
UK IT SECURITY EVALUATION & CERTIFICATION SCHEME

UK CC Interpretation - UK/3.1/007

12 March 2007

Status: Endorsed for use in UK Scheme

Subject: Verdict justifications in CEM compliant evaluations

REFERENCES CEM, Version 3.1, Revision 1, September 2006

Note The interpretation is formulated for the EAL4 assurance level. The inclusion/exclusion of other components in the assurance package does not affect the work to be performed, and reported, for individual work units. Therefore, deriving equivalent interpretations for lower assurance levels is straightforward.

Issue

1. CEM section 8.2.5 outlines the process by which verdicts are assigned by the evaluator. It states (paragraph 55) 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 8.5.5.3.4 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 132 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 133 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 133 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 8.5.5.2.3).
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 over-simplification. 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, 1074]) and AGD_OPE.1-6 (where coverage of individual security objectives for the operational environment 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. ADV_ARC.1-4, where the developer’s analysis of how the TOE provides self-protection 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 AGD_OPE.1-2 (where affirmation should be provided for each user role).

e) **Report**

Such types are explicitly identified by inclusion of the words *shall report* and *shall record* 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 ALC_CMC.4-5, ALC_DEL.1-2 and ATE_IND.2-6).
 - 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. ADV_ARC.1-4, where the developer's analysis of how the TOE provides self-protection 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. 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

21. The interpretation at paragraph 7 above 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_VAN.3-8, ATE_IND.2-11).
22. 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).
23. 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.2.4C; in this case a Level 4 OR must be raised. For the work unit ASE_OBJ.2-4, 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?
24. The verdict justification in the ETR must therefore explicitly address both these concerns (see Annex A).
25. 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 above).
26. 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 demonstration that the evidence is suitable and sufficient 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 repeating

extracts from the evidence provided.

27. 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.2-1 (see Annex A below).
28. 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	
ASE_INT.1-4	Affirmation	That the TOE reference is not misleading
ASE_INT.1-5	Reference	
ASE_INT.1-6	Reference	
ASE_INT.1-7	Affirmation	That the TOE type is not misleading
ASE_INT.1-8	Reference	
ASE_INT.1-9	Reference	
ASE_INT.1-10	Reference	
<i>ASE_INT.1.2E – Confirm TOE reference, TOE overview and TOE description are internally consistent</i>		
ASE_INT.1-11	Affirmation	That no inconsistencies were found

Evaluation of Conformance Claims (ASE_CCL.1)

CEM Work Unit	Type	Comment
<i>ASE_CCL.1.1E – Check content and presentation of evidence</i>		
ASE_CCL.1-1	Reference	
ASE_CCL.1-2	Reference	
ASE_CCL.1-3	Reference	
ASE_CCL.1-4	Affirmation	That the CC conformance claim for CC Part 2 is consistent with the extended components definition
ASE_CCL.1-5	Affirmation	That the CC conformance claim for CC Part 3 is consistent with the extended components definition
ASE_CCL.1-6	Reference	
ASE_CCL.1-7	Reference	
ASE_CCL.1-8	Reference	
ASE_CCL.1-9	Affirmation	That the TOE type of the TOE is consistent with the TOE types of the PPs

CEM Work Unit	Type	Comment
ASE_CCL.1-10	Affirmation*	That the statement of the security problem definition is [strictly/demonstrably] (as required by the PP) consistent with the statement of the security problem definition in the PPs for which conformance is claimed
ASE_CCL.1-11	Affirmation*	That the statement of security objectives is strictly/demonstrably] (as required by the PP) consistent with the statement of security objectives in the PPs for which conformance is claimed
ASE_CCL.1-12	Affirmation*	That the statement of security requirements is strictly/demonstrably] (as required by the PP) consistent with the statement of security requirements in the PPs for which conformance is claimed

Evaluation of Security Problem Definition (ASE_SPD.1)

CEM Work Unit	Type	Comment
<i>ASE_SPD.1.1E – Check content and presentation of evidence</i>		
ASE_SPD.1-1	Reference	
ASE_SPD.1-2	Reference*	That each threat is described in terms of a threat agent, asset and adverse action
ASE_SPD.1-3	Reference	
ASE_SPD.1-4	Reference	

Evaluation of Security Objectives (ASE_OBJ.2)

CEM Work Unit	Type	Comment
<i>ASE_OBJ.2.1E – Check content and presentation of evidence</i>		
ASE_OBJ.2-1	Reference	
ASE_OBJ.2-2	Affirmation*	That each TOE security objective is traced back to at least one threat or OSP (referencing the mappings)
ASE_OBJ.2-3	Affirmation*	That each security objective for the environment is traced back to at least one threat, OSP or assumption (referencing the mappings)
ASE_OBJ.2-4	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.2-5	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.2-6	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).

