



**UK IT SECURITY EVALUATION
AND CERTIFICATION SCHEME**

UK Scheme Publication No 2

CLEF REQUIREMENTS

Part II

CONDUCT OF AN EVALUATION

**Issue 2.4
December 2009**

© Crown Copyright 2009 – All Rights Reserved

Reproduction is authorised provided the
document is copied in its entirety.

UK IT Security Evaluation and Certification Scheme
IA Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

FOREWORD

The UK IT Security Evaluation and Certification Scheme ('the Scheme') has been established to evaluate and certify the trustworthiness of security features of Information Technology products and systems.

Scheme Publication UKSP 02 defines the set of requirements on the Commercial Evaluation Facilities (CLEFs) appointed to operate under the Scheme.

This document, UKSP 02 Part II, describes the requirements on the conduct of evaluations performed by CLEFs under the Scheme.

In the event of any questions concerning this publication, or for further information, please consult the Certification Body.

Address: UK IT Security Evaluation and Certification Scheme
IA Delivery Office
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Telephone: +44 (0)1242 221491, Ext 30074

Facsimile: +44 (0)1242 709194

Email: iacs@cesg.gsi.gov.uk

Website: <http://www.cesg.gov.uk>

**UK IT Security Evaluation & Certification Scheme
Conduct of an Evaluation**

AMENDMENT RECORD

Amendments to this document will be published as and when required.

| Issue Number | Major Changes | Date |
|---------------------|--|---------------|
| 2.0 | Version for use with Revised Certification Processes. (Issue 1.1 remains applicable for applications that still use the previous certification processes.) | December 2005 |
| 2.1 | Added requirement for consideration of public domain vulnerability information. | March 2006 |
| 2.3 | Refinements and clarifications. | October 2008 |
| 2.4 | Refinements and clarifications. | December 2009 |

**UK IT Security Evaluation & Certification Scheme
Conduct of an Evaluation**

ABBREVIATIONS AND REFERENCES

Please refer to the *Abbreviations and References* document [UKSP00] on the Formal Documentation page of the CESG website at <http://www.cesg.gov.uk>.

**UK IT Security Evaluation & Certification Scheme
Conduct of an Evaluation**

CONTENTS

| | | |
|-------------|---|----------|
| I. | INTRODUCTION..... | 1 |
| | General | 1 |
| | Objectives | 1 |
| | Scope | 2 |
| II. | CLEF ORGANISATION | 3 |
| | Introduction | 3 |
| | Scheme Related Work | 3 |
| | Booking Certification Services..... | 3 |
| | Evaluation Tasks | 3 |
| | Supply of Documentation to the CB | 4 |
| | Task Initiation | 4 |
| | Independence | 4 |
| | Task Confidentiality | 4 |
| | Marking of Evaluation Outputs | 5 |
| III. | PREPARATION PHASE..... | 6 |
| | Introduction | 6 |
| | Evaluation Work Programme | 6 |
| | Task Startup Review | 7 |
| | Deliverables List | 8 |
| | Security Target Review | 8 |
| IV. | EVALUATION AND CERTIFICATION PHASE | 9 |
| | Introduction | 9 |
| | Evaluation Process | 9 |
| | Evaluation Progress Reviews..... | 10 |
| | Task Records | 10 |
| | Observation Reports | 11 |
| | Observation Report Status Register..... | 13 |
| | Evaluation Technical Report | 14 |
| | Certification Report | 17 |
| | Task Closedown..... | 18 |
| | Disposal of Task Material | 18 |

**UK IT Security Evaluation & Certification Scheme
Conduct of an Evaluation**

(This page is intentionally left blank¹)

¹ Regarding the “Blank Page” problems, and their solutions in Word, please refer to:
<http://sbarnhill.mvps.org/WordFAQs/BlankPage.htm>

