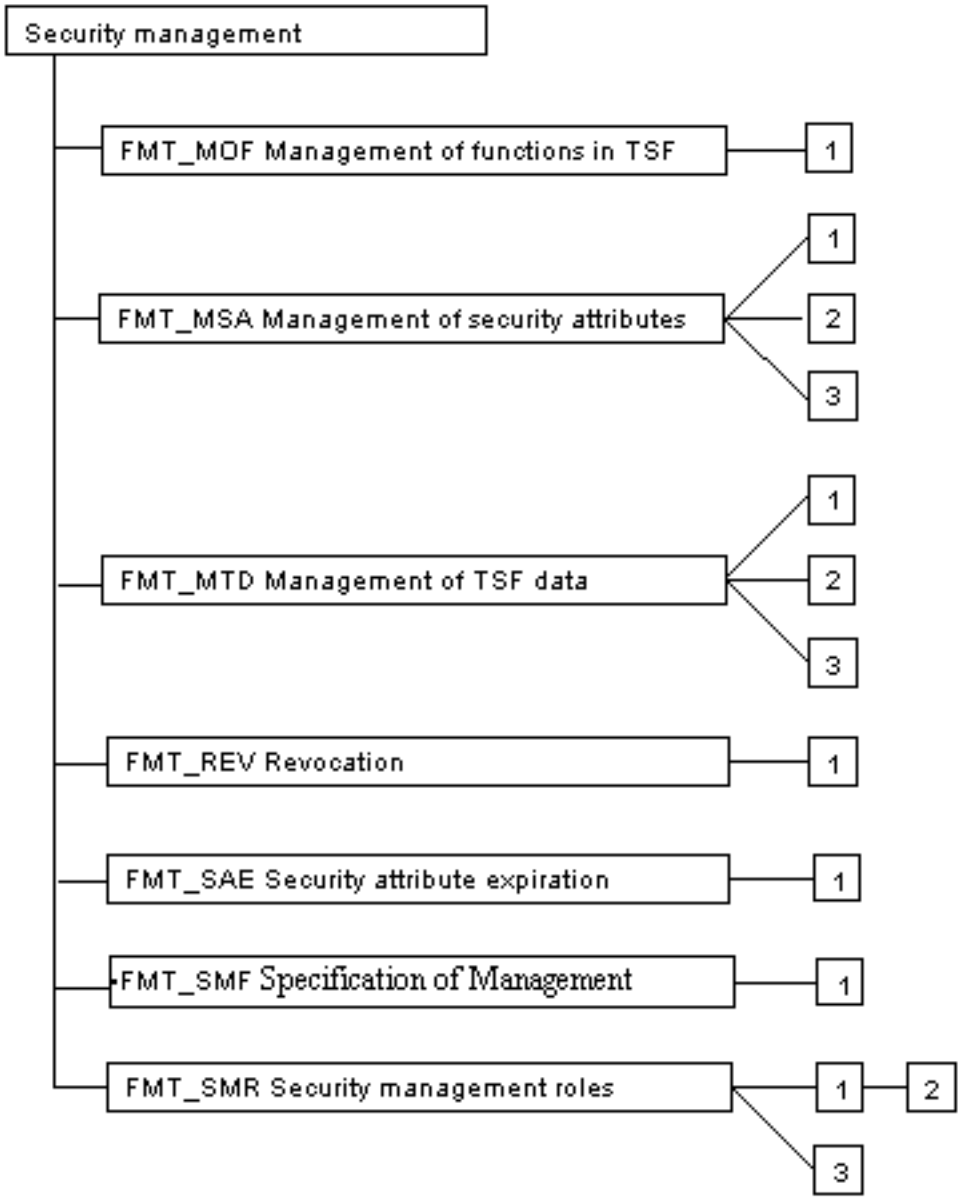
Assignment:

In FMT_SMF.1, the PP/ST author should specify the management functions to be provided by the TSF, either security attribute management, TSF data management, or security function management.

Clause 8, Figure 8.1, is modified to show an additional family, FMT_SMF Specification of Management Functions, with one component.



Clause H, Figure H.1, is modified to show an additional family, FMT_SMF Specification of Management Functions, with one hierarchical component.



The following dependency is added to FMT_MOF.1: FMT_SMF.1 Specification of Management Functions

The following dependency is added to FMT_MSA.1: FMT_SMF.1 Specification of Management Functions

The following dependency is added to FMT_MTD.1: FMT_SMF.1 Specification of Management Functions

Final Interpretation for RI # 67 - Application notes missing

Date:	10 / 15 / 2000
Subject:	Application notes missing
CC Part #1 Reference:	CC Part 1, Annex C
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	

Issue:

Annex B of CC Part 1 indicates the presence of an application notes section for a protection profile (PP), but Annex C of CC Part 1 does not for a security target (ST). Yet it appears that application notes are just as likely in an ST as in a PP.

Interpretation

Application notes are an optional part of an ST in a manner similar to PP application notes. The CC is interpreted as detailed in the specific change below.

Specific Changes

An additional subclause is added after CC Part 1 subclause C.2.8:

> "Application notes:
>
> This optional part of an ST may contain additional information considered relevant or useful for the understanding of the ST. Note that if the ST claims compliance with the requirements of a PP, it may be appropriate that certain information contained in a potential application notes section of the PP is incorporated into other sections of the ST. For example, information concerning the construction of the TOE is probably more appropriately presented in the TOE summary specification or the ST rationale than in a separate application notes section. To ease evaluation of the ST, and given that the structure for the presentation of an ST outlined in this annex is not normative, an application note containing evaluation relevant material should be a part of the section of the ST that provides the evidence for that evaluation aspect."

Final Interpretation for RI # 69 - Informal Security Policy Model

Date:	03/30/2001
Subject:	Informal Security Policy Model
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 8.6.7 (ADV_SPM.1)

Issue:

The CEM for ADV_SPM.1 defines the evaluator actions for the evaluation of the Informal TOE Security Policy Model (ISPM). It remains unclear what additional material is needed to meet this requirement over and above that supplied in the ST. Similarly, it is unclear what actions beyond those required by ASE are needed to meet the ADV_SPM requirements.

Interpretation

The requirement for an ISPM is met by a clear statement of the security policy. The need for a separate ISPM is not absolute, since for very straightforward policies, or those very clearly expressed in the ST, there may be no need for a separate ISPM. While the activities required by ASE and ADV_SPM are related (and may, in fact, be performed in concert), they are distinct.

Specific Changes

In the CEM the following paragraphs are added after paragraph 1473:

> Assurance is to be gained from an explicit and general statement of the policies underlying the TOE security functional requirements. The assurance gained is two-fold: collecting the description of each security policy into a concise whole aids in understanding the details of the policies being enforced. Additionally, such a collected description makes it much easier to see any gaps or inconsistencies (which must be sought as part of the ADV_SPM.*.3C element), and provides a clear characterisation of secure states (sought as part of the ADV_SPM.*.2C element).
>
> The requirement for an Informal Security Policy Model (ISPM) is met by a clear statement of the security policy. The need for a separate ISPM is not absolute, since for very straightforward policies, or those very clearly expressed in the ST, there may be no need for a separate ISPM. In such cases, different sections of the ST (e.g. security requirements, TOE summary specification) may combine together to provide a sufficient level of detail for the security policy. However, this is often not the case. For example, audit requirements may be spread throughout the statement of TOE security functional requirements, which may not provide a clear model of the overall policy. Unless another section of the ST (perhaps the TOE summary specification) pulls together the audit requirements into a cohesive whole, then having a separate ISPM would be necessary in order to allow for the detection of inconsistencies within the ST requirements that may otherwise pass undetected.
>
> Where a developer claims that the ISPM requirements for some or all of the security policies are met by the ST, the evaluator needs to determine that this is the case by applying the requirements of the ADV_SPM.1 component: determining that the policy is clearly expressed, and that the model is consistent with the remainder of the ST. As part of the ISPM rationale, it is likely that, in cases where the developer claims that the ISPM is met entirely by the ST, that the rationale will reference the demonstrations of suitability and correspondence between portions of the ST. When evaluating this work-unit, the evaluator may draw upon the results of the ST evaluation in this area.

In the CEM the following paragraph is added after paragraph 1475:

> Where a developer claims that the ISPM requirements for some or all of the security policies are met by the ST, the evaluator needs to determine that this is the case by applying the requirements of the ADV_SPM.1 component:

determining that the policy is clearly expressed, and that the model is complete with respect to the remainder of the ST. When evaluating this work-unit, the evaluator may draw upon the results of the evaluation of the completeness of the various portions of the ST.

Final Interpretation for RI # 74 - Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3

Date:	10 / 15 / 2000
Subject:	Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 7.9.2 (ATE_COV.2) CEM, Section 7.9.3 (ATE_DPT.1)

Issue:

In the CEM chapter for EAL3, work units ATE_COV.2-3 and ATE_DPT.1-3 have the same words and informative text. They both reference CEM section 7.9.1.3, which contains guidance pertaining to the functional specification and the high-level design. This implies that both ATE_COV.2 and ATE_DPT.1 are part of the Security Target, which may not necessarily be the case.

Thus, this guidance is misleading when only one of these assurance components is in the Security Target. Furthermore, since both work units have the same wording and informative text, this may cause confusion on the part of the evaluator as to how the work effort for these two work units might differ. Finally, section 7.9.1.3 does not address the difference in rigour between ATE_COV.2 (which has completeness requirements) and ATE_DPT.1 (which does not). The same issue pertains to these work units as they are stated in the CEM chapter for EAL4, where they both reference CEM section 8.9.1.3.