Evaluation of Extended Components Definition (ASE_ECD.1)

CEM Work Unit	Type	Comment
<i>ASE_ECD.1.1E – Check content and presentation of evidence</i>		
ASE_ECD.1-1	Affirmation	That all security requirements in the statement of security requirements that are not identified as extended security requirements are defined in Part 2 or Part 3, thereby identifying those components that are extended
ASE_ECD.1-2	Reference	
ASE_ECD.1-3	Affirmation	That the extended components fit into the existing CC components, families and classes
ASE_ECD.1-4	Affirmation	For each extended component, that no dependencies have been overlooked
ASE_ECD.1-5	Affirmation	That each new functional component defined is consistent with CC Part 2 component structure
ASE_ECD.1-6	Affirmation	That each new functional family defined is consistent with CC Part 2 family structure
ASE_ECD.1-7	Affirmation	That each new functional class defined is consistent with CC Part 2 class structure
ASE_ECD.1-8	Affirmation	That each new assurance component defined is consistent with CC Part 3 component structure
ASE_ECD.1-9	Affirmation	That methodology is provided for each defined assurance component
ASE_ECD.1-10	Affirmation	That each new assurance family defined is consistent with CC Part 3 family structure
ASE_ECD.1-11	Affirmation	That each new assurance class defined is consistent with CC Part 3 class structure
ASE_ECD.1-12	Affirmation	That conformance/non-conformance can be demonstrated for each element in each extended component
<i>ASE_ECD.1.2E – Confirm no extended component may be clearly expressed using existing components</i>		
ASE_ECD.1-13	Affirmation*	That the requirements expressed in the extended components can not be clearly expressed using existing components, identifying differences from similar components in Part 2/3.

Evaluation of IT Security Requirements (ASE_REQ.2)

CEM Work Unit	Type	Comment
<i>ASE_REQ.2.1E – Check content and presentation of evidence</i>		
ASE_REQ.2-1	Reference	
ASE_REQ.2-2	Reference	
ASE_REQ.2-3	Affirmation	That all terms used in the SFRs/SARs are defined
ASE_REQ.2-4	Affirmation*	That completed operations are identified, stating the method used

CEM Work Unit	Type	Comment
ASE_REQ.2-5	Affirmation	That all assignment operations are performed correctly
ASE_REQ.2-6	Affirmation	That all iteration operations are performed correctly
ASE_REQ.2-7	Affirmation	That all selection operations are performed correctly
ASE_REQ.2-8	Affirmation	That all refinement operations are performed correctly
ASE_REQ.2-9	Affirmation*	That the dependencies are satisfied and/or that there is an appropriate justification for non-satisfaction of any dependencies (referencing the rationale identifying aspects of dependencies that have not been satisfied)
ASE_REQ.2-10	Affirmation*	That each SFR is traced back to at least one security objective for the TOE (referencing the mappings)
ASE_REQ.2-11	Affirmation*	For each security objective for the TOE, that a) it is suitably met by the SFRs; b) that the security requirements rationale provides an appropriate justification (referencing the rationale)
ASE_REQ.2-12	Affirmation	That the security requirements rationale provides a coherent explanation of why the SARs were chosen and that is consistent with the remainder of the ST
ASE_REQ.2-13	Affirmation	That the statement of security requirements is internally consistent

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	
<i>ASE_TSS.1.2E – Confirm TSS is consistent with the TOE overview and TOE description</i>		
ASE_TSS.1-2	Affirmation	That the TOE summary specification is consistent with the TOE overview and TOE description

TOE Evaluation – EAL4

Evaluation of TSF Representations (ADV)

Evaluation of Functional Specification (ADV_FSP.4)