UK IT Security Evaluation & Certification Scheme

Conduct of an Evaluation

I. INTRODUCTION

General

1. Scheme Publication UKSP 02 defines the requirements on the startup and day-to-day operation of a Commercial Evaluation Facility (CLEF), and is divided into two parts:
 - a) Part I sets out the objectives, assessment criteria and requirements for evidence for a Company wishing to be appointed as a CLEF.
 - b) Part II, this document, sets out the procedural requirements pertaining to the conduct of evaluations performed by a CLEF.
2. This document should be read in conjunction with UKSP 01, Description of the Scheme, and UKSP 03, Sponsor's Guide. For a list of abbreviations and references, see the *Abbreviations and References* document on the CESG website at <http://www.cesg.gov.uk>

Objectives

3. The objective of this document is to define the procedures to be applied during the course of evaluations conducted under the Scheme and, in particular, how the Scheme should be implemented in the CLEFs.

4. All CLEF responsibilities for evaluations with respect to Scheme requirements are indicated, thus, in text boxes.

5. To satisfy the accreditation criteria of the United Kingdom Accreditation Service (UKAS), it is necessary that established procedures are used for the conduct of all evaluations performed under the Scheme. Many of the CLEF responsibilities identified in this document reflect UKAS requirements; however the appropriate UKAS documentation must be consulted concerning the full accreditation requirements for the CLEF.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

Scope

6. The evaluation procedures defined here are applicable to the Information Technology (IT) security evaluations of products² against the criteria laid down in the Common Criteria or IT Security Evaluation Criteria, subject to the relevant International Interpretations, UK Interpretations and Scheme Information Notices (SINs). These procedures cover the following phases of an evaluation task:

- Preparation;
- Evaluation and Certification;

7. These procedures are applicable equally to concurrent or consecutive evaluation, i.e. when performed simultaneously with the development of a Target of Evaluation (TOE) or after the development of a TOE. They also apply to re-evaluations or re-use of the results of a previous evaluation of a TOE.

² The processes described by this document relate to internationally recognised evaluation and certification of products. Some aspects may also be more widely applicable to similar IA services.

II. CLEF ORGANISATION

Introduction

8. A CLEF has a number of obligations placed on it by the Scheme. The fundamental aim of these obligations is that each CLEF organises its work in a way that allows the Certification Body (CB) to ensure the Scheme is adhered to and provide certificates in a timely, repeatable, manner.

9. This chapter provides a framework for the organisation of a CLEF conducting evaluations under the Scheme.

Scheme Related Work

10. The CLEF must keep the CB informed of all Scheme related work that is being performed.

11. It is the responsibility of the CLEF to notify the CB of the status of all Scheme related work being performed in the CLEF. CLEF Progress Meetings offer a general opportunity for this.

Booking Certification Services

12. The CLEF and Sponsor must ensure that the necessary certification services are booked.

13. For specific evaluation tasks the required certification services will need to be booked. The CLEF and Sponsor are individually responsible for making the necessary bookings. An initial booking will be needed for the Task Startup Review and Task Startup Meeting. Thereafter bookings will be needed for the certification activities specified in the Certification Work Programme³ and for other issues where the CLEF or Sponsor requests the input of the CB. Bookings should be made with either the CB's service support team or the service delivery manager appointed for the task.

Evaluation Tasks

14. The CLEF must partition its work into discrete tasks.

15. For the purposes of planning and reporting, a task corresponds to the work performed by a CLEF for the evaluation of a single TOE.

16. A task must be uniquely identified throughout its life-time. The identification shall be such that the TOE and related items cannot be confused physically or when referenced in records or other documents.

³ The *UK CB Standard Certification Work Programme* may be used either as provided or as a template to incorporate contract specific details. It is available at:
http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/formal_docs.shtml

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

Supply of Documentation to the CB

17. All documentation supplied by the CLEF to the CB must be in softcopy format, either on suitable removable media or via email.

18. In some cases hardcopy documents will be accepted as a temporary measure - on the understanding that softcopy versions will be supplied before task closedown.

Task Initiation

19. The CLEF must notify the CB when it is ready to perform an evaluation task, naming the appointed task leader.

20. Certification activity will not normally commence until:

- a contract is in place covering the provision of the CB's services;
- the CLEF is ready to perform its preparation phase activities.