Interpretation

The guidance to the evaluator for performing the correspondence work units ATE_COV and ATE_DPT is similar but must be taken in context with the work underway. The CEM is interpreted as detailed in the specific change below.

Specific Changes

CEM paragraph 1122 is reworded as:

> "Guidance on this work units, as it pertains to the functional specification, can be found in:
>
> a) Application notes, Section 7.9.1.3, Verifying the adequacy of tests." CEM paragraph 1130 is reworded as:
> "Guidance on this work unit, as it pertains to the high-level design, can be found in:
>
> a) Application notes, Section 7.9.1.3, Verifying the adequacy of tests." CEM paragraph 1581 is reworded as:
> "Guidance on this work unit, as it pertains to the functional specification, can be found in:
>
> a) Application notes, Section 8.9.1.3, Verifying the adequacy of tests." CEM paragraph 1589 is reworded as:
> "Guidance on this work unit, as it pertains to the high-level design, can be found in:
>
> a) Application notes, Section 8.9.1.3, Verifying the adequacy of tests."

Final Interpretation for RI # 75 - Duplicate informative text for different work units

Date:	10 / 15 / 2000
Subject:	Duplicate informative text for different work units
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 8.9.4 (ATE_FUN.1) CEM, Section 8.9.5 (ATE_IND.2)

Issue:

The informative text for *:ATE_IND.2-1 is a superset of the informative text for *:ATE_FUN.1-4, and all that is added is an additional short paragraph regarding test resources. An evaluator that has recently performed *:ATE_FUN.1-4 might assume that the bulk of *:ATE_IND.2-1 has been completed due to the similarity of the informative text.

Interpretation

There is some unnecessary duplication of text in the supporting paragraphs for work units *:ATE_IND.*-1 and *:ATE_FUN.*-4.

Specific Changes

CEM paragraphs 806, 1144 and 1603 are reworded as follows:

> "It is possible for the ST to specify more than one configuration for evaluation. The TOE may be composed of a number of distinct hardware and software implementations that need to be tested in accordance with the ST. The evaluator verifies that there are test configurations identified in the developer test documentation that are consistent with each evaluated configuration described in the ST."

CEM paragraphs 617, 839, 1177 and 1636 are reworded as follows:

> "It is possible for the ST to specify more than one configuration for evaluation.The TOE may be composed of a number of distinct hardware and software implementations that need to be tested in accordance with the ST. The evaluator's TOE test configurations should be consistent with each evaluated configuration described in the ST."

CEM paragraph 616 is reworded as follows:

> "The TOE used for evaluator testing should have the same unique reference as established by the ACM_CAP.1 sub-activity."

CEM paragraph 805 is reworded as follows:

> "The TOE referred to in the developer's test plan should have the same unique reference as established by the ACM_CAP.2 sub-activity."

CEM paragraph 838 is reworded as follows:

"The TOE used for evaluator testing should have the same unique reference as established by the ACM_CAP.2 sub-activity."

CEM paragraph 1143 is reworded as follows:

"The TOE referred to in the developer's test plan should have the same unique reference as established by the ACM_CAP.3 sub-activity."

CEM paragraph 1176 is reworded as follows:

"The TOE used for evaluator testing should have the same unique reference as established by the ACM_CAP.3 sub-activity."

CEM paragraph 1602 is reworded as follows:

"The TOE referred to in the developer's test plan should have the same unique reference as established by the ACM_CAP.4 sub-activity."

CEM paragraph 1635 is reworded as follows:

"The TOE used for evaluator testing should have the same unique reference as established by the ACM_CAP.4 sub-activity."

Final Interpretation for RI # 80 - APE_REQ.1-12 does not use ‘shall examine..to determine’

Date:	10 / 15 / 2000
Subject:	APE_REQ.1-12 does not use ‘shall examine..to determine’
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 3.4.5 (APE_REQ.1)

Issue:

Work unit APE_REQ.1-12 of CEM Part 2 is inconsistent with the other work units using the verb "shall examine".

Interpretation

Evaluators 'examine' something to make a determination about it. This work unit did not make that clear. The CC is interpreted as detailed in the specific change below.

Specific Changes

Work unit APE_REQ.1-12 in the CEM is changed to:

> "The evaluator shall examine the statement of IT security requirements to determine that all uncompleted operations are identified".

Final Interpretation for RI # 84 - Aspects of objectives in TOE and environment

Date:	02 / 16 / 2001
Subject:	Aspects of objectives in TOE and environment
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 3.4.5 (APE_REQ.1) CEM, Section 4.4.6 (ASE_REQ.1)

Issue:

For APE_REQ.1.13C and ASE_REQ.1.12C, the CEM uses different wording for similar work units for the TOE and for the environment.

Interpretation

Interpret work unit APE_REQ.1-20 and ASE_REQ.1-20 to include: "are suitable to meet that security objective ***for the TOE.".***

Specific Changes

The CEM work units APE_REQ.1-20 and ASE_REQ.1-20 are changed to:

> The evaluator shall examine the security requirements rationale to determine that for each security objective for the TOE it contains an appropriate justification that the TOE security requirements are suitable to meet that security objective for the TOE.

Final Interpretation for RI # 85 - SOF Claims additional to the overall claim

Date:	02 / 11 / 2002
Subject:	SOF Claims additional to the overall claim
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 4.5 (APE_REQ) CC Part 3, Section 5.6 (ASE_REQ)
CEM Reference:	

Issue:

The circumstances under which claims are made under APE_REQ.1.11C, ASE_REQ.1.10C (CEM APE / ASE_REQ.1-16) are unclear.

Interpretation

Work units APE / ASE_REQ.1-16 refer to the case where a PP or ST author wishes to set specific SOF requirements (e.g. higher than the minimum level or by using a metric). Requirements under this heading are at the discretion of the PP or ST author, but must be consistent with other parts of the PP or ST (e.g. TOE description).

Specific Changes

In CC, Part 3 the following changes are made

The requirement APE_REQ.1.11C is updated as follows:

> The statement of security requirements shall identify all security functional requirements for which an explicit strength of function claim is required, together with the explicit strength of function claim for each such security functional requirement.

The requirement ASE_REQ.1.10C is updated as follows:

> The statement of security requirements shall identify all security functional requirements for which an explicit strength of function claim is required, together with the explicit strength of function claim for each such security functional requirement.

In the CEM the following changes are made:

- The work unit APE_REQ.1-16 is modified to state:

The evaluator ***shall check*** that the PP identifies any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific strength of function or metric as applicable.

- The following text is added to the end of paragraph 239:

This work unit refers to the case where a PP author requires to set specific SOF requirements (i.e. higher than the overall SOF claim of the PP) or by using a metric. A specific SOF claim for a TOE security functional requirement may be specified by a PP author. In the absence of any specific claim, the overall claim for the PP applies for all TOE security functional requirements stated in the PP. The evaluator should confirm the presence or absence of explicit SOF claims is consistent with other parts of the PP.

- The following new paragraph is included after paragraph 239:

A PP could potentially have varying specifications of SOF claims. There can be an overall SOF claim for a PP and within a PP the TOE security functional requirements could have a SOF claim specified for it.

- Work unit ASE_REQ.1-16 is modified to state:

The evaluator ***shall check*** that the ST identifies any specific TOE security functional requirements for which an explicit strength of function is appropriate, together with the specific strength of function or metric as applicable.

- The following text is added to the end of paragraph 428:

This work unit refers to the case where an ST author requires to set specific SOF requirements (i.e. higher than the overall SOF claim of the ST) or by using a metric. A specific SOF claim for a TOE security functional requirement may be specified by a PP author. In the absence of any specific claim, the overall claim for the ST applies for all TOE security functional requirements stated in the ST. The evaluator should confirm the presence or absence of explicit SOF claims is consistent with other parts of the ST.

- The following new paragraph is inserted after paragraph 428:

An ST could potentially have varying specifications of SOF claims. There can be an overall SOF claim for an ST and within an ST the TOE security functional requirements could have a SOF claim specified for it.

Final Interpretation for RI # 92 - Release of the TOE

Date:	07/31/2001
Subject:	Release of the TOE
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 12.2 (ALC_FLR)
CEM Reference:	

Issue:

The current wording of ALC_FLR.*.1C includes the phrase "each release of the TOE". It is unclear what this phrase means.

Interpretation

In ALC_FLR, the phrase "Each release of the TOE" refers to a product or system that is a release of a certified TOE to which changes have been applied. The flaw remediation procedures apply throughout the life-cycle of the TOE.

Specific Changes

In the CC Part 3, the following paragraph is added after paragraph 391:

> Once the evaluation of a TOE is complete, it is no longer the target for an evaluation. Furthermore, any changes to this evaluated TOE result in the original evaluation results being no longer applicable to the changed version. The phrase "release of the TOE" used in this family therefore refers to a version of a product or system that is a release of a certified TOE to which changes have been applied.

Final Interpretation for RI # 95 - SCP Dependency in ACM_CAP

Date:	02 / 16 / 2001
Subject:	SCP Dependency in ACM_CAP
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 8.2 (ACM_CAP)
CEM Reference:	

Issue:

ACM_CAP.3, .4, and .5 have a dependency on ACM_SCP.1. This is an incorrect dependency and should be deleted.

