
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/2.2/007

24 March 2005

Status : Endorsed for use in UK Scheme

Effective from: 24 March 2005

Subject: Verdict justifications in CEM compliant evaluations

REFERENCES CEM, Version 2.2, January 2004

Note The interpretation is formulated for the EAL4 assurance level. The basis which it offers for deriving equivalent interpretations for lower assurance levels is discussed in paragraph 20.

Issue

1. CEM section 1.4 outlines the process by which verdicts are assigned by the evaluator. It states (paragraph 27) that the most granular structure to which a verdict is assigned is the evaluator action element (this includes implicit evaluator actions identified by CEM).
2. CEM section 2.3.4.3.4 provides further elaboration on how the results of a TOE evaluation should be presented in an ETR, in terms of these assigned verdicts. In particular:
 - a) Paragraph 105 states that the ETR must include a verdict for each assurance component and a supporting rationale, as a result of performing the corresponding CEM action and its constituent work units.
 - b) Paragraph 106 states that this rationale justifies the verdict, and notes that the rationale **may** provide detail to the level of a CEM work unit.
 - c) Paragraph 106 goes on to say that the verdict is justified *using the CC, the CEM, any interpretations and the evaluation evidence examined*. The rationale *shows how the evaluation evidence does or does not meet each aspect of the criteria* and includes a *description of the work performed, the method used, and any derivation of results*.
3. Similar paragraphs apply to PP evaluation (CEM section 2.3.4.2.3).
4. Whilst the process of assigning verdicts is clear enough, CEM provides little guidance on the level of detail expected in an ETR to **justify** the verdicts. Although a justification to the granularity of work units is not mandated, it is not obvious what alternative approach would provide a convincing demonstration that the work was performed in accordance with CEM. And if the ETR **does** report the results to this granularity, the question then remains as to what level of detail is appropriate for each work unit.

5. This lack of clarity promotes inconsistency in the amount of detail provided in ETRs. In particular, CEM generally provides guidance for each work unit describing recommended or ‘preferred’ approaches. Some evaluators and certifiers have assumed this to imply that an ETR needs to explicitly demonstrate that each such ‘preferred approach’ has been fully applied. This is undesirable, for several reasons:
 - a) It results in lengthy ETRs which are expensive both to produce and to review.
 - b) By focusing on the ‘fine print’ it can result in evaluators and certifiers losing sight of the ‘big picture’, i.e. the overall goal of gaining confidence in the absence of exploitable vulnerabilities.
 - c) It can lead to a proliferation of ORs identifying technical non-compliances with the criteria which do not signify much in assurance terms. This can in turn encourage a perception amongst sponsors and developers that evaluation is mainly concerned with ensuring that the documentation is perfect rather than finding vulnerabilities.
6. Nonetheless, the requirement to justify verdicts is an important one. If sensibly applied, it can make a significant contribution to assurance by requiring the evaluator to defend their results, and by discouraging a superficial approach to evaluation (characterised in some quarters as ‘box-ticking’) that reduces the cost at the expense of a reduction in technical understanding and consequently in assurance. Therefore, this interpretation proposes a balanced approach to the justification of verdicts which will minimise costs **without** compromising assurance, and lead to more concise and better focused ETRs.

Interpretation

Assignment of verdicts

7. Verdicts must be assigned for all applicable evaluator action elements, whether explicitly defined in CC Part 3 or identified as an implicit evaluator action in CEM. Verdicts are **not** to be assigned at any finer granularity than this, e.g. to the level of the CEM work unit.

Justification of verdicts

8. The justification of verdicts for CEM evaluator actions should be provided to the granularity of the CEM work unit. In other words, the ETR should provide a report for each work unit which contributes to the verdict justification for the CEM evaluator action with which it is associated.
9. Verdict justifications do **not** need to demonstrate coverage of individual CEM paragraphs associated with work units. Provided the ETR contains a clear statement to the effect that the CEM has been followed except where explicitly stated otherwise, then it should be clearly understood by the reader that, if there is no explicit statement of deviation from the ‘preferred approaches’, the relevant CEM guidance has been applied. This general rule is qualified only by the requirements detailed at paragraph 12 below.
10. The level of detail that must be provided for an individual work unit varies according to its type. As a general principle, work units associated with the standard *check content and presentation of evidence* evaluator actions will usually require no more than pointers to the evidence that

satisfies the requirement. In contrast, other evaluator actions (which usually require some form of independent analysis or testing) will require a more detailed justification to demonstrate that the approach has been complete and sufficiently thorough.

11. A study of the CEM work units reveals, however, that this general principle is an oversimplification. In reality, there are a number of different types of work unit that can be identified, and different approaches are appropriate in different cases.
12. The following categories of work unit report are therefore identified (note that no specific category is needed for those CEM work units for which the definition includes the words *shall record*; these work units are adequately catered for by the categories identified):

a) **Reference**

This type is appropriate where the work unit relates to a specific *content and presentation of evidence* requirement and a specific document reference can be given, e.g. to a particular section of a design document. A simple reference is all that is needed for the work unit report in such cases.

b) **Elaborated Reference**

This type is again appropriate for work units for *content and presentation of evidence* requirements. However, for this type a simple reference is insufficient, and needs to be elaborated in some way. The following cases are identified:

- Where a single reference would be too general (e.g. the required information is distributed throughout one or more documents). In such cases the reference needs to be elaborated by describing how specific instances of the evidence can be located (e.g. describing how to identify a named external TSF interface, or how the evidence addresses the requirement).
- Where the work unit, or the associated CEM guidance, indicates that coverage with respect to a particular aspect is important. In such cases references should be given for each aspect. Examples include ALC_DVS.1-1 (where coverage of different types of security measure should be demonstrated as described in [CEM, 1446]) and AVA_MSU.2-4 (where coverage of individual assumptions should be demonstrated).

c) **Affirmation**

For this type the CEM requires the evaluator to affirm that the evidence exhibits some specific property (e.g. that it is coherent or free from inconsistencies). In these cases a simple affirmation in the ETR is all that is required for the work unit report (this assumes that a reference has already been given in the ETR to the evidence examined). It should be noted that this type generally applies where:

- the evidence being examined is localised and relatively brief (e.g. checking for inconsistencies in the ST introduction), or

- the CEM guidance offers no form of ‘completeness checklist’ (e.g. the check for inconsistencies in the functional specification), or
- the nature of the work unit is such that any elaboration would add little to assurance (e.g. checking conformance of SFRs to CC Part 2).

d) **Elaborated Affirmation**

This type is similar to the ‘Affirmation’ type, but some form of elaboration is required. The following types are identified:

- Where a specific reference to a developer-provided justification or mapping is needed.
- Where it is necessary to elaborate (in the form of a brief summary) **how** the developer has met the requirement as well as affirming that the evidence meets it (e.g. AVA_VLA.2-2, where the developer’s analysis of potential vulnerabilities should be outlined).
- Where the evidence was sampled. In such cases the affirmation needs to be elaborated by an identification of the sample chosen as well as a description of a sampling approach adopted.
- Where coverage may need to be demonstrated with respect to a checklist that is implied by either the work unit definition or the associated CEM guidance to demonstrate the rigour of the evaluator’s examination. This applies where a failure to cover all relevant aspects would introduce a significant likelihood that a vulnerability is overlooked. Examples include ATE_IND.2-10 (where the results of individual tests should be indicated) and AVA_MSU.2-10 (where affirmation should be provided for each identified mode of operation).

e) **Report**

Such types are explicitly identified by inclusion of the words *shall report* in the CEM work unit definition. In such cases the evaluators need to provide the information required by CEM in the ETR, or reference the work unit reports which satisfy the requirement. The evaluator should aim to provide a concise summary of the information required rather than a comprehensive blow-by-blow account. (This general guidance applies in the absence of any specific direction to the contrary, e.g. as might appear in the CCRA.)

f) **Analysis**

The CC or CEM work unit requires the evaluator to perform some form of independent analysis or testing. Generally, these will be the ‘additional’ evaluator actions (i.e. other than the standard *check content and presentation of evidence* action) associated with an assurance component, but this is not always the case. For example, this type is also appropriate where CC requires some form of developer analysis which the evaluators may validate through their own independent analysis; this may apply to the *content and presentation of evidence* work units where there is no other explicit work unit to

independently validate the developer analysis. The following types are identified according to how the rigour of the evaluator's analysis is to be demonstrated:

- Where a description of the evaluator's approach needs to be provided (typically this applies where there is no implied checklist in CC or CEM, and where a number of different approaches are possible; examples include ACM_AUT.1-2, ADO_DEL.2-4 and ATE_IND.2-4).
 - Where completeness or sufficiency needs to be demonstrated with respect to some specific aspect (e.g. coverage of SFs or generic types of vulnerability). For each such aspect, mere affirmation of the absence of problems is in itself insufficient; to demonstrate proper consideration, the evaluators need to give, for each aspect, a description of their approach and/or findings and conclusions. For example, in the case of traceability analysis, this takes the form of a brief summary of the role of key TSF components in achieving each SF. In the case of development environment activities it includes a summary of the findings from each interview conducted with descriptions of relevant characteristics of the example evidence examined.
13. The descriptions in the above list relate to the cases where performing the work unit revealed no problems. All required ORs and other concerns should be discussed, with the justification for clearance of any given OR reported to a level commensurate with the report for the associated work unit(s). Note that this does not require full repetition of details relating to their history and impact, where previously documented and supplied to the CB; however the ETR should always present an accurate picture of the status of ORs, and their relationship to verdicts, at the time that the ETR is issued.

Application of the Interpretation

14. Annex A demonstrates application of this interpretation by assigning all EAL4 work units to one of the categories listed at paragraph 12 above, thereby identifying the type of information that should be reported in the ETR for that work unit in order to support the assignment of a **pass** verdict for the corresponding evaluator action.
15. It should be noted that Annex A indicates the **minimum** level of justification required in an ETR. Where the claims made for the TOE include factors such as a multi-platform element, or where a requirement is met in a novel or particularly complex way, there may be a need for additional explanation to support the assigned verdict, beyond that indicated in this categorisation. As appropriate a certifier may therefore request additional evidence to support a verdict justification, but such requests **must** always be justified in terms of any (relevant) significant concern that the evaluator may have overlooked a vulnerability.
16. It should also be noted that aspects of the interpretation may be superseded by other interpretations of the CEM work units.
17. For some work units, additional details may need to be provided to satisfy CEM or CCRA reporting requirements (e.g. a definition of the architecture, testing and evaluated configuration), or to provide recommendations for inclusion in the Certification Report (CR) (e.g.

recommendations for secure use of the TOE), or to provide consumer-relevant information for inclusion in the CR (e.g. TOE delivery aspects).

18. In some instances it may be appropriate for the certifier to be provided with a copy of a particular deliverable (or extract) in order to avoid undue repetition of information in the ETR (e.g. AVA_VLA.2-2, where the developer's analysis of potential vulnerabilities should be outlined).
19. Annex A notes a number of instances where work units are interrelated. The key requirement is that the evaluator performs the work in a sensible manner, and provides an intelligible presentation of the necessary information to the certifier, without being over-constrained by the defined work units.
20. This interpretation is also generally applicable to EAL1 to EAL3. A subset of Annex A commensurate with the relevant assurance components will apply. However care should be taken where the EAL4 categorisation reflects the interrelationship of work units (e.g. the AVA_MSU.2-3 requirement to give references to the documentation of SFs relates also to AGD_ADM.1-1 and AGD_USR.1-2; below EAL3 these references would need to be provided for AGD_ADM.1-1 and AGD_USR.1-2).
21. There is potential tension between the objective of providing an appropriate level of verdict justification for a given evaluation and the possible objective of collating and recording further information which would aid a subsequent re-evaluation. The focus of this interpretation is on the former objective, although it does not exclude the possibility, where desired by the sponsor, of additional information being assembled to aid a subsequent re-evaluation.

Rationale

22. The interpretation at paragraph 7 is no more than a restatement of the CEM requirements. However, it is worth noting that there is no value in trying to assign verdicts at the level of the work unit, given that this is not required by CEM, and given the stated desire to avoid a focus on the ‘fine print’ of CEM. Reports for individual work units only **contribute** to a verdict justification, and need to be viewed in conjunction with the reports for other related work units. Furthermore, there are several cases where a ‘work unit verdict’ would make no sense (e.g. AVA_VLA.2-6, ATE_IND.2-11).
23. The approach to justifying verdicts in an ETR is based on an underlying philosophy of needing to ensure that the ETR demonstrates that all ‘significant concerns’ have been addressed. In this context a *significant concern* relates to the possibility that a vulnerability might be missed by the evaluator (cf. Level 2 ORs), or that a specific CC requirement might not be met (cf. Level 4 ORs).
24. For example, in the case of independent validation of the security objectives rationale, the evaluators must first determine whether the specified security objectives are suitable to counter the identified threats; if this fails then a Level 2 OR must be raised. However, it may be the case that the security objectives **are** suitable, but that the ST rationale is inadequate for some reason, causing a failure against ASE_OBJ.1.4C; in this case a Level 4 OR must be raised. For the work unit ASE_OBJ.1-4, the ‘significant concerns’ are therefore, for each threat:
 - a) Are the security objectives suitable to counter it?
 - b) Does the ST rationale provide an appropriate justification for suitability?
25. The verdict justification in the ETR must therefore explicitly address both these concerns (see Annex A).
26. A fundamental principle is that in demonstrating that *significant concerns* have been addressed, a work unit report must add value to the ETR, and in so doing demonstrate understanding of the evidence examined. With this in mind, it should be noted that the following neither adds value to an ETR nor demonstrates understanding:
 - a) Use of ‘stock phrases’ from CEM (cf. paragraph 5 above).
 - b) Repetition of information from the evidence examined (however, see paragraph 18).
27. In many cases, the *significant concern* is represented by the CEM work unit itself. For these cases the ETR need go no further than demonstrate that the work unit is addressed. This applies in the **Reference** and **Affirmation** types described above. These are typically associated with *content and presentation of evidence* checks, where normally the concern is that sufficient information is provided on which to base subsequent independent analysis. The ‘proof of the pudding’ thus lies in the report for the subsequent analysis. Any additional information in the work unit report would be nugatory, as the evaluation result is obtained from an examination that cannot be usefully captured in the ETR, except by using ‘stock phrases’ or by simply regurgitating