CEM Work Unit	Type	Comment
<i>ADV_FSP.4.1E – Check content and presentation of evidence</i>		
ADV_FSP.4-1	Affirmation*	That the evaluator did not identify any omission of external interfaces detailed in the TOE Design that were not considered in the FS. 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.4-2	Affirmation	That the purpose of each TSFI is stated
ADV_FSP.4-3	Affirmation	That the method of use of each TSFI is stated
ADV_FSP.4-4	Affirmation	That all parameters associated with each TSFI are described
ADV_FSP.4-5	Affirmation	That the parameter descriptions are complete and accurate
ADV_FSP.4-6	Affirmation	That the actions associated with each TSFI are described
ADV_FSP.4-7	Affirmation	That all error messages resulting from invocation of each TSFI are completely and accurately described
ADV_FSP.4-8	Affirmation	That the meaning of all errors associated with each TSFI are completely and accurately described
ADV_FSP.4-9	Affirmation	That the tracing between the TSFI and SFRs is complete and accurate. The results of ADV_FSP.4-10 and ADV_FSP.4-11 may be referenced in support.
<i>ADV_FSP.4.2E – Determine that SFRs are completely and accurately instantiated</i>		
ADV_FSP.4-10	Analysis	For every SFR identify each relevant TSFI, giving a summary of its relevance
ADV_FSP.4-11	Analysis	As for ADV_FSP.4-10, ensuring the description of the TSFI is consistent with the SFR.

Notes:

1. The significant concern of ADV_FSP.4-1 is that all TSFI are described. Completeness is validated by performing ADV_TDS.3-13 as described in CEM.
2. The affirmations provided for ADV_FSP.4-2 to ADV_FSP.4-8 are 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 TSFIs whose descriptions do not satisfy the CC requirements.
3. Explicit identification of TSFI is otherwise only required in the case of ADV_FSP.2.2E, and then only for those TSFI that are relevant to the SFRs (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 TOE Design (ADV_TDS.3)

CEM Work Unit	Type	Comment
<i>ADV_TDS.3.1E – Check content and presentation of evidence</i>		
ADV_TDS.3-1	Affirmation*	That the entire TOE (not just the TSF) has been decomposed into subsystems, referencing the description in the TOE design, or in the case of a simple TOE, that the evaluator agrees the modular description of the TOE is sufficient
ADV_TDS.3-2	Affirmation*	That the entire TSF is described in terms of modules and that no omissions have been identified, giving reference to the modular description
ADV_TDS.3-3	Affirmation*	That the TSF subsystems are identifiable, referencing the security architecture description in support. All subsystems identified in the security architecture description should be described in the TOE Design, and vice versa.
ADV_TDS.3-4	Affirmation	That a description of each TSF subsystem is provided in terms of the role the subsystem plays in the enforcement of the SFRs
ADV_TDS.3-5	Affirmation	That interactions among all TSF subsystems are described
ADV_TDS.3-6	Affirmation	That all subsystems map to at least one module and that all modules map to one subsystem
ADV_TDS.3-7	Affirmation	That no inconsistencies have been found in the mapping. The results of ADV_TDS.3-2 (subsystem descriptions) and ADV_TDS.3-8 to ADV_TDS.3-12 (module descriptions) may be referenced in support
ADV_TDS.3-8	Affirmation	That the function the SFR-enforcing module is fulfilling is described
ADV_TDS.3-9	Affirmation*	That the SFR-related interfaces between modules are described, including details of return values, identifying instances where global data is used pass values between modules
ADV_TDS.3-10	Affirmation	That the non-SFR-supporting modules are correctly categorised, identifying any modules for which the categorisation was queried due to an apparent inconsistency
ADV_TDS.3-11	Affirmation	That no inconsistencies or omissions were identified in description of the purpose of each non-SFR-supporting module
ADV_TDS.3-12	Affirmation	That no inconsistencies or omissions were identified in the description of the non-SFR-supporting module's interaction with other modules
ADV_TDS.3-13	Affirmation	That each TSFI map to at least one module and that no inconsistencies or omissions were identified in the mapping. If the information is distributed across the TOE design documentation, the evaluator should assemble a tabular/matrix summary, which could be integrated into the traceability analysis report for ADV_TDS.3.2E.