Interpretation

The dependency of ACM_CAP.3,.4 and .5 on ACM_SCP.1 is not required.

Specific Changes

The dependency of ACM_CAP.3,.4 and .5 on ACM_SCP.1 in the CC is removed.

Final Interpretation for RI # 98 - Limitation of refinement

Date:	02 / 11 / 2002
Subject:	Limitation of refinement
CC Part #1 Reference:	CC Part 1, Section 4.4.1
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	

Issue:

What is the difference between refinement and explicit requirements?

Interpretation

Any change to an existing CC requirement (from Part 2 or Part 3) is either a refinement or an extension. In order for a change to be a refinement, in lieu of an extension, the change must satisfy both the following conditions:

- a TOE meeting the changed requirement would also meet the unchanged requirement, as interpreted in the context of a particular PP or ST; and
- the changed requirement does not extend the scope of the original.

Specific Changes

The CC v2.1, Part 1, section 4.4.1.3 is updated per interpretation 019.

Final Interpretation for RI # 103 - Association Of Access Control Attributes With Subjects And Objects

Date:	7/15/2003
Subject:	Association Of Access Control Attributes With Subjects And Objects
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FDP_ACF
CC Part #3 Reference:	
CEM Reference:	

Issue:

The Common Criteria does not currently provide functional requirements for identifying the clear association of controlled entities (subjects, information) with relevant security attributes. The existing FDP_ACF family provides only for a simple list of security attributes, without the ability to describe the required association to controlled entities.

Interpretation

The statement of Access Control Policy provides a clear association of controlled entities (subjects, objects) with relevant security attributes.

Specific Changes

To address this interpretation, the following changes are made to CC v2.1, Part 2:

- The FDP_ACF.1.1 element is replaced as follows:

  > FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on the following: [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

- In Subclause F.2, the first sentence in paragraph 763 is replaced with:

  > In FDP_ACF.1.1, the PP/ST author should specify, for each controlled subject and object, the security attributes and/or named groups of security attributes that the function will use in the specification of the rules.

Final Interpretation for RI # 104 - Association of Information Flow Attributes with Subjects and Objects

Date:	07 / 15 / 2003
Subject:	Association of Information Flow Attributes with Subjects and Objects
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FDP_IFF
CC Part #3 Reference:	
CEM Reference:	

Issue:

The Common Criteria does not currently provide functional requirements for identifying the clear association of controlled entities (subjects, information) with relevant security attributes. The existing FDP_IFF family provides only for a simple list of security attributes, without the ability to describe the required association to controlled entities.

Interpretation

The statement of Information Flow Control Policy should provide a clear association of controlled entities (subjects, information) with relevant security attributes.

Specific Changes

To address this interpretation, the following changes are made to CC Part 2 v2.1:

The FDP_IFF.1.1 element is replaced as follows:

> FDP_IFF.1.1: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

The FDP_IFF.2.1 element is replaced as follows:

> FDP_IFF.2.1: The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [*assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

Subclause F.6, paragraph 810 is replaced by:

> In FDP_IFF.1.1, the PP / ST author should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The types of security attributes should be sufficient to support the environmental needs.

Subclause F.6, paragraph 822 is replaced by:

In FDP_IFF.2.1, the PP/ST author should specify, for each type of controlled subject and information, the security attributes that are relevant to the specification of the SFP rules. For example, such security attributes may be things such the subject identifier, subject sensitivity label, subject clearance label, information sensitivity label, etc. The types of security attributes should be sufficient to support the environmental needs.

Final Interpretation for RI # 111 - Settable Failure Limits are Permitted

Date:	October 31, 2003
Subject:	Settable Failure Limits are Permitted
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FIA_AFL CC Part 2, Annex G (FIA)
CC Part #3 Reference:	
CEM Reference:	

Issue:

In element FIA_AFL.1.1, the PP/ST author should specify the default number of unsuccessful authentication attempts that, when met or surpassed, will cause the TSF to perform some action or actions. Part 2, Annex G.1, paragraph 958 states that the PP/ST author may specify that the number is: "an authorised administrator configurable number". However, the wording used in element FIA_AFL.1.1 ("[assignment: number]") does not allow a phrase to be inserted

Interpretation

It should be possible for the PP/ST author to specify that the administrator is able to specify the number of unsuccessful authentication attempts permitted before the TSF performs some set of actions. This number of unsuccessful authentication attempts should be a value taken from the range of values acceptable to the PP/ST author.

The PP/ST author should specify the range of acceptable values by giving the upper and lower bounds for the range of acceptable values. The adminstrator selects a value from that range. Thus, the number of authentication attempts should be less than or equal to the upper bound and greater or equal to the lower bound values. The number of unsuccessful authentication attempts specified must be a positive integer.

Specific Changes

The CC v2.1 Part 2 is changed as follows:

- FIA_AFL.1.1 is replaced by the following:

  FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], "*an administrator configurable positive integer within* [assignment: *range of acceptable values*]"] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*]".

- In Annex G.1, FIA_AFL.1, Operations, the following is added before the "Assignment" operation:

  Selection:
  In FIA_AFL.1.1, the PP/ST author should select either the assignment of a positive integer, or the phrase "an administrator configurable positive integer" specifying the range of acceptable values of the range.

- In Annex G.1, FIA_AFL.1, Operations, paragraph 958 (the first "Assignment") is replaced with the following:

  In FIA_AFL.1.1, if the assignment of a positive integer is selected, the PP/ST author should specify the

default number (positive integer) of unsuccessful authentication attempts that, when met or surpassed, will trigger the events.

In FIA_AFL.1.1, if an administrator configurable positive integer is selected, the PP / ST author should specify the range of acceptable values from which the administrator of the TOE may configure the number of unsuccessful authentication attempts. The number of authentication attempts should be less than or equal to the upper bound and greater or equal to the lower bound values.

Rationale

This interpretation permits the specification of the number of unauthorised authentication attempts to be specified by the administrator, within a range of values acceptable to the PP / ST author. This ensures the 'number' specified is a positive integer.

Final Interpretation for RI # 116 - Indistinguishable work units for ADO_DEL

Date:	07/31/2001
Subject:	Indistinguishable work units for ADO_DEL
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 7.5.1 (ADO_DEL.1) CEM, Section 8.5.1 (ADO_DEL.2)

Issue:

There seems to be no difference between *:ADO_DEL.*-1 and *:ADO_DEL.*-2. While *:ADO_DEL.*-1 concentrates upon what is necessary, *:ADO_DEL.*-2 concentrates upon what is suitable (a distinction absent in the CC).

Interpretation

With respect to the evaluator actions associated with *:ADO_DEL.*-1 and *:ADO_DEL.*-2, there is no difference between necessity and suitability; both are in the context of the security objectives. Consequently, work unit *:ADO_DEL.*-2 adds nothing to *:ADO_DEL.*-1 (other than the examples in the second paragraph of guidance for *:ADO_DEL.*-2).

Specific Changes

The following changes are made to the CEM:

- The following paragraphs are added immediately after paragraphs 670, 966, and 1340:

  > Standard commercial practice for packaging and delivery may be acceptable. This includes shrink wrapped packaging, a security tape or a sealed envelope. For the distribution, the public mail or a private distribution service may be acceptable.
  >
  > The suitability of the choice of the delivery procedures is influenced by the TOE (e.g. whether it is software or hardware) and by the security objectives. In cases where the delivery procedures differ for different parts of the TOE, the totality of procedures are suitable to meet the overall security objectives.

- Work unit 2:ADO_DEL.1-2 and its guidance (paragraphs 671-672) are deleted.
- Work unit 3:ADO_DEL.1-2 and its guidance (paragraphs 967-968) are deleted.
- Work unit 4:ADO_DEL.2-2 and its guidance (paragraphs 1341-1342) are deleted.

Final Interpretation for RI # 120 - Sampling of process expectations unclear

Date:	07 / 31 / 2001
Subject:	Sampling of process expectations unclear
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Annex B.2

Issue:

The following sentence (CEM v1.0 part 2 section B.2 p. 348 paragraph 1791a) is poorly worded: "Where sampling relates to gaining evidence that a process (e.g. visitor control or design review), a percentage figure is not appropriate, [...]"

Interpretation

The evidence needed is that the process is being followed.

Specific Changes

The CEM, second half of paragraph 1791a, is replaced with:

> Where sampling relates to gaining evidence that a process (e.g. visitor control or design review) is being followed, a percentage figure is not appropriate. The evaluator should sample sufficient information to gain reasonable confidence that the process is being followed, and justify the sample size.

Revised Final Interpretation for RI # 127 - Work unit not at the right place

Date:	10 / 25 / 2002
Subject:	Work unit not at the right place
Revision:	1
Reason for revision:	Editorial changes for readability
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 4.4.8 (ASE_TSS.1)

Issue:

In the CEM, work unit ASE_TSS.1-6 deals with the SOF claim for functions; it should be in ASE_TSS.1.10C. In addition, it is unclear in the CEM whether the evaluator performs the analysis or the evaluator checks an analysis provided by the developer.

Interpretation

The work unit is in the right location.

The developer provides the analysis.

Specific Changes

In the CEM, paragraph 490 is changed to:

The evaluator determines that for each IT security function for which a strength of function claim is appropriate, the TOE summary specification rationale demonstrates that this claim is adequate for all TOE security functional requirements that it traces back to.