extracts from the evidence provided.

28. In other cases, the *significant concerns* are at a finer granularity than the work unit definition. This leads to the **Elaborated Reference** and **Elaborated Affirmation** types. Often in these cases the work unit can be viewed as being repeated or iterated for each important aspect (e.g. threats, SFs). In others the CEM guidance presents some form of checklist which can be used to demonstrate completeness. However, this does not mean that references or affirmations must be elaborated in **all** cases where issues of completeness arise. A judgement has to be made regarding the likelihood that a vulnerability might be overlooked, and whether an elaboration would add value to the ETR. For example, including an explicit affirmation of conformance to CC Part 2 for every SFR in the ST would add no value to the ETR; furthermore, in this case a failed check would (in itself) be unlikely to lead to a vulnerability. A simple affirmation is therefore sufficient for the work unit ASE_REQ.1-3 (see Annex A).
29. Finally (leaving aside the self-explanatory **Report** type), there is the **Analysis** type, for which the evaluators are required to perform some form of independent analysis. Here the *significant concern* is not simply the result of the activity, but also whether the evaluators have fully understood the key issues or whether they have overlooked something important. This is reflected in the need to demonstrate coverage and understanding in the work unit report, but to do so in a concise and focused way.

Annex A

Application of the Interpretation to EAL4 Evaluation

ST Evaluation

Evaluation of ST Introduction (ASE_INT.1)

CEM Work Unit	Type	Comment
<i>ASE_INT.1.1E – Check content and presentation of evidence</i>		
ASE_INT.1-1	Reference	
ASE_INT.1-2	Reference	
ASE_INT.1-3	Reference	
<i>ASE_INT.1.2E – Confirm ST introduction is coherent and internally consistent</i>		
ASE_INT.1-4	Affirmation	That the ST introduction is coherent
ASE_INT.1-5	Affirmation	That no internal inconsistencies were found
<i>ASE_INT.1.3E – Confirm ST introduction is consistent with other parts of ST</i>		
ASE_INT.1-6	Affirmation	That no inconsistencies were found between ST introduction and rest of ST

Evaluation of TOE Description (ASE_DES.1)

CEM Work Unit	Type	Comment
<i>ASE_DES.1.1E – Check content and presentation of evidence</i>		
ASE_DES.1-1	Reference	
ASE_DES.1-2	Reference	
ASE_DES.1-3	Reference	
<i>ASE_DES.1.2E – Confirm TOE description is coherent and internally consistent</i>		
ASE_DES.1-4	Affirmation	That the TOE description is coherent
ASE_DES.1-5	Affirmation	That no internal inconsistencies were found
<i>ASE_DES.1.3E – Confirm ST description is consistent with other parts of ST</i>		
ASE_DES.1-6	Affirmation	That no inconsistencies were found between TOE description and rest of ST

Evaluation of Security Environment (ASE_ENV.1)

CEM Work Unit	Type	Comment
<i>ASE_ENV.1.1E – Check content and presentation of evidence</i>		
ASE_ENV.1-1	Reference	

CEM Work Unit	Type	Comment
ASE_ENV.1-2	Reference	
ASE_ENV.1-3	Reference	
<i>ASE_ENV.1.2E – Confirm TOE security environment is coherent and internally consistent</i>		
ASE_ENV.1-4	Affirmation	That the statement of TOE security environment is coherent
ASE_ENV.1-5	Affirmation	That no inconsistencies were found between different parts of the statement of TOE security environment

Evaluation of Security Objectives (ASE_OBJ.1)

CEM Work Unit	Type	Comment
<i>ASE_OBJ.1.1E – Check content and presentation of evidence</i>		
ASE_OBJ.1-1	Reference	
ASE_OBJ.1-2	Affirmation*	That each TOE security objective is traced back to at least one threat or OSP (referencing the mappings)
ASE_OBJ.1-3	Affirmation*	That each security objective for the environment is traced back to at least one threat, OSP or assumption (referencing the mappings)
ASE_OBJ.1-4	Affirmation*	For each threat, that: a) it is suitably countered by the security objectives; b) that the security objectives rationale provides an appropriate justification (referencing the rationale).
ASE_OBJ.1-5	Affirmation*	For each OSP, that: a) it is suitably met by the security objectives; b) that the security objectives rationale provides an appropriate justification (referencing the rationale).
ASE_OBJ.1-6	Affirmation*	For each assumption, that: a) it is suitably met by the security objectives; b) that the security objectives rationale provides an appropriate justification (referencing the rationale).
<i>ASE_OBJ.1.2E – Confirm security objectives complete, coherent and consistent</i>		
ASE_OBJ.1-7	Affirmation	That the security objective statements are coherent
ASE_OBJ.1-8	Affirmation	That the security objectives are complete
ASE_OBJ.1-9	Affirmation	That the security objectives are internally consistent

Evaluation of PP Claims (ASE_PPC.1)

CEM Work Unit	Type	Comment
<i>ASE_PPC.1.1E – Check content and presentation of evidence</i>		
ASE_PPC.1-1	Reference	
ASE_PPC.1-2	Reference	

CEM Work Unit	Type	Comment
ASE_PPC.1-3	Reference	
<i>ASE_PPC.1.2E – Confirm PP claims are valid</i>		
ASE_PPC.1-4	Affirmation	That all operations on SFRs or SARs are within the bounds of the PP(s) claimed

Evaluation of IT Security Requirements (ASE_REQ.1)