CEM Work Unit	Type	Comment
<i>ADV_TDS.3.2E – Determine that SFRs are correctly and accurately instantiated</i>		
ADV_TDS.3-14	Analysis	For every SFR, identify each relevant module giving a summary of its role in providing the SFR
ADV_TDS.3-15	Analysis	As ADV_TDS.3-14, , ensuring the description of the module is consistent with the SFR

Notes:

1. ADV_TDS.3-1 relies on the examination of the guidance documentation during the conduct of AGD_OPE.1 and AGD_PRE.1 and also the conduct of the ASE activities to determine that the entire TOE is covered by the subsystem description.
2. Similarly, ADV_TDS.3-2 relies on the conduct of the other work units for ADV_TDS.3, particularly ADV_TDS.3-14 and ADV_TDS.3-15, to determine that the entire TSF is covered by the modular description.
3. To determine the accuracy of the mapping between subsystems and modules in work unit ADV_TDS.3-7, the evaluator should take into account the understanding of the subsystems gained during the conduct of work unit ADV_TDS.3-2 and that of the modules gained during the conduct of work units ADV_TDS.3-8 to ADV_TDS.3-12.

Evaluation of Security Architecture (ADV_ARC.1)

CEM Work Unit	Type	Comment
<i>ADV_ARC.1.1E – Check content and presentation of evidence</i>		
ADV_ARC.1-1	Affirmation*	That the security architecture contains implementation dependent information and no inconsistencies have been identified between this description and the specification of subsystems and modules in the TOE design. List any specific mechanisms implemented for self protection, non-bypassability, etc
ADV_ARC.1-2	Affirmation	That security domains are maintained by the TSF
ADV_ARC.1-3	Affirmation*	That the initialisation process preserves security, providing a summary as to how the TOE initialises securely.
ADV_ARC.1-4	Affirmation*	That the TOE security architecture protects itself from tampering, providing a summary of how the user input is handled by the TSF to protect itself from tampering
ADV_ARC.1-5	Affirmation*	That a convincing analysis has been provided describing how SFR-enforcing mechanisms cannot be bypassed (giving reference)

Evaluation of Implementation Representation (ADV_IMP.1)

CEM Work Unit	Type	Comment
<i>ADV_IMP.1.1E – Check content and presentation of evidence</i>		
ADV_IMP.1-1	Affirmation	That the implementation representation is suitable for analysis

CEM Work Unit	Type	Comment
ADV_IMP.1-2	Affirmation*	That the implementation representation provided to the evaluator is in the same form as used by the development personnel, detailing how this was determined
ADV_IMP.1-3	Analysis	Demonstrate coverage of all SFRs relevant to the subset and consistency between the TOE design and the implementation representation

Notes:

1. Where there is no 1:1 mapping between low level design modules and implementation portions, the justification for ADV_IMP.1-3 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).

Evaluation of Guidance Documents (AGD)

Evaluation of Operational User Guidance (AGD_OPE.1)

CEM Work Unit	Type	Comment
<i>AGD_OPE.1.1E – Check content and presentation of evidence</i>		
AGD_OPE.1-1	Affirmation*	That, for each user role, functions and privileges are described in the guidance and that no appropriate warnings have been overlooked
AGD_OPE.1-2	Affirmation*	That, for each user role, the guidance describes how to operate the TOE in a secure manner
AGD_OPE.1-3	Affirmation*	That, for each role, security parameters under the control of the user are described and indicating secure values where appropriate
AGD_OPE.1-4	Affirmation*	That security relevant events are detailed for each user role
AGD_OPE.1-5	Affirmation*	For each role, that guidance related to the TSFI is sufficient and there is no conflict with other TSFI
AGD_OPE.1-6	Affirmation*	That, for each user role, security measures to be followed are described in order to fulfil the security objectives for the operational environment
AGD_OPE.1-7	Affirmation	That the guidance documentation was found to be clear
AGD_OPE.1-8	Affirmation	That the guidance documentation was found to be reasonable and consistent with the ST

Notes:

1. Work units AGD_OPE.1-1 to AGD_OPE.1-6 are Elaborated Affirmations as the evaluator should affirm that the properties exist for each of the user roles. In effect, the evaluator is to iterate these work units for each type of user.