Revised Final Interpretation for RI # 128 - Coverage of the Delivery Procedures

Date:	11 / 15 / 2002
Subject:	Coverage of the Delivery Procedures
Revision:	1
Reason for revision:	This clarifies the effects of CEM text changes resulting from multiple Interpretations
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 8.5.1 (ADO_DEL.2)

Issue:

Paragraph 1338 states:
The procedures describe which parts of the TOE need to be covered by these procedures. (...) The delivery procedures refer to the entire TOE, ...

It is not clear whether the procedures cover all the TOE or just parts of the TOE.

Interpretation

The delivery documentation should cover the entire TOE, but it may contain different procedures for different parts of the TOE.

Specific Changes

Para 1338 is replaced with:

> The delivery documentation describes proper procedures to determine the identification of the TOE and to maintain security of the TOE during transfer of the TOE or its component parts. The delivery documentation contains procedures for physical or electronic (e.g. for downloading off the Internet) distribution where applicable. The delivery documentation covers the entire TOE, but may contain different procedures for different parts of the TOE.

Revised Final Interpretation for RI # 133 - Consistency analysis in AVA_MSU.2

Date:	10 / 25 / 2002
Subject:	Consistency analysis in AVA_MSU.2
Revision:	1
Reason for revision:	The specific change paragraph reference was the page reference
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	CEM, Section 8.10.1 (AVA_MSU.2)

Issue:

On Page 322, paragraph 1688 there is a reference to the annex on consistency analysis. There is no consistency analysis in this work unit so the reference to the guidance on consistency analysis is not useful.

Interpretation

Consistency analysis is not necessary in work unit 4:AVA_MSU.2-8

Specific Changes

Paragraph 1688 on page 322 of the CEM is removed.

Final Interpretation for RI # 138 - Iteration and narrowing of scope

Date:	06 / 05 / 2002
Subject:	Iteration and narrowing of scope
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, Section 2.1.4
CC Part #3 Reference:	
CEM Reference:	CEM, Section 3.4.5 (APE_REQ.1) CEM, Section 4.4.6 (ASE_REQ.1)

Issue:

The question of "narrowing of scope" (i.e., limiting the applicability of an element) has recently been debated as to whether it is an acceptable refinement. It is not clear from the CC and the CEM that all aspects of a requirement must be covered.

Interpretation

If iteration is used to narrow applicability to a portion of the TOE, the collection of all the iterations must cover all aspects of the requirement.

Specific Changes

The CC v2.1, Part 1, section 4.4.1.3 is updated per interpretation 019.

Final Interpretation for RI # 140 - Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR

Date:	07 / 15 / 2003
Subject:	Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
CC Part #1 Reference:	
CC Part #2 Reference:	
CC Part #3 Reference:	CC Part 3, Section 11 AGD
CEM Reference:	

Issue:

The CC defines the TOE as the IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. In turn, the CC explicitly defines two guidance document types: User Guidance and Administrator Guidance, however, these two documents do not include all the information that constitutes guidance to the users and administrators of the TOE.

This raises the issue of 1) who are the users of the TOE that require guidance, 2) where does the delivery, installation, and startup guidance and the flaw remediation guidance fit into the overall scheme of guidance document requirements?

The definition of the TOE should not single out specific 'types' of users. Guidance documentation is required by 'all' users of the TOE to ensure the secure delivery, installation, configuration, operation, management, and use of the TOE. As an example, that includes general users, privileged users, integrators, installers, maintainers - and the scope of such documentation covers guidance for installation, configuration, operation, general use, management use, error reporting, recovery, etc.

The TOE should be defined in terms of 1) the product or system to be evaluated and
2) the guidance documentation that supports the application and use of the TOE.

Interpretation

The TOE is defined as the IT product or system and its associated guidance documentation that is the subject of an evaluation. The scope of guidance documentation is that which is required to securely deliver, install, configure, operate, maintain and use the TOE for its intended purpose.

Specific Changes

The following changes are made to CC Part 1, Glossary:

Target of Evaluation - An IT product or system and its associated guidance documentation that is the subject of an evaluation.

Guidance Documentation - Guidance documentation describes the delivery, installation, configuration, operation, management and use of the TOE as these activities apply to the users, administrators, and integrators of the TOE. The requirements on the scope and contents of guidance documents are defined in a PP or ST.

Additionally, the following text is appended to Part 3, Clause 11, paragraph 370:

Guidance documentation includes user and administrator guidance and, when included in the assurance package, the specific guidance for users and administrators resulting from the requirements in the ADO class and the ALC_FLR family.

Final Interpretation for RI # 141 - Some Modifications to the Audit Trail Are Authorized

Date:	07 / 15 / 2003
Subject:	Some Modifications to the Audit Trail Are Authorized
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FAU_STG
CC Part #3 Reference:	
CEM Reference:	

Issue:

The second element within each component of the FAU_STG family does not distinguish between authorised and unauthorised modifications to the audit records. The modification controls imposed appear to be related only to unauthorised modifications.

Interpretation

Only unauthorised modifications are prohibited. Modifications to audit records performed in accordance with TSP are permitted.

Specific Changes

Element FAU_STG.1.2 is reworded as follows:

FAU_STG.1.2 The TSF shall be able to [selection: *prevent*, *detect*] unauthorised modifications to the audit records in the audit trail.

Element FAU_STG.2.2 is reworded as follows:

FAU_STG.2.2 The TSF shall be able to [selection: *prevent*, *detect*] unauthorised modifications to the audit records in the audit trail

Final Interpretation for RI # 150 - A Completely Evaluated ST is not Required when TOE evaluation starts

Date:	07 / 15 / 2003
Subject:	A Completely Evaluated ST is not Required when TOE evaluation starts
CC Part #1 Reference:	CC Part 1, Section 4.2.2 CC Part 1, Section 4.5.3
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	

Issue:

How complete must the ST evaluation be in order to be used as part of a TOE evaluation?

Interpretation

An evaluated ST is not required before TOE evaluation may start, however a level of completeness is required on which to base evaluation.

Specific Changes

In order to address this interpretation, the following changes are made to CC v2.1, Part 1:

- Reword Subclause 4.2.2, paragraph 110, item (a) as follows:

  a) the set of TOE evidence, which includes an ST as the basis for TOE evaluation;

- Reword Subclause 4.5.3, paragraph 161 as follows:

  The TOE evaluation is carried out against the evaluation criteria contained in Part 3 using a substantially complete ST as the basis. A substantially complete ST reduces the risk of problems later on in the evaluation process and is where all sections have been completed to an extent acceptable by the evaluation scheme and for which no significant evaluation hurdles are foreseen. The result of a TOE evaluation is to demonstrate that the TOE meets the security requirements contained in the evaluated ST.

Final Interpretation for RI # 151 - Security Attributes Include Attributes of Information and Resources

Date:	October 31, 2003
Subject:	Security Attributes Include Attributes of Information and Resources
CC Part #1 Reference:	CC Part 1, Section 2.3
CC Part #2 Reference:	
CC Part #3 Reference:	
CEM Reference:	

Issue:

There is a discrepancy between the definition of "Security attribute" in CC Part 1 and the use of the term in other portions of the CC, where security attributes are referred to in the context of information and resources.

Interpretation

The term "security attribute" also applies to security-related characteristics associated with information (under an information flow policy) and resources.

Specific Changes

In order to address this interpretation, the following changes are made to CC v2.1, Part 1:

- Reword Subclause 2.3, paragraph 46 as follows:

  > **Security attribute** - Characteristics of subjects, users, objects, information, and / or resources that are used for the enforcement of the TSP.

Rationale

No additional rationale required, the interpretation speaks for itself.

Final Interpretation for RI # 201 - "Other properties" specified by assignment

Date:	October 31, 2003
Subject:	"Other properties" specified by assignment
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FMT_MSA CC Part 2, FMT_REV CC Part 2, FPT_AMT
CC Part #3 Reference:	
CEM Reference:	

Issue:

The CC paradigm is to have PP / ST authors specify "other" information through assignment. The FMT_MSA.3, FPT_AMT.1 and FMT_REV.1 component do not follow this paradigm; the Part 2 annex explicitly calls out the use of refinement to specify the other property.

For example, in FMT_MSA.3.1, the selection of "other property" for the default values is specified by assignment.

In the Common Criteria, when arbitrary information is added, this is typically done through the assignment operation. Refinement is used in those cases where additional implementation detail is provided. This particular issue appears to be due to a case where the CC authors mistakenly used refinement instead of assignment, probably to avoid embedding an assignment within a selection. This interpretation corrects the error by making the assignment explicit..

Interpretation

The method of specifying other information in assignment operations should be consistently presented in the CC.

Specific Changes

To address this interpretation, the following changes are made to CC v2.1 Part 2:

- Subclause 8.2, FMT_MSA.3, element FMT_MSA.3.1 is replaced as follows:

  FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, [assignment: other property]*] default values for security attributes thatare used to enforce the SFP.

- Subclause 8.4, FMT_REV.1, element FMT_REV.1.1 is replaced as follows:

  FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the [selection: *users, subjects, objects, [assignment: other additional resources]*] within the TSC to [assignment: *the authorised identified roles*].

- Subclause 10.1, FPT_AMT.1, element FPT_AMT.1.1 is replaced as follows:

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorised user, [assignment: other conditions]*] to demonstrate the correct operation of the security assumptions provide by the abstract machine that underlies the TSF.