21. The CLEF's contract with the Sponsor must ensure adequate provision for technical support from the Sponsor during the evaluation.

22. This should include CLEF contact with the Developer, where different from the Sponsor, and any other relevant consultants. The CLEF should arrange any Specialist Evaluators as appropriate.

Independence

23. The work performed by the Evaluators must be independent of the development of the TOE.

24. For more details of the rules of independence, see UKSP 02 Part I.

Task Confidentiality

25. Task information must be handled in accordance with confidentiality agreements and the CLEF's Security Manual. This applies especially to information on tasks that are being run remotely or virtually.

26. Confidentiality agreements may be required between the parties involved.

27. The CLEF must implement policies and procedures to protect the confidentiality of a client's proprietary information. These policies and procedures should include protection for the electronic storage and transmission of results.

28. Task information must also be stored and handled in accordance with the CLEF's Security Manual (see Part I of UKSP 02) which is required to comply with the requirements for CLEF appointment.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

29. The Evaluators should advise the CB of the Sponsor's and Developer's wishes with regard to the confidentiality of proprietary information and ensure that evaluation output is appropriately structured and marked.

Marking of Evaluation Outputs

30. All evaluation outputs must be marked "<LF_/T___> EVALUATION IN CONFIDENCE" (unless not required).

31. The marking "EVALUATION IN CONFIDENCE" is used to indicate the presence within a document of sensitive material which, if misused, could undermine the security of a TOE or compromise client confidentiality. The material is, therefore, releasable only to those with a need to know. The "<LF_/T___>" prefix is used to identify the particular CLEF and task concerned.

III. PREPARATION PHASE

Introduction

32. This chapter describes the procedures to be followed by a CLEF in performing the Preparation Phase.

33. The CLEF is required to:

- a) produce an Evaluation Work Programme and participate in the Task Startup Review, which may involve attending a Task Startup Meeting;
- b) check on the availability of deliverables for evaluation;
- c) review the Security Target.

Evaluation Work Programme

34. The Evaluators must agree their Evaluation Work Programme during the Task Startup Review, or Task Startup Meeting, to communicate task specific details of the evaluation process to the CB.

35. Evaluations have a generic form which should be tailored to the specific TOE. The Evaluation Work Programme describes task specific details in the context of this generic form.

36. The Evaluation Work Programme must contain the following information as a minimum.

- Reference to applicable criteria, interpretations and Scheme requirements, together with a statement confirming that these will be followed.
- The approach to the evaluation where the criteria or methodology needs to be applied to novel technology or where the environmental IT security is complex, including the approach to any specialist security field.
- Initial ideas about potential vulnerabilities and how this will affect evaluation activities such as vulnerability analysis and testing.
- Initial ideas for planned test configurations, including the IT environment, and rationales about the sufficiency of test configurations.
- Any responsibility for and method of cryptographic evaluation.
- The method of verifying acknowledgement of any complementary assurance results (e.g. checking published certification information for cryptographic functionality).
- The approach to the task, if a re-evaluation of a previously certified TOE.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

37. The Evaluation Work Programme is reviewed and approved initially at the Task Startup Meeting (or as part of the Task Startup Review process).

Task Startup Review

38. A Task Startup Review will be arranged to carry out the initial assessment of the definition and scope of the TOE. If a Task Startup Meeting is required, this is normally chaired by the CB and involves the CLEF, the Sponsor and, if appropriate other stakeholders, such as the Developer.

39. The CB may agree not to hold a Task Startup Meeting in some cases, for example for a straightforward re-evaluation, in which case the Task Startup Review will be performed without the need for a meeting.

40. The CLEF must attend a Task Startup Meeting, if it is required. If a Task Startup Meeting is not held then the CLEF, the Sponsor and the CB must address by other means all of the relevant issues that are required by the Task Startup Review.