Evaluation of Preparative Procedures (AGD_PRE.1)

CEM Work Unit	Type	Comment
<i>AGD_PRE.1.1E – Check content and presentation of evidence</i>		
AGD_PRE.1-1	Reference	
AGD_PRE.1-2	Affirmation*	That the acceptance procedures describe the steps for secure acceptance of the TOE and that these steps are consistent with those implied by the developer's delivery procedures (ALC_DEL.1). Provide a summary of what the end user is supposed to do upon acceptance of the TOE.
AGD_PRE.1-3	Reference	
AGD_PRE.1-4	Affirmation	That the procedures describe steps necessary for secure installation of the TOE, preparation of the operational environment
<i>AGD_PRE.1.2E – Apply the preparative procedures to confirm the TOE can be prepared securely for operation</i>		
AGD_PRE.1-5	Affirmation*	That the evaluator found the procedures to be sufficient to securely prepare the TOE and its operational environment. The results of ATE_IND.2-2 may be referenced in support.

Evaluation of Life-cycle Support (ALC)

Evaluation of CM Capabilities (ALC_CMC.4)

CEM Work Unit	Type	Comment
<i>ALC_CMC.4.1E – Check content and presentation of evidence</i>		
ALC_CMC.4-1	Reference*	Explain how the TOE version is identified
ALC_CMC.4-2	Affirmation	That TOE references used are consistent
ALC_CMC.4-3	Reference*	Briefly describing the referencing system used
ALC_CMC.4-4	Affirmation	That CIs are identified in a manner consistent with the CM documentation
ALC_CMC.4-5	Analysis	Describe what the evaluators did to arrive at their conclusion
ALC_CMC.4-6	Reference	
ALC_CMC.4-7	Affirmation	That the TOE production support procedures are effective in ensuring that a TOE is generated that reflects its implementation representation
ALC_CMC.4-8	Reference	
ALC_CMC.4-9	Reference*	Identifying the various aspects covered, e.g. as listed at [CEM, 985]
ALC_CMC.4-10	Reference*	Addressing each item listed at [CEM, 986]
ALC_CMC.4-11	Analysis	Describe the types of CIs covered by the check

CEM Work Unit	Type	Comment
ALC_CMC.4-12	Reference*	List the types of example output produced by the CM system
ALC_CMC.4-13	Analysis	Describe what evidence was examined and the finding/conclusions from each interview carried out, demonstrating coverage of each type of CM-relevant operation

Evaluation of CM Scope (ALC_CMS.4)

CEM Work Unit	Type	Comment
<i>ALC_CMS.4.1E – Check content and presentation of evidence</i>		
ALC_CMS.4-1	Affirmation	That the configuration List identifies the CIs
ALC_CMS.4-2	Affirmation	That the CIs are uniquely identified
ALC_CMS.4-3	Affirmation*	List the development organisations ¹

Evaluation of TOE Delivery (ALC_DEL.1)

CEM Work Unit	Type	Comment
<i>ALC_DEL.1.1E – Check content and presentation of evidence</i>		
ALC_DEL.1-1	Affirmation*	That delivery procedures are defined (giving reference) and providing all detail “necessary to maintain security” (see [CEM, 1065]), giving a brief summary of the procedures.
ALC_DEL.1-2	Analysis	Describe the approach used by evaluators, e.g. as listed in [CEM, 1066]

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, 1074] are described.
ALC_DVS.1-2	Affirmation	That the security measures are sufficient
<i>ALC_DVS.1.2E – Check application of procedures</i>		
ALC_DVS.1-3	Analysis	Describe the evidence examined, and the findings and conclusions from the interviews conducted, showing how the measures uphold the TOE integrity and confidentiality

¹ The list of developers will feed into sampling activities for ALC_CMC.4-10 to ALC_CMC.1-13.