- The following sentence is deleted from paragraph 1032:

  "In case of another property, the PP / ST author should refine this to a specific property."

- The following is added before paragraph 1033:

  Assignment:
  In FMT_MSA.3.1, if the PP / ST author selects another property, the PP / ST author should specify the desired characteristics of the default values.

- Paragraph 1049 is replaced by the following paragraphs:

  In FMT_REV.1.1, the PP / ST author should specify whether the ability to revoke security attributes from users, subject, objects, or any additional resources shall be provided by the TSF.

  Assignment:
  In FMT_REV.1.1, the PP / ST author should, if additional resources is selected, specify whether the ability to revoke their security attributes shall be provided by the TSF.

- Paragraph 1181 is replaced by the following paragraphs:

  In FPT_AMT.1.1, the PP / ST author should specify when the TSF will execute the abstract machine testing, during initial start-up, periodically during normal operation, at the request of an authorized user, or under other conditions. If the tests are run often, then the end users should have more confidence that the TOE is operating correctly then if the tests are run less frequently. However, this need for confidence that the TOE is operating correctly must be balanced with the potential impact on the availability of the TOE, as often times, self tests may delay the normal operation of a TOE.

  Assignment:
  In FPT_AMT.1.1, the PP / ST author should, if other conditions is selected, specify the frequency with which the self tests will be run.

Rationale
No additional rationale is required, the interpretation speaks for itself.

Final Interpretation for RI # 202 - Selecting One or More items in a selection operation and using "None" in an assignment

Date:	8/26/2003
Subject:	Selecting One or More items in a selection operation and using "None" in an assignment
CC Part #1 Reference:	CC Part 1, Section 4.4.1
CC Part #2 Reference:	CC Part 2, FAU_GEN CC Part 2, FAU_STG CC Part 2, FMT_MSA CC Part 2, FPR_PSE CC Part 2, Annex C.2 (FAU_GEN) CC Part 2, Annex C.6 (FAU_STG) CC Part 2, Annex H.2 (FMT_MSA) CC Part 2, Annex I.2 (FPR_PSE)
CC Part #3 Reference:	
CEM Reference:	

Issue:

It is unclear if, in a selection operation, selection of multiple items is permissible.

It should be clear that more than one selection from a selection list may be made, unless it is expressly prohibited. It should also be clarified in those selection lists where selecting multiple options would introduce an internal contradiction.

It was unclear when "None" would be a valid completion in an assignment.

Interpretation

The Part 2 Annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions shall be followed unless the PP/ST author justify the deviation.

- "None" is only available as a choice for the completion of a selection if explicitly provided.

  The lists provided for the completion of selections must be non-empty. If a "None" option is chosen, no additional selection options may be chosen. If "None" is not given as an option in a selection, it is permissible to combine the choices in a selection with "and"s and "or"s, unless the selection explicitly states "choose one of".

  Selection operations may be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration should not overlap the subject of the other iterated selection, since they are intended to be exclusive.

- For the completion of assignments, the Part 2 Annexes indicate when "None" would be a valid completion.

Specific Changes

The following change is made to CC v2.1, Part 1.

Insert the following paragraphs before paragraph 149:

The Part 2 Annexes provide the guidance on the valid completion of selections and assignments. This guidance provides normative instructions on how to complete operations, and those instructions shall be followed unless the PP / ST author justify the deviation.

- "None" is only available as a choice for the completion of a selection if explicitly provided.

  The lists provided for the completion of selections must be non-empty. If a "None" option is chosen, no additional selection options may be chosen. If "None" is not given as an option in a selection, it is permissible to combine the choices in a selection with "and"s and "or"s, unless the selection explicitly states "choose one of".

  Selection operations may be combined by iteration where needed. In this case, the applicability of the option chosen for each iteration should not overlap the subject of the other iterated selection, since they are intended to be exclusive.

- For the completion of assignments, the Part 2 Annexes indicate when "None" would be a valid completion.

The following changes are made to CC v2.1, Part 2..

Annexes B through M : all the brackets of the titles are deleted.

Paragraph 10 of CC part 2, section 1.2 is changed as follows:

> Annexes B through M provide the application notes for the functional classes. This material must be seen as normative instructions on how to apply relevant operations and select appropriate audit or documentation information; the use of the auxiliary verb *should* means that the instruction is strongly preferred, but others may be justifiable. Where different options are given, the choice is left to the PP / ST author.

- Subclause 3.2, FAU_GEN.1.1 is replaced with the following:

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: *choose one of: minimum, basic, detailed, not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

- Subclause C.2, FAU_GEN.1, paragraph 567 is replaced with the following:

For FAU_GEN.1.1b, the PP / ST author should select the level of auditable events called out in the audit section of other functional components included in the PP / ST. This level is one of the following: "minimum", "basic", "detailed" or "not specified".

- Subclause C.2, FAU_GEN.1, paragraph 568, is replaced with the following:

For FAU_GEN.1.1c, the PP / ST author should assign a list of other specifically defined auditable events to be included in the list of auditable events. The assignment may comprise none, or events that could be auditable events of a functional requirement that are of a higher audit level than requested in FAU_GEN.1.1b, as well as the events generated through the use of a specified Application Programming Interface (API).

- Subclause C.2, FAU_GEN.1, paragraph 569, is replaced with the following:

For FAU_GEN.1.1c, the PP / ST author should assign, for each auditable events included in the PP / ST, either a list of other audit relevant information to be included in audit events records or none.

- Subclause C.3, FAU_SAA.1, paragraph 577, the following sentence is added to the end of the paragraph:

If there are no additional rules that the TSF should use in the analysis of the audit trail, this assignment can be completed with none.

- Subclause C.5, FAU_SEL.1, paragraph 625, the following sentence is added to the end of the paragraph:

If there are no additional rules upon which audit selectivity is based, this assignment can be completed with none.

- Subclause 3.6, FAU_STG.1.2 is replaced with the following:

FAU_STG.1.2 The TSF shall be able to [*selection: choose one of: prevent*, *detect*] modifications to the audit records in the audit trail.

- Subclause C.6, FAU_STG.1, paragraph 629, is replaced with the following:

In FAU_STG.1.2, the PP / ST author should specify whether the TSF shall prevent or only be able to detect modifications of the audit trail. Only one of these options may be chosen.

- Subclause 3.6, FAU_STG.2.2 is replaced with the following:

FAU_STG.2.2 The TSF shall be able to [*selection: choose one of: prevent*, *detect*] modifications to the audit records in the audit trail.

- Subclause C.6, FAU_STG.2, paragraph 632, is replaced with the following:

In FAU_STG.2.2, the PP / ST author should specify whether the TSF shall prevent or only be able to detect modifications of the audit trail. Only one of these options may be chosen.

- Subclause C.6, FAU_STG.2, paragraph 633 replace the last sentence with the following:

This condition can be any of the following: audit storage exhaustion, failure, attack.

- Subclause 3.6, FAU_STG.4.1 is replaced with the following:

FAU_STG.4.1 The TSF shall [*selection: choose one of: "ignore auditable events", "prevent auditable events, except those taken by the authorised user with special rights", "overwrite the oldest stored audit records"*] and [*assignment: other actions to be taken in case of audit storage failure*] if the audit trail is full.

- Subclause C.6, FAU_STG.4, paragraph 639 insert the following sentence at the end of the paragraph:

Only one of these options may be chosen.

- Subclause C.6, FAU_STG.4, paragraph 640 insert the following sentence at the end of the paragraph:

If there is no other action to be taken in case of audit storage failure, this assignment can be completed with none.

- Subclause 8.2, FMT_MSA.3.1 is replaced with the following:

FMT_MSA.3.1 The TSF shall enforce the [*assignment: access control SFP, information flow control SFP*] to provide [*selection: choose one of: restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

- Subclause H.2, FMT_MSA.3.1 insert the following sentence at the end of the paragraph:

Only one of these options may be chosen.

- Subclause 9.2, FPR_PSE.1.3 is replaced with the following:

FPR_PSE.1.3 The TSF shall [*selection: choose one of: determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [*assignment: alias metric*].

- Subclause I.2, FPR_PSE.1, paragraph 1110, insert the following sentence at the end of the paragraph:

Only one of these options may be chosen.

- Subclause 9.2, FPR_PSE.2.3 is replaced with the following:

FPR_PSE.2.3 The TSF shall [*selection: choose one of: determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [*assignment: alias metric*].

- Subclause I.2, FPR_PSE.2, paragraph 1118, insert the following sentence at the end of the paragraph:

Only one of these options may be chosen.

- Subclause 9.2, FPR_PSE.3.3 is replaced with the following:

FPR_PSE.3.3 The TSF shall [*selection: choose one of: determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [*assignment: alias metric*].

- Subclause I.2, FPR_PSE.3, paragraph 1129, insert the following sentence at the end of the paragraph:

Only one of these options may be chosen.

Final Interpretation for RI # 212 - Relationship between FPT_PHP and FMT_MOF

Date:	October 31, 2003
Subject:	Relationship between FPT_PHP and FMT_MOF
CC Part #1 Reference:	
CC Part #2 Reference:	CC Part 2, FPT_PHP CC Part 2, Annex J.7 (FPT_PHP)
CC Part #3 Reference:	
CEM Reference:	

Issue:

Management activities are incorrectly handled in FPT_PHP.1. CC v2.1 indicates that FPT_PHP.1 is dependent on FMT_MOF.1. However, FPT_PHP.1 does not require user roles to be present in order to determine whether physical tampering has occurred, although a management function could be considered for such a role.