41. The following is a proposed agenda for Task Startup Meetings, with notes on the individual items.

1. *TOE Overview*. The Sponsor presents the proposed TOE based on the TOE Scope Information provided in advance of the meeting. The CB may accept this as suitable at the meeting or may defer its decision for a few days.
2. *Evaluation Work Programme*. The CLEF presents its plans and an Evaluation Work Programme. The CB may accept this as suitable at the meeting or may defer its decision for a few days.
3. *Certification Work Programme*⁴. The CB presents its Certification Work Programme which defines any requirements for further review processes.
4. *Vulnerability Management*. The meeting discusses the status of known and potential vulnerabilities, together with proposals for risk management and recommendations for the frequency of review (monthly, quarterly, annually, etc).
5. *Other Items* as required. This gives an opportunity for the CB, CLEF, Sponsor or any other stakeholder to raise any further issues about the evaluation and certification processes.
6. *Summary of Actions*. Normally this includes formal issue of revised agreed documentation - the TOE Scope Information from the Sponsor, the Evaluation Work Programme from the CLEF and the Certification Work Programme from the CB.

⁴ The UK CB Standard Certification Work Programme may be used either as provided or as a template to incorporate contract specific details. It is available at:
http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/formal_docs.shtml

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

42. The CLEF must produce a formal record of any required TSM and distribute the record appropriately.

43. If the TSM is not required then the reason shall be documented (e.g. in an email) by the CB as part of the Task Startup Review and distributed to the CLEF and the Sponsor.

Deliverables List

44. The CLEF must ensure that the Sponsor has contractually agreed to supply deliverables that are appropriate to the scope of the evaluation and the target assurance level.

45. It is recommended that Evaluators record deliverables received for a specific task in a task specific deliverables list on receipt, to help facilitate referencing during the evaluation and its archive and disposal after completion of the work. However, only those deliverables pertinent to the evidence required to support the evaluation need be referenced in the final Evaluation Technical Report (ETR).

Security Target Review

46. Following the Task Startup Review or Task Startup Meeting, the Evaluators must:

- (a) carry out the formal evaluation of the Security Target according to the appropriate criteria and methodology, and**
- (b) ensure that the Security Target defines a TOE which corresponds to the scope of evaluation agreed in the Task Startup Review or at the Task Startup Meeting.**

47. The CB determines at the Task Startup Meeting whether the proposed TOE is certifiable in principle under the Scheme. It then determines whether the Security Target is an acceptable document describing the agreed TOE through its own and the CLEF's review.

48. If satisfied, the CB will formally accept the TOE into the Scheme.

IV. EVALUATION AND CERTIFICATION PHASE

Introduction

49. This chapter describes the procedures that should be followed in performing the following aspects of the evaluation work:

- a) performing the evaluation and reporting evaluation progress;
- b) producing Observation Reports (ORs);
- c) reporting the detailed results of the evaluation;
- d) drafting the Certification Report.

Evaluation Process

50. During the Evaluation and Certification phase, the Evaluators perform the technical evaluation work as defined by the Evaluation Work Programme and relevant evaluation methodology and interpretations, together with the Vulnerability-Centric Evaluation paper [VUL]. This will result in the task records, ORs and ETR discussed later in this chapter.

51. The Evaluators must consider public domain vulnerability information relevant to the TOE.

52. Understanding the TOE and the identification of potential vulnerabilities are central to the evaluation process. In addition to the deliverables supplied to the CLEF to support the evaluation, public sources may also give information relating to potential vulnerabilities in the TOE.

53. The Evaluators must keep a record of all significant contacts with the CB, the Developer and the Sponsor that influence the evaluation results.

54. During the evaluation there will be occasions when the Evaluators need to consult with one or more of the other parties involved in the evaluation and certification process:

- The Developer will host a Development Environment Assessment, if required by the evaluation assurance level⁵, and may be consulted on other issues associated with the evaluation of the deliverables.
- The Developer or Sponsor will need to be consulted if they will be providing facilities for Evaluator testing.
- The Sponsor will be informed of evaluation progress and made aware of significant issues which arise in the course of the evaluation.