CEM Work Unit	Type	Comment
<i>ASE_REQ.1.1E – Check content and presentation of evidence</i>		
ASE_REQ.1-1	Reference	
ASE_REQ.1-2	Affirmation	That CC Part 2 component references are correct
ASE_REQ.1-3	Affirmation	That CC Part 2 components are correctly reproduced
ASE_REQ.1-4	Reference	
ASE_REQ.1-5	Affirmation	That CC Part 3 component references are correct
ASE_REQ.1-6	Affirmation	That CC Part 3 components are correctly reproduced
ASE_REQ.1-7	Affirmation*	That an EAL is included, or a justification provided (giving reference)
ASE_REQ.1-8	Affirmation*	That there is an appropriate justification of the assurance requirement (giving reference)
ASE_REQ.1-9	Reference	
ASE_REQ.1-10	Affirmation*	That completed operations are identified, stating the method used
ASE_REQ.1-11	Affirmation	That all assignment and selections are performed
ASE_REQ.1-12	Affirmation	That all operations are performed correctly
ASE_REQ.1-13	Affirmation*	Of the extent to which dependencies are satisfied (referencing any dependency analysis)
ASE_REQ.1-14	Affirmation*	That there is an appropriate justification for non-satisfaction of dependencies (referencing the rationale)
ASE_REQ.1-15	Reference	
ASE_REQ.1-16	Reference	
ASE_REQ.1-17	Affirmation*	That SOF rating is consistent with security objectives (referencing the rationale)
ASE_REQ.1-18	Affirmation*	That each TOE SFR is traced back to at least one TOE security objective (referencing the mappings)
ASE_REQ.1-19	Affirmation*	That each IT environment security requirement is traced back to at least one security objective for the IT environment (referencing the mappings)

CEM Work Unit	Type	Comment
ASE_REQ.1-20	Affirmation*	For each TOE security objective, that: a) it is suitably met by the TOE SFRs; b) that the security requirements rationale provides an appropriate justification (referencing the rationale).
ASE_REQ.1-21	Affirmation*	For each IT environment security objective, that: a) it is suitably met by the IT environment security requirements; b) that the security requirements rationale provides an appropriate justification (referencing the rationale).
ASE_REQ.1-22	Reference	
ASE_REQ.1-23	Affirmation*	That: a) the set of IT security requirements is mutually supportive; b) the security requirements rationale provides an appropriate justification (referencing the rationale).
<i>ASE_REQ.1.2E – Confirm IT security requirements are coherent, complete and internally consistent</i>		
ASE_REQ.1-24	Affirmation	That IT security requirements are coherent
ASE_REQ.1-25	Affirmation	That IT security requirements are complete
ASE_REQ.1-26	Affirmation	That no inconsistencies or conflicts were found between IT security requirements

Evaluation of Explicitly Stated IT Security Requirements (ASE_SRE.1)

CEM Work Unit	Type	Comment
<i>ASE_SRE.1.1E – Check content and presentation of evidence</i>		
ASE_SRE.1-1	Reference	
ASE_SRE.1-2	Reference	
ASE_SRE.1-3	Affirmation*	That an appropriate justification is provided (giving reference)
ASE_SRE.1-4	Affirmation	That CC Part 2 or Part 3 is used as a model for presentation
ASE_SRE.1-5	Affirmation	That requirements are measurable and objective
ASE_SRE.1-6	Affirmation	That requirements are clear and unambiguous
ASE_SRE.1-7	Affirmation*	That the assurance requirements are applicable and appropriate (referencing the rationale)
<i>ASE_SRE.1.2E – Determine that dependencies have been identified</i>		
ASE_SRE.1-8	Affirmation*	For each explicitly stated requirement, that no applicable dependencies have been overlooked

Evaluation of TOE Summary Specification (ASE_TSS.1)

CEM Work Unit	Type	Comment
<i>ASE_TSS.1.1E – Check content and presentation of evidence</i>		
ASE_TSS.1-1	Reference	
ASE_TSS.1-2	Affirmation	That each IT security function is traced to at least one TOE SFR (referencing the mappings)
ASE_TSS.1-3	Affirmation	That each IT security function is described informally in sufficient detail to understand its intent
ASE_TSS.1-4	Affirmation*	That references to security mechanisms are traced back to IT security functions (referencing the mappings)
ASE_TSS.1-5	Affirmation*	That the TOE SFRs are suitably met by the IT security functions, and that the TOE summary specification rationale provides an appropriate justification (referencing the rationale)
ASE_TSS.1-6	Affirmation*	That the SOF claims are consistent with the TOE SFR SOF rating(s) (referencing the rationale)
ASE_TSS.1-7	Affirmation*	That the combination of IT security functions work together to meet the TOE SFRs (referencing the rationale)
ASE_TSS.1-8	Affirmation*	That each assurance measure is mapped to at least one SAR (referencing the mappings)
ASE_TSS.1-9	Affirmation*	That the TOE SARs are suitably met by the assurance measures, and that the TOE summary specification rationale provides an appropriate justification (referencing the rationale)
ASE_TSS.1-10	References*	Identify the IT security functions with a SOF claim
ASE_TSS.1-11	Reference	
<i>ASE_TSS.1.2E – Confirm TSS is coherent, complete and internally consistent</i>		
ASE_TSS.1-12	Affirmation	That the TSS is complete
ASE_TSS.1-13	Affirmation	That the TSS is coherent
ASE_TSS.1-14	Affirmation	That no inconsistencies or conflicts were found within the TSS

TOE Evaluation – EAL4

Evaluation of Configuration Management (ACM)

Evaluation of CM Automation (ACM_AUT.1)

CEM Work Unit	Type	Comment
<i>ACM_AUT.1.1E – Check content and presentation of evidence</i>		
ACM_AUT.1-1	Reference	
ACM_AUT.1-2	Analysis	Describe what evaluators did to arrive at their conclusion
ACM_AUT.1-3	Reference	
ACM_AUT.1-4	Affirmation	
ACM_AUT.1-5	Reference	
ACM_AUT.1-6	Reference	
<i>ACM_AUT.1.1D – Implied evaluator action</i>		
ACM_AUT.1-7	Analysis	Describe the evidence that was examined

Evaluation of CM Capabilities (ACM_CAP.4)