Interpretation

FPT_PHP.1 is not dependent on FMT_MOF.1, although inclusion of the FPT_PHP.1 component in a PP or ST could require a management function for the user or role that determines whether physical tampering has occurred.

Specific Changes

The following changes are made to CC v2.1 Part 2:

- Within subclause 10.7, in the section "Management: FPT_PHP.1" paragraph 408 is replaced with:

  The following actions could be considered for the management functions in FMT:
  a) management of the user or role that determines whether physical tampering has occurred.

- In the component FPT_PHP.1, the text following "Dependencies:" is replaced with:

  No dependencies

- In Annex J.7, paragraph 1223 is replaced with:

  FPT_PHP.1 should be used when threats from unauthorised physical tampering with parts of the TOE are not countered by procedural methods. It addresses the threat of undetected physical tampering with the TSF. Typically, an authorised user would be given the function to verify whether tampering took place. As written, this component simply provides a TSF capability to detect tampering. Specification of management functions in FMT_MOF.1 should be considered to specify who can make use of that capability, and how they can make use of that capability. If this function is realised by non-IT mechanisms (e.g. physical inspection) management functions are not required.

Rationale
No additional rationale required, the interpretation speaks for itself.

Final Interpretation for RI # 222 - Meaning and use of "normative" and "informative"?

Date:	October 31, 2003
Subject:	Meaning and use of "normative" and "informative"?
CC Part #1 Reference:	CC Part 1, Section 2
CC Part #2 Reference:	CC Part 2, Section 1.2 CC Part 2, all Annexes
CC Part #3 Reference:	
CEM Reference:	CEM, Section 1.3.2

Issue:

What is the meaning of "normative" and "informative", and to what does each apply? In cases where the terms "normative" and "informative" are used, they seem to be used in a manner inconsistent with the dictionary definitions, yet there is no definition within the CC or CEM. In other cases (such as paragraph 23 of CEM Part 2, Section 1.3.2), there is no clear statement of whether guidance text accompanying work units and sub-tasks is normative or informative.

In addition, the phrase "Application Notes" is used in the context of both the CC/CEM and PPs. Are both contexts comparable?

Interpretation

The following terms are used in accordance with the ISO definitions contained in ISO/IEC Directives Part 2, Rules for the structure and drafting of International Standards: "Normative", "informative", "Shall", "Should", "May", and "Can". The ISO definition for each is to be added to the glossary in CC, Part 1.

All portions of the CC and CEM should be considered "Normative" unless specifically denoted as "Informative".

Any inconsistencies with this usage will be addressed in a future version of the CC.

Specific Changes

The following changes are made to the CC v2.1 Part 1:

- The following section is added after Subclause 2.3, Glossary:

  2.4 Reserved Terms

  The following terms are used in accordance with the ISO definitions contained in ISO/IEC Directives Part 2, Rules for the structure and drafting of International Standards: All text should be considered "Normative" unless specifically denoted as "Informative".

  Normative: Normative text is that which "describes the scope of the document, and which set out provisions." (ISO/IEC Directives, Part 2) Within normative text, the verbs "shall", "should", "may", and "can" have the ISO standard meanings described in this glossary and the verb "must" is not used. Unless explicitly labeled "informative", all CC text is normative. Any text related to meeting requirements is

considered normative.

Informative: Informative text is that which "provides additional information intended to assist the understanding or use of the document."(ISO / IEC Directives, Part 2). Informative text is not related to meeting requirements.

Shall: Within normative text, "shall" indicates "requirements strictly to be followed in order to conform to the document and from which no deviation is permitted." (ISO / IEC Directives, Part 2)

Should: Within normative text, should indicates "that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required."(ISO / IEC Directives, Part 2) The CC interprets 'not necessarily required' to mean that the choice of another possibility requires a justification of why the preferred option was not chosen.

May: Within normative text, may indicates "a course of action permissible within the limits of the document"(ISO / IEC Directives, Part 2)

Can: Within normative text, can indicates "statements of possibility and capability, whether material, physical or causal"(ISO / IEC Directives, Part 2)

The following changes are made to the CC v2.1 Part 2:

- The text of paragraph 9 is replaced with:

  Annex A provides explanatory information for potential users of the functional components including a complete cross reference table of the functional component dependencies.

- The first sentence of paragraph 10 is replaced with:
  "Annexes B through M provide explanatory information for the functional classes."

- The identifier for each of the Annexes is changed from "Informative" to "Normative".

- The text of paragraph 526 is replaced with:

  This annex contains additional guidance for the families and components defined in the elements of this CC Part 2, which may be required by users, developers or evaluators to use the components. To facilitate finding the appropriate information, the presentation of the classes, families and components in this annex is similar to the presentation within the elements.

- The text of paragraph 543 is replaced with:

  The following annexes C through M provide explanatory notes for the functional classes defined in the main body of this part of the CC.

The following changes are made to the CEM Part 2 v1.0:

- Paragraph 23 of CEM Part 2, Section 1.3.2, is changed as follows:

  Guidance text accompanying work units and sub-tasks gives further explanation on how to apply the CC words in an evaluation. The described method is normative, meaning that the verb usage is in accordance with ISO definitions for these verbs; that is: the auxiliary verb "should" is used when the described method

is strongly preferred and the auxiliary verb "may" is used where the described method(s) is allowed but no preference is indicated. (The auxiliary verb "shall" is used only for the text of work units.)

Rationale

It was the original intention of the CEM authors to make the guidance text normative. In order to avoid confusion between the guidance text and the work units or sub-tasks, it was decided by the CEM authors not to use the verb "shall"; however, this original intention is not clearly stated in the referenced paragraph. It was never the intention of the CEM authors to make any part of the CEM informative verses normative. Because the relationship of the annexes to Part 2 is the same as the relationship of the CEM to Part 3, the Part 2 annexes are likewise normative. They were inadvertently mislabelled as "informative" when v2.1 was published.

The interpretation simply makes explicit the ISO standard definitions that have always been used within the CC and restores the intended labeling of the Part 2 annexes.

Index to CCIMB Interpretations (sorted by Source CC Reference)

(as of 01 December 2003)

This index page lists the collected interpretations that have been approved by the CCIMB, sorted by CC / CEM reference. Both direct references (locations of text changes resulting from the interpretations) and indirect references (locations of text whose meaning is clarified or in other ways affected, yet not changed, by the interpretation) are included.
Dates indicate when approved.

Interpretations Related to CC Part 1

- **CC v2.1 Part 1, section 2.3**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 1, section 2.3**
  - Interpretation 140 -- Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR (15 July 2003)
  - Interpretation 151 -- Security Attributes Include Attributes of Information and Resources (31 October 2003)

- **CC v2.1 Part 1, section 4.2.2**
  - Interpretation 150 -- A Completely Evaluated ST is not Required when TOE evaluation starts (15 July 2003)

- **CC v2.1 Part 1, section 4.4.1**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 098 -- Limitation of refinement (11 February 2002)
  - Interpretation 138 -- Iteration and narrowing of scope (05 June 2002)
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (15 July 2003)

- **CC v2.1 Part 1, section 4.5.3**
  - Interpretation 150 -- A Completely Evaluated ST is not Required when TOE evaluation starts (15 July 2003)

- **CC v2.1 Part 1, section 5.3**
  - Interpretation 008 -- Augmented and Conformant overlap (31 July 2001)

- **CC v2.1 Part 1, section 5.4**
  - Interpretation 008 -- Augmented and Conformant overlap (31 July 2001)

- **CC v2.1 Part 1 Annex B**
  - Interpretation 049 -- Threats met by environment (16 February 2001)
  - Interpretation 067 -- Application notes missing in ST (15 October 2000)

- **CC v2.1 Part 1 Annex B.2.6**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 058 -- Confusion over refinement (31 July 2001)
  - Interpretation 098 -- Limitation of refinement (11 February 2002)

- **CC v2.1 Part 1, Annex C**
  - Interpretation 032 -- Strength of Function Analysis in ASE_TSS (15 October 2000)
  - Interpretation 067 -- Application notes missing in ST (15 October 2000)

- **CC v2.1 Part 1 Annex C.2.4**
  - Interpretation 049 -- Threats met by environment (16 February 2001)

- **CC v2.1 Part 1 Annex C.2.5**
  - Interpretation 049 -- Threats met by environment (16 February 2001)

- **CC v2.1 Part 1 Annex C.2.6**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 058 -- Confusion over refinement (31 July 2001)
  - Interpretation 098 -- Limitation of refinement (11 February 2002)

- **CC v2.1 Part 1 Annex C.2.7**
  - Interpretation 032 -- Strength of Function Analysis in ASE_TSS (15 October 2000)
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (11 February 2002)

Interpretations Related to CC Part 2

- **CC v2.1 Part 2 Section 1**
  - Interpretation 058 -- Confusion over refinement (31 July 2001)

- **CC v2.1 Part 2 Section 1.2**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2, section 2.1.4**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 098 -- Limitation of refinement (11 February 2002)
  - Interpretation 138 -- Iteration and narrowing of scope (05 June 2002)

- **CC v2.1 Part 2 FAU_GEN**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 FAU_STG**
  - Interpretation 141 -- Some Modifications to the Audit Trail Are Authorized (15 July 2003)
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 FDP_ACF**