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 the different aspects of the life-cycle model (see [CEM, 1168]) are described, providing a brief summary of the life-cycle model
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 TSFI 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 TSFI is suitable, identifying any TSFIs where alternate approaches are used (see [CEM, 14.2.2]), and describing what these approaches were.
ATE_COV.2-3	Affirmation	That the tests are adequate to exercise the TSFI behaviour described in the FS
ATE_COV.2-4	Affirmation	That all TSFIs 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 subsystems 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. Any specific mechanisms cited in the Security Architecture (ADV_ARC.1 evidence) should also be included in the developer’s correspondence of tests to subsystems and the evaluator’ summary.
ATE_DPT.1-2	Affirmation*	That the testing approach for each TSF subsystem demonstrates the behaviour of the subsystem described in the TOE Design, identifying any subsystems where alternate approaches are used (see [CEM, 14.2.2]) and describing what these approaches were.
ATE_DPT.1-3	Affirmation*	That the testing approach for each TSF subsystem demonstrates the behaviour of the subsystem described in the TOE Design, identifying any subsystems where alternate approaches are used (see [CEM, 14.2.2]) and describing what these approaches were.
ATE_DPT.1-4	Affirmation	That all TSF subsystem behaviour and interaction 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 describes the scenarios for performing each test. Describe sampling strategy if appropriate
ATE_FUN.1-3	Affirmation*	That all test configurations described are consistent with the ST (see [CEM, 1320]) and relevant security objectives stated in the ST are considered in the test environments (see [CEM, 1321]). List security objectives relevant to the test environment and, if appropriate, describe sampling strategy
ATE_FUN.1-4	Affirmation(*)	That the test plans provide sufficient instructions to determine ordering dependencies are satisfied. Describe sampling strategy if appropriate
ATE_FUN.1-5	Affirmation(*)	That all expected results are included. Describe sampling strategy if appropriate.
ATE_FUN.1-6	Affirmation*	That the actual results are consistent with expected results (not noting any unexpected effects). Describe sampling strategy if appropriate.
ATE_FUN.1-7	Report	Provide information described in [CEM, 1333] where not addressed by other WU reports

Notes:

2. An elaborated affirmation is only required for work units ATE_FUN.1-2, 1-4 and 1-5 if a sampling strategy has been employed by the evaluators, as indicated by “(*)”. If no sampling strategy is employed only an affirmation is required.

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
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 – Execute sample of developer’s tests</i>		
ATE_IND.2-4	Analysis	Describe criteria used for selecting tests and justify sampling strategy
ATE_IND.2-5	Affirmation*	List the results of each test performed (in terms of pass or fail)
<i>ATE_IND.2.3E – Test subset of TSF</i>		
ATE_IND.2-6	Analysis	Describe and justify the test strategy adopted
ATE_IND.2-7	Reference	To the evaluator’s test documentation (which must be provided to the CB)
ATE_IND.2-8	Reference	To the evaluator’s completed test documentation, giving dates for testing
ATE_IND.2-9	Reference	To the evaluator’s test documentation
ATE_IND.2-10	Affirmation*	List the results of each test performed (in terms of pass or fail, noting any unexpected effects)
ATE_IND.2-11	Report	Provide information described in [CEM, 1385] where not addressed by other WU reports

Vulnerability Assessment (AVA)

Evaluation of Vulnerability Analysis (AVA_VAN.3)

CEM Work Unit	Type	Comment
<i>AVA_VAN.3.1E – Check content and presentation of evidence</i>		
AVA_VAN.3-1	Affirmation	That the test configuration is consistent with the ST. The results of ATE_IND.2-1 may be referenced in support.
AVA_VAN.3-2	Affirmation	That the TOE was installed properly and in a known state. The results of ATE_IND.2-2 may be referenced in support.

CEM Work Unit	Type	Comment
<i>AVA_VAN.3.2E – Perform search of public domain to identify potential vulnerabilities in the TOE</i>		
AVA_VAN.3-3	Report	Provide details of search performed (see [CEM, 1494-1495])
<i>AVA_VAN.3.3E – Perform independent vulnerability analysis</i>		
AVA_VAN.3-4	Analysis	Describe the evaluator's approach to the vulnerability analysis, including the evidence considered and demonstration the each of the generic vulnerabilities described in [CEM, Annex B]) have been considered. Describe sampling strategy of any evidence, if appropriate.
AVA_VAN.3-5	Report	Potential vulnerabilities to be used as input into penetration testing from both AVA_VAN.3-3 and AVA_VAN.3-4).
<i>AVA_VAN.3.4E – Perform penetration testing based on identified potential vulnerabilities</i>		
AVA_VAN.3-6	Analysis	Describe approach for identifying penetration tests based on independent vulnerability analysis results
AVA_VAN.3-7	Reference	To the evaluator's penetration test documentation
AVA_VAN.3-8	Reference*	To the evaluator's completed penetration test documentation (which must be provided to the CB), giving dates of testing
AVA_VAN.3-9	Affirmation*	List results of penetration tests performed (in terms of pass or fail, noting any unexpected effects)
AVA_VAN.3-10	Report	Provide additional information where not covered by other WU reports
AVA_VAN.3-11	Analysis	Analyse impact of vulnerabilities found and determine exploitability
AVA_VAN.3-12	Report	Provide vulnerability information in ETR as required