CEM Work Unit	Type	Comment
<i>ACM_CAP.4.1E – Check content and presentation of evidence</i>		
ACM_CAP.4-1	Affirmation*	That the TOE version is uniquely referenced, describing the referencing system used
ACM_CAP.4-2	Reference*	Explain how the TOE version is identified
ACM_CAP.4-3	Affirmation	That TOE references used are consistent
ACM_CAP.4-4	Reference	
ACM_CAP.4-5	Reference	
ACM_CAP.4-6	Reference	
ACM_CAP.4-7	Affirmation	That the CIs are uniquely identified
ACM_CAP.4-8	Affirmation	That the configuration list identifies the CIs
ACM_CAP.4-9	Reference*	Briefly describing the referencing system used
ACM_CAP.4-10	Affirmation	That the CIs are consistently identified as defined in the CM documentation
ACM_CAP.4-11	Reference*	Identifying the various aspects covered, e.g. as listed at [CEM, 1237]
ACM_CAP.4-12	Reference*	List the types of example output produced by the CM system

CEM Work Unit	Type	Comment
ACM_CAP.4-13	Analysis	Describe what evidence was examined and the findings/conclusions from each interview carried out, demonstrating coverage of each type of CM-relevant operation
ACM_CAP.4-14	Analysis	Describe the types of CI covered by the check
ACM_CAP.4-15	Analysis	Describe what the evaluators did to arrive at their conclusions
ACM_CAP.4-16	Reference	
ACM_CAP.4-17	Affirmation	That the TOE generation procedures are effective
ACM_CAP.4-18	Reference*	Addressing each item listed at [CEM, 1252a)-c]

Evaluation of CM Scope (ACM_SCP.2)

CEM Work Unit	Type	Comment
<i>ACM_SCP.2.1E – Check content and presentation of evidence</i>		
ACM_SCP.2-1	Affirmation	That the configuration list covers all items given at [CEM, 1256] (the list need not be repeated)

Evaluation of Delivery and Operation (ADO)

Evaluation of TOE Delivery (ADO_DEL.2)

CEM Work Unit	Type	Comment
<i>ADO_DEL.2.1E – Check content and presentation of evidence</i>		
ADO_DEL.2-1	Affirmation*	That delivery procedures are defined (giving reference) and the level of protection is commensurate with the ST (see [CEM, 1260]), giving a brief summary of the procedures.
ADO_DEL.2-2	Affirmation*	That tampering or discrepancies can be detected, stating the method(s) used and giving references to the procedures
ADO_DEL.2-3	Affirmation*	That attempted masquerade can be detected, stating the method(s) used and giving references to the procedures
<i>ADO_DEL.2.1D – Implied evaluator action</i>		
ADO_DEL.2-4	Analysis	Describe approach used by evaluators, e.g. as listed in [CEM, 1270]

Evaluation of Installation, Generation and Start-up (ADO_IGS.1)

CEM Work Unit	Type	Comment
<i>ADO_IGS.1.1E – Check content and presentation of evidence</i>		
ADO_IGS.1-1	Reference	

CEM Work Unit	Type	Comment
<i>ADO_IGS.1.2E – Determine that procedures describe installation, generation and start-up</i>		
ADO_IGS.1-2	Affirmation	That the procedures describe steps necessary for secure installation, generation and start-up. The results of ATE_IND.2-2 and AVA_MSU.2-7 may be referenced in support.

Evaluation of TSF Representations (ADV)

Evaluation of Functional Specification (ADV_FSP.1)

CEM Work Unit	Type	Comment
<i>ADV_FSP.2.1E – Check content and presentation of evidence</i>		
ADV_FSP.2-1	Affirmation	Likely to be trivial – see [CEM, 1289]
ADV_FSP.2-2	Affirmation	That no inconsistencies have been found in the FS (referencing other WUs as appropriate)
ADV_FSP.2-3	Reference*	A general reference is expected, possibly for different interface types (e.g. GUI, command line), together with an indication of how a specific interface specification can be located
ADV_FSP.2-4	Affirmation	That all external interfaces are described. The results of ADV_FSP.2-6 and ADV_FSP.2-7 may be referenced in support.
ADV_FSP.2-5	Affirmation	That the complete behaviour of the external interfaces is described. The results of ADV_FSP.2-8 and ADV_FSP.2-9 may be referenced in support.
ADV_FSP.2-6	Affirmation	That no SFs are absent from the FS
ADV_FSP.2-7	Affirmation*	That a convincing argument has been provided (giving reference)
<i>ADV_FSP.2.2E – Determine that SFRs are completely and accurately instantiated</i>		
ADV_FSP.2-8	Analysis	For every SFR or SF, identify each relevant external interface, giving a summary of its relevance
ADV_FSP.2-9	Analysis	As ADV_FSP.2-8

Notes:

1. The significant concern of ADV_FSP.2-4 is that all external interfaces are described. Completeness is validated by performing ADV_FSP.2-6 and ADV_FSP.2-7 as described in CEM.
2. The affirmation provided for ADV_FSP.2-5 is supported by the results of the traceability analysis (as required by ADV_FSP.2.2E). Reporting for this work unit should be done by exception, i.e. identifying any interfaces whose descriptions do not satisfy the CC requirements.
3. Explicit identification of external interfaces is otherwise only required in the case of ADV_FSP.2.2E, and then only for those external interfaces that are relevant to the SFRs or SFs (together with a brief summary of their relevance). Note that a pass verdict can only be assigned for ADV_FSP.2.2E if

the relevant interface specifications satisfy the content and presentation of evidence requirements.

Evaluation of High-Level Design (ADV_HLD.2)

CEM Work Unit	Type	Comment
<i>ADV_HLD.2.1E – Check content and presentation of evidence</i>		
ADV_HLD.2-1	Affirmation	Likely to be trivial – see [CEM, 1307]
ADV_HLD.2-2	Affirmation	That no inconsistencies have been found in the HLD (referencing other WUs as appropriate)
ADV_HLD.2-3	Affirmation*	That the decomposition into TSF subsystems is sufficient for a high-level understanding, referencing the description in the HLD
ADV_HLD.2-4	Affirmation*	That the security functional behaviour of the TSF subsystems is described. The architectural description [CEM, 99] and the results of ADV_HLD.2-11 and ADV_HLD.2-12 may be referenced in support.
ADV_HLD.2-5	Reference	
ADV_HLD.2-6	Reference	
ADV_HLD.2-7	Reference*	A general reference may be required if the information is distributed throughout the HLD, describing how the evaluators located the required information
ADV_HLD.2-8	Affirmation	That externally visible subsystem interfaces are identified
ADV_HLD.2-9	Affirmation	That sufficient descriptive information is provided on the subsystem interfaces, e.g. in support of ATE_DPT.1
ADV_HLD.2-10	Reference	The architectural description [CEM, 99] may be referenced in support
<i>ADV_HLD.2.2E – Determine that SFRs are correctly and accurately instantiated</i>		
ADV_HLD.2-11	Analysis	For every SFR or SF, identify each relevant TSF subsystem, giving a summary of its role in providing the SFR or SF
ADV_HLD.2-12	Analysis	As ADV_HLD.2-11

Notes:

1. A similar philosophy applies to the reporting of the ADV_HLD.2.1E work units as that described for ADV_FSP.2 above. However, the CEM requirement for an architectural description, combined with the fact that there will be a small number of TSF subsystems to address, means that the ETR is likely to explicitly describe each of the TSF subsystems.