- Interpretation 103 -- Association Of Access Control Attributes With Subjects And Objects (15 July 2003)

- **CC v2.1 Part 2 FDP_IFF**
  - Interpretation 104 -- Association of Information Flow Attributes with Subjects and Objects (15 July 2003)

- **CC v2.1 Part 2 FIA_AFL**
  - Interpretation 111 -- Settable Failure Limits are Permitted (31 October 2003)

- **CC v2.1 Part 2 FMT**
  - Interpretation 065 -- No component to call out security function management (31 July 2001)

- **CC v2.1 Part 2 FMT_MOF**
  - Interpretation 212 -- Relationship between FPT_PHP and FMT_MOF (31 October 2003)

- **CC v2.1 Part 2 FMT_MSA**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 FMT_REV**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)

- **CC v2.1 Part 2 FPR_PSE**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 FPT_AMT**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)

- **CC v2.1 Part 2 FPT_PHP**
  - Interpretation 212 -- Relationship between FPT_PHP and FMT_MOF (31 October 2003)

- **CC v2.1 Part 2 FPT_RCV**
  - Interpretation 056 -- When can the FPT_RCV dependency on FPT_TST be argued away? (31 October 2003)

- **CC v2.1 Part 2 FPT_TST**
  - Interpretation 056 -- When can the FPT_RCV dependency on FPT_TST be argued away? (31 October 2003)

- **CC v2.1 Part 2 Annex A**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex B**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex C**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex C.2 (FAU_GEN)**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26

August 2003)

- **CC v2.1 Part 2 Annex C.6 (FAU_STG)**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 Annex D**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex E**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex E.1 (FCS_CKM)**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CC v2.1 Part 2 Annex F**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex F.2 (FDP_ACF)**
  - Interpretation 103 -- Association Of Access Control Attributes With Subjects And Objects (15 July 2003)

- **CC v2.1 Part 2 Annex F.6 (FDP_IFF)**
  - Interpretation 104 -- Association of Information Flow Attributes with Subjects and Objects (15 July 2003)

- **CC v2.1 Part 2 Annex G**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex G.1 (FIA_AFL)**
  - Interpretation 111 -- Settable Failure Limits are Permitted (31 October 2003)

- **CC v2.1 Part 2 Annex H**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex H.2 (FMT_MSA)**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 Annex H.4 (FMT_REV)**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)

- **CC v2.1 Part 2 Annex I**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex I.2 (FPR_PSE)**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment (26 August 2003)

- **CC v2.1 Part 2 Annex J**

- Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex J.1 (FPT_AMT)**
  - Interpretation 201 -- "Other properties" specified by assignment (31 October 2003)

- **CC v2.1 Part 2 Annex J.7 (FPT_PHP)**
  - Interpretation 212 -- Relationship between FPT_PHP and FMT_MOF (31 October 2003)

- **CC v2.1 Part 2 Annex J.8 (FPT_RCV)**
  - Interpretation 055 -- Incorrect Component referenced in Part 2 Annexes, FPT_RCV (15 October 2000)
  - Interpretation 056 -- When can the FPT_RCV dependency on FPT_TST be argued away? (31 October 2003)

- **CC v2.1 Part 2 Annex K**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex L**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CC v2.1 Part 2 Annex M**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

Interpretations Related to CC Part 3

- **CC v2.1 Part 3, section 2.1.4**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 098 -- Limitation of refinement (11 February 2002)

- **CC v2.1 Part 3 Section 2.4**
  - Interpretation 009 -- Definition of "Counter" (13 April 2001)
  - Interpretation 033 -- Use of "check" in Part 3 (15 October 2000)

- **CC v2.1 Part 3, APE_DES**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CC v2.1 Part 3 APE_OBJ**
  - Interpretation 043 -- Meaning of "clearly stated" in APE / ASE_OBJ.1 (16 February 2001)
  - Interpretation 049 -- Threats met by environment (16 February 2001)

- **CC v2.1 Part 3 APE_REQ**
  - Interpretation 013 -- Multiple SOF Claims for Multiple Domains in a Single TOE (15 October 2000)
  - Interpretation 049 -- Threats met by Environment (16 February 2001)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)

- **CCv2.1 Part 3, APE_SRE**
  - Interpretation 064 -- Apparent higher standard for explicitly stated requirements (16 February 2001)

- **CC v2.1 Part 3, ASE_DES**

- Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CC v2.1 Part 3 ASE_OBJ**
  - Interpretation 043 -- Meaning of "clearly stated" in APE / ASE_OBJ.1 (16 February 2001)
  - Interpretation 049 -- Threats met by environment (16 February 2001)

- **CC v2.1 Part 3 ASE_REQ**
  - Interpretation 013 -- Multiple SOF Claims for Multiple Domains in a Single TOE (15 October 2000)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)

- **CCv2.1 Part 3, ASE_SRE**
  - Interpretation 064 -- Apparent higher standard for explicitly stated requirements (16 February 2001)

- **CC v2.1 Part 3, ASE_TSS**
  - Interpretation 032 -- Strength of Functionality Analysis in ASE_TSS (15 October 2000)

- **CC v2.1 Part 3 ASE_INT**
  - Interpretation 008 -- Augmented and Conformant overlap (31 July 2001)

- **CC v2.1 Part 3 ASE_OBJ**
  - Interpretation 043 -- Meaning of "clearly stated" in APE / ASE_OBJ.1 (16 February 2001)
  - Interpretation 049 -- Threats met by environment (16 February 2001)

- **CC v2.1 Part 3 ASE_REQ**
  - Interpretation 013 -- Multiple SOF Claims for Multiple Domains in a Single TOE (15 October 2000)
  - Interpretation 049 -- Threats met by Environment (16 February 2001)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)

- **CCv2.1 Part 3, ASE_SRE**
  - Interpretation 064 -- Apparent higher standard for explicitly stated requirements (16 February 2001)

- **CC v2.1 Part 3, ASE_TSS**
  - Interpretation 032 -- Strength of Function Analysis in ASE_TSS (15 October 2000)

- **CC v2.1 Part 3, Class ACM**
  - Interpretation 024 -- Required evaluation evidence for commercial off the shelf (COTS) products (16 February 2001)
  - Interpretation 037 -- ACM on Product or TOE? (16 February 2001)

- **CC v2.1 Part 3 ACM_CAP**
  - Interpretation 003 -- Unique identification of configuration items in the configuration list (11 February 2002)
  - Interpretation 037 -- ACM on Product or TOE? (16 February 2001)
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)
  - Interpretation 095 -- ACM_CAP dependency on ACM_SCP (16 February 2001)

- **CC v2.1 Part 3 ACM_SCP**
  - Interpretation 004 -- ACM_SCP.*.1C requirements unclear (12 November 2001)
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)
  - Interpretation 095 -- ACM_CAP dependency on ACM_SCP (16 February 2001)

- **CC v2.1 Part 3 ADO_DEL**
  - Interpretation 016 -- Objective for ADO_DEL (11 February 2002)
  - Interpretation 116 -- Indistinguishable work units for ADO_DEL (31 July 2001)

- **CC v2.1 Part 3, Class ADV**
  - Interpretation 024 -- Required evaluation evidence for commercial off the shelf (COTS) products (16 February 2001)

- **CCv2.1 Part 3 ADV_HLD**
  - Interpretation 006 -- Virtual machine description (15 October 2000)

- **CCv2.1 Part 3 ADV_SPM**
  - Interpretation 069 -- Informal Security Policy Model (30 March 2001)

- **CC v2.1, Part 3 ADO**
  - Interpretation 140 -- Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR (15 July 2003)

- **CC v2.1, Part 3 ADO_IGS**
  - Interpretation 051 -- Use of documentation without C & P elements (25 October 2002)

- **CC v2.1, Part 3 AGD**
  - Interpretation 140 -- Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR (15 July 2003)

- **CC v2.1, Part 3 AGD_ADM**
  - Interpretation 027 -- Events and functions in AGD_ADM (16 February 2001)

- **CC v2.1 Part 3 ALC_FLR**
  - Interpretation 062 -- Confusion over source of flaw reports (31 July 2001) [INCORPORATED into FLR Supplement]
  - Interpretation 092 -- Release of the TOE (31 July 2001) [INCORPORATED into FLR Supplement]
  - Interpretation 094 -- FLR Guidance Documents Missing (31 July 2001) [SUPERCEDED by FLR Supplement]
  - Interpretation 140 -- Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR (15 July 2003)

- **CC v2.1 Part 3, Class AVA**
  - Interpretation 024 -- Required evaluation evidence for commercial off the shelf (COTS) products (16 February 2001)

- **CC v2.1 Part 3 AVA_SOF**
  - Interpretation 013 -- Multiple SOF claims for multiple domains in a single TOE (15 October 2000)
  - Interpretation 032 -- Strength of Function Analysis in ASE_TSS (15 October 2000)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)

- **CCv2.1 Part 3, AVA_VLA**
  - Interpretation 031 -- Obvious vulnerabilities (16 February 2001)
  - Interpretation 051 -- Use of documentation without C & P elements (25 October 2002)

- **CCv2.1 Part 3, Section 15**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CCv2.1 Part 3, AMA_AMP**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CCv2.1 Part 3, AMA_CAT**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CCv2.1 Part 3, AMA_SIA**
  - Interpretation 033 -- Use of 'check' in part 3 (15 October 2000)