Evaluation of Implementation Representation (ADV_IMP.1)

CEM Work Unit	Type	Comment
<i>ADV_IMP.1.1E – Check content and presentation of evidence</i>		

CEM Work Unit	Type	Comment
ADV_IMP.1-1	Affirmation	That the implementation representation is suitable for analysis
ADV_IMP.1-2	Analysis	Describe and justify sampling strategy
ADV_IMP.1-3	Affirmation	That no inconsistencies were identified during the performance of ADV_IMP.1-4
<i>ADV_IMP.1.2E – Determine that SFRs are correctly and accurately instantiated</i>		
ADV_IMP.1-4	Analysis	Demonstrate coverage of all SFRs or SFs relevant to the subset

Notes:

- Where there is no 1:1 mapping between low level design modules and implementation portions, the justification for ADV_IMP.1-4 might be achieved by giving, for each implementation portion included in the subset, a summary of its role in providing, or contributing to the provision of, SFR(s) or SF(s).

Evaluation of Low-Level Design (ADV_LLD.1)

CEM Work Unit	Type	Comment
<i>ADV_LLD.1.1E – Check content and presentation of evidence</i>		
ADV_LLD.1-1	Affirmation	Likely to be trivial – see [CEM, 1349]
ADV_LLD.1-2	Affirmation	That no inconsistencies have been found in the LLD (referencing other WUs as appropriate)
ADV_LLD.1-3	Affirmation	That the modules are clearly and unambiguously identified
ADV_LLD.1-4	Affirmation	That the purpose of each module is described.
ADV_LLD.1-5	Affirmation*	That interrelationships between modules are described, with an indication of how the two types of interaction at [CEM, 1354] can be identified for a given module
ADV_LLD.1-6	Affirmation	That sufficient information is provided for implementation of module.
ADV_LLD.1-7	Affirmation	That the module interfaces are identified.
ADV_LLD.1-8	Affirmation	That externally visible interfaces are identifiable
ADV_LLD.1-9	Affirmation	That sufficient information is provided on interfaces to support understanding of module interactions.
ADV_LLD.1-10	Reference	
<i>ADV_LLD.1.2E – Determine that SFRs are correctly and accurately instantiated</i>		
ADV_LLD.1-11	Analysis	For every SFR or SF, identify each relevant module, giving a summary of its role in providing the SFR or SF
ADV_LLD.1-12	Analysis	As ADV_LLD.1-11

Notes:

- The affirmations provided for ADV_LLD.1-3 through ADV_LLD.1-9 are supported by the results

of the traceability analysis (as required by ADV_LLD.1.2E). Reporting for these work units should be done by exception, i.e. identifying any modules whose descriptions do not satisfy the CC requirements.

2. Explicit identification of modules is otherwise only required in the case of ADV_LLD.1.2E, and then only for those modules that are relevant to the SFRs or SFs (together with a brief summary of the role of each module in providing the SFR or SF). Note that a pass verdict can only be assigned for ADV_LLD.1.2E if the relevant module specifications satisfy the content and presentation of evidence requirements.

Evaluation of Representation Correspondence (ADV_RCR.1)

CEM Work Unit	Type	Comment
<i>ADV_RCR.1.1E – Check content and presentation of evidence</i>		
ADV_RCR.1-1	Affirmation	That FS correctly and completely represents SFs
ADV_RCR.1-2	Affirmation	That HLD correctly and completely represents FS
ADV_RCR.1-3	Affirmation	That LLD correctly and completely represents HLD
ADV_RCR.1-4	Affirmation	That the implementation representation subset correctly and completely represents LLD portions

Notes:

1. The work unit reports here are only of the **Affirmation** type because the traceability analyses for ADV_FSP.2.2E, ADV_HLD.2.2E, ADV_LLD.1.2E and ADV_IMP.1.2E demonstrate appropriate coverage of the SFs and thus (indirectly) provide confidence in the representation correspondence.

Evaluation of security policy modelling (ADV_SPM.1)

CEM Work Unit	Type	Comment
<i>ADV_SPM.1.1E – Check content and presentation of evidence</i>		
ADV_SPM.1-1	Affirmation	Likely to be trivial – see [CEM, 1377]
ADV_SPM.1-2	Reference*	To where each explicit policy is modelled
ADV_SPM.1-3	Reference*	To where each implicit policy is modelled
ADV_SPM.1-4	Affirmation	That detail and level of abstraction is sufficient and appropriate for understanding
ADV_SPM.1-5	Affirmation	That the ISPM is consistent with the policies in ST
ADV_SPM.1-6	Affirmation*	For each policy modelled, that the ISPM is complete with respect to modelling of behaviour, mapping SFRs to the ISPM
ADV_SPM.1-7	Affirmation	That the ISPM is complete with respect to the FS
ADV_SPM.1-8	Affirmation	That the ISPM is consistent with the FS

Notes:

1. If the ST satisfies the requirements of an ISPM (in accordance with [CEM, 1387-1389, 1392])

then the verdict justifications are rendered trivial for all work units, with the exception of ADV_SPM.1-4 which needs to confirm that the ST is sufficiently clear to enable the evaluators to understand the underlying security policy (i.e. that the rules and characteristics of the ISPM can be identified and are clearly defined)

Evaluation of Guidance Documents (AGD)

Evaluation of Administrator Guidance (AGD_ADM.1)

CEM Work Unit	Type	Comment
<i>AGD_ADM.1.1E – Check content and presentation of evidence</i>		
AGD_ADM.1-1	Affirmation	That administrative security functions and interfaces are described in the guidance
AGD_ADM.1-2	Affirmation	That the guidance describes how to operate the TOE in a secure manner
AGD_ADM.1-3	Affirmation	That no appropriate warnings have been overlooked by the guidance
AGD_ADM.1-4	Affirmation	That user assumptions are described in the guidance
AGD_ADM.1-5	Affirmation	That sufficient guidance is provided relating to security parameters under control of the administrator
AGD_ADM.1-6	Affirmation	That sufficient guidance is provided relating to security relevant events
AGD_ADM.1-7	Affirmation	That no inconsistencies were found between the guidance and other documents including the ST and functional specification
AGD_ADM.1-8	Reference*	Where each administrator-relevant IT security requirement is described in the guidance

Notes:

1. The work unit reports for AGD_ADM.1-1 through AGD_ADM.1-7 are simple **Affirmations** since completeness of the administrator guidance is addressed by AVA_MSU.2, and is demonstrated in the corresponding work unit reports. Therefore, the AVA_MSU.2 work units may be referenced in support of the above verdict justification.

Evaluation of User Guidance (AGD_USR.1)

CEM Work Unit	Type	Comment
<i>AGD_USR.1.1E – Check content and presentation of evidence</i>		
AGD_USR.1-1	Affirmation	That security functions and interfaces available to non-administrative users are described in the guidance
AGD_USR.1-2	Affirmation	That sufficient guidance is provided relating to the use of user-accessible SFs
AGD_USR.1-3	Affirmation	That no appropriate warnings have been overlooked by the guidance

CEM Work Unit	Type	Comment
AGD_USR.1-4	Affirmation	That user responsibilities necessary for secure operation of the TOE are described
AGD_USR.1-5	Affirmation	That no inconsistencies were found between the guidance and other documents including the ST and functional specification
AGD_USR.1-6	Reference*	To where each user-relevant IT security requirement is described in the guidance

Notes:

1. The work unit reports for AGD_USR.1-1 through AGD_USR.1-5 are simple **Affirmations** since completeness of the user guidance is addressed by AVA_MSU.2, and is demonstrated in the corresponding work unit reports. Therefore, the AVA_MSU.2 work units may be referenced in support of the above verdict justification.

Evaluation of Life-cycle Support (ALC)

Evaluation of Development Security (ALC_DVS.1)

CEM Work Unit	Type	Comment
<i>ALC_DVS.1.1E – Check content and presentation of evidence</i>		
ALC_DVS.1-1	Reference*	Identify where the different types of security measure [CEM, 1446] are described
ALC_DVS.1-2	Affirmation	That the security measures are sufficient
ALC_DVS.1-3	Reference*	Identify the types of evidence generated by application of the procedures
<i>ALC_DVS.1.2E – Check application of procedures</i>		
ALC_DVS.1-4	Analysis	Describe the evidence examined, and the findings and conclusions from the interviews conducted, showing how the measures uphold the TOE integrity and confidentiality

Evaluation of Life-cycle Definition (ALC_LCD.1)

CEM Work Unit	Type	Comment
<i>ALC_LCD.1.1E – Check content and presentation of evidence</i>		
ALC_LCD.1-1	Reference*	Identify where: a) information on procedures, tools and techniques is provided; b) where the overall management structure governing application of the procedures is described (see [CEM, 1460]); including a brief summary of the life-cycle model used by the developer.
ALC_LCD.1-2	Affirmation	That the life-cycle model makes the necessary positive contribution to the development and maintenance of the TOE.

Evaluation of Tools and Techniques (ALC_TAT.1)

CEM Work Unit	Type	Comment
<i>ALC_TAT.1.1E – Check content and presentation of evidence</i>		
ALC_TAT.1-1	Affirmation*	That the development tools are well-defined (giving references for each tool)
ALC_TAT.1-2	Affirmation	That the meaning of all statements used in the implementation representation is unambiguously defined
ALC_TAT.1-3	Affirmation	That the meaning of all implementation-dependent options is unambiguously defined

Notes:

1. The results of the ADV_IMP.1 work units may be referenced in support of this verdict justification.

Tests (ATE)

Evaluation of Coverage (ATE_COV.2)

CEM Work Unit	Type	Comment
<i>ATE_COV.2.1E – Check content and presentation of evidence</i>		
ATE_COV.2-1	Affirmation*	That the correspondence of tests to FS is accurate. A tabular/matrix summary (which will need to be assembled by the evaluators if the information is distributed across the test documentation) should be provided to the CB.
ATE_COV.2-2	Affirmation*	That the testing approach for each SF is suitable, identifying any SFs where alternate approaches are used (see [CEM, 7.9.1.2]), and describing what these approaches were.
ATE_COV.2-3	Affirmation	That the tests are adequate to exercise the SF behaviour described in the FS
ATE_COV.2-4	Affirmation	That all SFs and interfaces in the FS are mapped to at least one test (see also ATE_COV.2-1)

Evaluation of Depth (ATE_DPT.1)

CEM Work Unit	Type	Comment
<i>ATE_DPT.1.1E – Check content and presentation of evidence</i>		
ATE_DPT.1-1	Affirmation*	That the correspondence of tests to HLD is accurate. A tabular/matrix summary (which will need to be assembled by the evaluators if the information is distributed across the test documentation) should be provided to the CB.
ATE_DPT.1-2	Affirmation*	That the testing approach for each SF is suitable, identifying any SFs where alternate approaches are used (see [CEM, 7.9.1.2]), and describing what these approaches were.

CEM Work Unit	Type	Comment
ATE_DPT.1-3	Affirmation	That the tests are adequate to exercise the SF behaviour described in the HLD
ATE_DPT.1-4	Affirmation	That all TSF subsystems and interfaces in the HLD are mapped to at least one test (see also ATE_DPT.1-1)

Evaluation of Functional Tests (ATE_FUN.1)

CEM Work Unit	Type	Comment
<i>ATE_FUN.1.1E – Check content and presentation of evidence</i>		
ATE_FUN.1-1	Reference	
ATE_FUN.1-2	Affirmation*	That the test plan identifies the SF(s) to be tested. Describe sampling strategy if appropriate.
ATE_FUN.1-3	Affirmation*	That the goal of the tests is identified. Describe sampling strategy if appropriate.
ATE_FUN.1-4	Affirmation	That TOE test configuration is consistent with ST
ATE_FUN.1-5	Affirmation*	That the test plan is consistent with test procedure descriptions. Describe sampling strategy if appropriate.
ATE_FUN.1-6	Affirmation*	That the test procedure descriptions identify the SF behaviour to be tested. Describe sampling strategy if appropriate.
ATE_FUN.1-7	Affirmation*	That the test instructions are sufficient to establish reproducible test conditions. Describe sampling strategy if appropriate.
ATE_FUN.1-8	Affirmation*	That the test instructions are sufficient to have a reproducible means of testing the SFs. Describe sampling strategy if appropriate.
ATE_FUN.1-9	Affirmation*	That test procedure descriptions are consistent with test procedures (may be trivial – see [CEM, 1523]). Describe sampling strategy if appropriate.
ATE_FUN.1-10	Affirmation*	That sufficient expected results are included. Describe sampling strategy if appropriate.
ATE_FUN.1-11	Affirmation*	That the actual results are consistent with expected results (but noting any unexpected effects) Describe sampling strategy if appropriate.
ATE_FUN.1-12	Report	Provide information described in [CEM, 1537] where not addressed by other WU reports