Interpretations Related to CEM Part 2

- **CEM Part 2 v1.0, Section 1.3.2**
  - Interpretation 222 -- Meaning and use of "normative" and "informative"? (31 October 2003)

- **CEM Part 2 v1.0, Chapter 2**
  - Interpretation 024 -- Required evaluation evidence for commercial off the shelf (COTS) products (16 February 2001)

- **CEM Part 2, v1.0, APE_OBJ**
  - Interpretation 049 -- Threats met by Environment (16 February 2001)

- **CEM Part 2, v1.0, APE_REQ**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 080 -- APE_REQ.1-12 does not use "shall examine...to determine" (15 October 2000)
  - Interpretation 084 -- Separate objectives for TOE and environment (16 February 2001)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)
  - Interpretation 138 -- Iteration and narrowing of scope (05 June 2002)

- **CEM Part 2, v1.0, APE_SRE**
  - Interpretation 064 -- Apparent higher standard for explicitly stated requirements (16 February 2001)

- **CEM Part 2, v1.0, ASE_ENV**
  - Interpretation 133 -- Consistency analysis in AVA_MSU.2 (25 October 2002)

- **CEM Part 2, v1.0, ASE_INT**
  - Interpretation 008 -- Augmented and Conformant overlap (31 July 2001)

- **CEM Part 2, v1.0, ASE_OBJ**
  - Interpretation 049 -- Threats met by Environment (16 February 2001)

- **CEM Part 2, v1.0, ASE_REQ**
  - Interpretation 019 -- Assurance Iterations (11 February 2002)
  - Interpretation 084 -- Separate objectives for TOE and environment (16 February 2001)
  - Interpretation 085 -- SOF Claims additional to the overall claim (11 February 2002)
  - Interpretation 138 -- Iteration and narrowing of scope (05 June 2002)

- **CEM Part 2, v1.0, ASE_SRE**
  - Interpretation 064 -- Apparent higher standard for explicitly stated requirements (16 February 2001)

- **CEM Part 2, v1.0, ASE_TSS**

- Interpretation 127 -- TSS Work unit not at the right place (25 October 2002)

- **CEM Part 2 v1.0, ACM_CAP**
  - Interpretation 003 -- Unique identification of configuration items in the configuration list (11 February 2002)

- **CEM Part 2 v1.0, ACM_SCP**
  - Interpretation 004 -- ACM_SCP.*.1C requirements unclear (12 November 2001)
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements (31 October 2003)

- **CEM Part 2 v1.0, ADO_DEL**
  - Interpretation 016 -- Objective for ADO_DEL (11 February 2002)
  - Interpretation 116 -- Indistinguishable work units for ADO_DEL (31 July 2001)
  - Interpretation 128 -- Coverage of the delivery procedures (15 November 2002)

- **CEM Part 2 v1.0, ADO_IGS**
  - Interpretation 051 -- Use of 'documentation' without C&P elements (11 February 2002)

- **CEM Part 2 v1.0, ADV_SPM**
  - Interpretation 069 -- Informal Security Policy Model (30 March 2001)

- **CEM Part 2 v1.0, ATE_COV.2**
  - Interpretation 074 -- Duplicate Informative Text for ATE_COV.2-3 and ATE_DPT.1-3 (15 October 2000)

- **CEM Part 2 v1.0, ATE_DPT.1**
  - Interpretation 074 -- Duplicate Informative Text for ATE_COV.2-3 and ATE_DPT.1-3 (15 October 2000)

- **CEM Part 2, v1.0, ATE_FUN.1**
  - Interpretation 075 -- Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

- **CEM Part 2, v1.0, ATE_IND.1**
  - Interpretation 075 -- Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

- **CEM Part 2, v1.0, ATE_IND.2**
  - Interpretation 075 -- Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1 (15 October 2000)

- **CEM, Part 2 v1.0 work unit 4:AVA_MSU.2-8**
  - Interpretation 133 -- Consistency analysis in AVA_MSU.2 (16 February 2001)

- **CEM Part 2 v1.0, AVA_VLA**
  - Interpretation 031 -- Obvious vulnerabilties (25 October 2002)
  - Interpretation 051 -- Use of 'documentation' without C&P elements (25 October 2002)

- **CEM, Part 2 v1.0 Annex B.2**
  - Interpretation 120 -- Sampling of process expectations unclear (12 November 2001)

- **CEM, Part 2 v1.0 Annex B.6**
  - Interpretation 025 -- Level of detail required for hardware descriptions (31 July 2001)
  - Interpretation 037 -- ACM on Product or TOE? (16 February 2001)

Finalised Interpretations

This index lists the collected RIs, sorted by the date each was finalised.

- **Finalised 15 October 2000**
  - Interpretation 006 -- Virtual machine description
  - Interpretation 032 -- Strength of Function Analysis in ASE_TSS
  - Interpretation 033 -- Use of 'check' in part 3
  - Interpretation 055 -- Incorrect Component referenced in Part 2 Annexes, FPT_RCV
  - Interpretation 067 -- Application notes missing in ST
  - Interpretation 074 -- Duplicate Informative Text for ATE_COV.2-3 and ATE_DPT.1-3
  - Interpretation 075 -- Duplicate Informative Text for ATE_FUN.1-4 and ATE_IND.2-1
  - Interpretation 080 -- APE_REQ.1-12 does not use "shall examine...to determine"

- **Finalised 30 October 2000**
  - Interpretation 013 -- Multiple SOF claims for multiple domains in a single TOE

- **Finalised 16 February 2001**
  - Interpretation 024 -- Required evaluation evidence for commercial off the shelf (COTS) products
  - Interpretation 027 -- Events and functions in AGD_ADM
  - Interpretation 031 -- Obvious vulnerabilities
  - Interpretation 037 -- ACM on Product or TOE?
  - Interpretation 043 -- Meaning of "clearly stated" in APE/ASE_OBJ.1
  - Interpretation 049 -- Threats met by environment
  - Interpretation 064 -- Apparent Higher Standard for Explicitly Stated Requirements
  - Interpretation 084 -- Separate objectives for TOE and environment
  - Interpretation 095 -- ACM_CAP dependency on ACM_SCP
  - Interpretation 133 -- Consistency analysis in AVA_MSU.2

- **Finalised 30 March 2001**
  - Interpretation 069 -- Informal Security Policy Model

- **Finalised 13 April 2001**
  - Interpretation 009 -- Definition of "Counter"

- **Finalised 31 July 2001**
  - Interpretation 008 -- Augmented and Conformant Overlap
  - Interpretation 025 -- Nature of extended requirements: assurance or function?
  - Interpretation 058 -- Confusion over Refinement
  - Interpretation 062 -- Confusion over source of flaw reports [INCORPORATED into FLR Supplement]
  - Interpretation 065 -- No component to call out security function management
  - Interpretation 092 -- Release of the TOE [INCORPORATED into FLR Supplement]
  - Interpretation 094 -- FLR Guidance Documents Missing [SUPERCEDED by FLR Supplement]
  - Interpretation 116 -- Indistinguishable Work units for ADO_DEL

- **Finalised 29 October 2001**
  - Interpretation 127 -- Work unit not at the right place
  - Interpretation 128 -- Coverage of the delivery procedures

- **Finalised 12 November 2001**
  - Interpretation 004 -- ACM_SCP.*.1C requirements unclear
  - Interpretation 120 -- Sampling of process expectations unclear

- **Finalised 11 February 2002**
  - Interpretation 003 -- Unique identification of configuration items in the configuration list
  - Interpretation 016 -- Objective for ADO_DEL
  - Interpretation 019 -- Assurance Iterations
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements
  - Interpretation 051 -- Use of 'documentation' without C&P elements
  - Interpretation 085 -- SOF Claims additional to the overall claim
  - Interpretation 098 -- Limitation of Refinement

- **Finalised 05 June 2002**
  - Interpretation 138 -- Iteration and narrowing of scope

- **Finalised 25 October 2002**
  - Interpretation 031 -- Obvious vulnerabilties
  - Interpretation 051 -- Use of documentation without C & P elements
  - Interpretation 127 -- TSS Work unit not at the right place
  - Interpretation 133 -- Consistency analysis in AVA_MSU.2

- **Finalised 15 November 2002**
  - Interpretation 128 -- Coverage of the delivery procedures

- **Finalised 15 July 2003**
  - Interpretation 103 -- Association Of Access Control Attributes With Subjects And Objects
  - Interpretation 104 -- Association of Information Flow Attributes with Subjects and Objects
  - Interpretation 140 -- Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
  - Interpretation 141 -- Some Modifications to the Audit Trail Are Authorized
  - Interpretation 150 -- A Completely Evaluated ST is not Required when TOE evaluation starts

- **Finalised 26 August 2003**
  - Interpretation 202 -- Selecting One or More items in a selection operation and using "None" in an assignment

- **Finalised 31 October 2003**
  - Interpretation 038 -- Use of 'as a minimum' in C&P elements
  - Interpretation 056 -- When can the FPT_RCV dependency on FPT_TST be argued away?
  - Interpretation 111 -- Settable Failure Limits are Permitted
  - Interpretation 151 -- Security Attributes Include Attributes of Information and Resources
  - Interpretation 201 -- "Other properties" specified by assignment
  - Interpretation 212 -- Relationship between FPT_PHP and FMT_MOF
  - Interpretation 222 -- Meaning and use of "normative" and "informative"?