Independent Testing (ATE_IND.2)

CEM Work Unit	Type	Comment
<i>ATE_IND.2.1E – Check content and presentation of evidence</i>		
ATE_IND.2-1	Affirmation	That the test configuration is consistent with ST

CEM Work Unit	Type	Comment
ATE_IND.2-2	Affirmation	That the TOE was installed properly and in a known state
ATE_IND.2-3	Affirmation	That the set of resources provided was equivalent to those used by the developer's tests
<i>ATE_IND.2.2E – Test subset of TSF</i>		
ATE_IND.2-4	Analysis	Describe and justify the test strategy adopted
ATE_IND.2-5	Reference	To the evaluator's test documentation (which must be provided to the CB)
ATE_IND.2-6	Reference	To the evaluator's completed test documentation, giving dates for testing
ATE_IND.2-7	Reference	To the evaluator's test documentation
ATE_IND.2-8	Affirmation*	List the results of each test performed (in terms of pass or fail, noting any unexpected effects)
<i>ATE_IND.2.3E – Execute sample of developer's tests</i>		
ATE_IND.2-9	Analysis	Describe criteria used for selecting tests and justify sampling strategy
ATE_IND.2-10	Affirmation*	List the results of each test performed (in terms of pass or fail)
ATE_IND.2-11	Report	Provide information described in [CEM, 1568] where not addressed by other WU reports

Vulnerability Assessment (AVA)

Evaluation of Misuse (AVA_MSU.2)

CEM Work Unit	Type	Comment
<i>AVA_MSU.2.1E – Check content and presentation of evidence</i>		
AVA_MSU.2-1	Affirmation*	For each SF, that guidance related to the SF is sufficient and there is no conflict with other SFs
AVA_MSU.2-2	Affirmation	That there are no identified instances of unclear or inconsistent guidance
AVA_MSU.2-3	Affirmation*	That there are no identified instances of unreasonable guidance and that the guidance is complete, giving, for each relevant SF, references to where guidance is provided in the user and/or administrator guidance (see also AVA_MSU.2-1)
AVA_MSU.2-4	Reference*	To where each relevant assumption about the TOE security environment is covered by the guidance
AVA_MSU.2-5	Reference*	To where each relevant security objective for the non-IT environment is covered by the guidance

CEM Work Unit	Type	Comment
AVA_MSU.2-6	Affirmation*	That the developer has taken adequate measures to ensure the guidance is complete, referencing the developer's analysis
<i>AVA_MSU.2.2E – Repeat installation, configuration and other procedures</i>		
AVA_MSU.2-7	Affirmation*	That no significant concerns were observed as a result of repeating installation and configuration procedures (giving references)
AVA_MSU.2-8	Analysis	Identify procedures selected and the criteria for selecting them, confirming that these gave rise to no significant concerns
<i>AVA_MSU.2.3E – Determine that insecure states can be detected using guidance</i>		
AVA_MSU.2-9	Analysis	Describe insecure states covered, how completeness is assured, and identify means by which each insecure state can be detected
<i>AVA_MSU.2.4E – Confirm developer's analysis shows all modes of operation covered</i>		
AVA_MSU.2-10	Affirmation*	For each identified mode of operation, that the developer's analysis shows that guidance is provided, outlining how completeness is assured

Evaluation of Strength of TOE Security Functions (AVA_SOF.1)

CEM Work Unit	Type	Comment
<i>AVA_SOF.1.1E – Check content and presentation of evidence</i>		
AVA_SOF.1-1	Reference	
AVA_SOF.1-2	Reference	
AVA_SOF.1-3	Affirmation*	That the SOF analysis is not based on any invalid assertions or assumptions, identifying any explicit or implicit assertions or assumptions made
AVA_SOF.1-4	Affirmation	That there are no errors in the developer's SOF calculations and that the supporting algorithms, principles and properties are correct
AVA_SOF.1-5	Affirmation	That each SOF claim is met or exceeded
<i>AVA_SOF.1.2E – Confirm that the strength claims are correct</i>		
AVA_SOF.1-6	Affirmation	That list of SFs realized by a probabilistic or permutational mechanism is complete
AVA_SOF.1-7	Analysis	Describe independent analysis and/or testing used to validate correctness of SOF claims (including an outline of the analysis for each function).

Evaluation of Vulnerability Analysis (AVA_VLA.2)

CEM Work Unit	Type	Comment
---------------	------	---------

CEM Work Unit	Type	Comment
<i>AVA_VLA.2.1E – Check content and presentation of evidence</i>		
AVA_VLA.2-1	Affirmation*	That all relevant information has been considered by the developer, referencing the developer's analysis.
AVA_VLA.2-2	Affirmation*	For each vulnerability, that an appropriate justification for non-exploitability has been provided, outlining the reasoning provided (which will typically be based on one of the types listed in [CEM, 1625])
AVA_VLA.2-3	Affirmation	That the analysis is consistent with the ST and guidance
<i>AVA_VLA.2.2E – Perform penetration testing building on developer analysis</i>		
AVA_VLA.2-4	Analysis	Describe evaluator's approach for identifying penetration tests covering the cases in [CEM, 1628]
AVA_VLA.2-5	Reference	To the evaluator's penetration test documentation
AVA_VLA.2-6	Reference*	To the evaluator's completed penetration test documentation (which must be provided to the CB), giving dates of testing
AVA_VLA.2-7	Affirmation*	List results for each penetration test performed (in terms of pass or fail, noting any unexpected effects)
AVA_VLA.2-8	Report	Provide additional information where not covered by other WU reports
<i>AVA_VLA.2.3E – Perform independent vulnerability analysis</i>		
AVA_VLA.2-9	Analysis	Demonstrate consideration of each of the generic vulnerabilities described in [CEM, 1643-1650]
<i>AVA_VLA.2.4E – Perform penetration testing based on independent vulnerability analysis</i>		
AVA_VLA.2-10	Analysis	Describe approach for identifying penetration tests based on independent vulnerability analysis results
AVA_VLA.2-11	Reference	To the evaluator's penetration test documentation
AVA_VLA.2-12	Reference*	To the evaluator's completed penetration test documentation (which must be provided to the CB), giving dates of testing
AVA_VLA.2-13	Affirmation*	List results of penetration tests performed (in terms of pass or fail, noting any unexpected effects)
AVA_VLA.2-14	Report	Provide additional information where not covered by other WU reports
<i>AVA_VLA.2.5E – Determine resistance of TSF to attacker with low attack potential</i>		
AVA_VLA.2-15	Analysis	Analyse impact of vulnerabilities found and determine exploitability
AVA_VLA.2-16	Report	Provide vulnerability information in ETR as required