⁵ The CB may waive the requirement if there has been a recent, relevant and successful DEA.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

- The CB's Evaluation Progress Reviews will be supported.
- For a system evaluation, the Accreditor and/or Procurement Bodies may need to be consulted with regard to operational aspects.

Evaluation Progress Reviews

55. Evaluators must participate in Evaluation Progress Reviews, as required by the CB. If a new UK National Interpretation is required then the CLEF must raise the issue with the CB. The interpretation will then be addressed through the CCUKSG.

56. Evaluation Progress Reviews give the CB visibility of significant aspects of the evaluation. The objective of these reviews is for CB contributions to add value to the evaluation in a timely manner. The Evaluators should therefore ensure that the CB sees those aspects of the evaluation identified in its Certification Work Programme, at appropriate points in the evaluation. Similarly the Evaluators should ensure that the CB sees any other significant issues which arise (e.g. if the Sponsor contests a level 1 or 2 OR) or if they become aware of flaws in the basis on which previous evaluation work was conducted (e.g. if the agreed scope of evaluation is brought into question). UKSP 01 lists examples of potential points of focus for Evaluation Progress Reviews.

57. When performing its Evaluation Progress Reviews the CB's checking of the CLEF's application of criteria and methodology to the TOE will either be indirect, in the context of considering significant aspects of the evaluation, or on a sampling basis.

58. Some Evaluation Progress Reviews may involve Evaluation Progress Meetings for which it may be appropriate for the Sponsor, Developer or other stakeholders to attend.

59. The CLEF must produce a formal record of any EPM and distribute the record appropriately.

60. During the Evaluation Progress Reviews the CB may wish to consider refinements proposed by the CLEF to the evaluation strategy previously specified in its Evaluation Work Programme, e.g. sample of source code selected for evaluation or detailed test strategy. These refinements may be added to the Evaluation Work Programme, Evaluation Technical Report or specified in other referenced evaluation documents.

61. During the course of its certification activities the CB may refine its Certification Work Programme, e.g. it may wish to follow through an issue arising in one evaluation activity through to another activity. Such refinements may be issued in the form of an updated Certification Work Programme.

Task Records

62. For each task, the Evaluators must ensure that a systematic record of all information is maintained in accordance with the CLEF's Quality Manual.

63. The records must include adequate cross referencing to enable correlation between, for example, ORs and deliverables affected.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

64. As the evaluation work is performed, the work done, observations made and results obtained must be recorded clearly and permanently as they occur, and must reference the source of the information to which the records relate in sufficient detail to establish an audit trail. For example, the record of work performed may comprise notes maintained in:

- Evaluator day books;
- working notes maintained in a separate work file;
- annotated deliverables, only where the Sponsor or Developer does not specifically require these deliverables to be returned or destroyed after the evaluation.

65. The records must be legible, readily retrievable and stored within an environment that reduces the risk of loss, damage and deterioration.

66. Where computer based tools are used, it is not necessary to retain all output generated, but as a minimum the output retained must include that which relates to and provides traceability to:

- evaluation results as reported in the ETR;
- ORs;
- parts of a TOE which may be re-evaluated or assurance maintained.

Observation Reports

67. Evaluators must raise ORs to draw attention to vulnerabilities and other significant problems, as and when they are discovered, during an evaluation.

68. The Evaluators will raise ORs to document vulnerabilities or other problems discovered in the course of performing the evaluation.

69. Each OR that is raised has a severity level assigned as follows:

- *Level 1* – For any failure of the TOE to comply with its security objectives and security requirements that constitutes an exploitable vulnerability.
- *Level 2* – For any inability to comply with assurance requirements which increases the risk of an exploitable vulnerability remaining undetected; or for any inability to comply with security functional requirements which constitutes a potential vulnerability. A Level 2 OR will also be used where an unacceptably high number of Level 4 ORs would otherwise exist.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

- *Level 3* – For requesting clarification⁶ from the Sponsor or Developer, in order to confirm whether a Level 2 or Level 4 OR is required⁷.
- *Level 4* – For reporting any inability to comply with the assurance requirements that does not warrant a Level 2 OR.

70. An OR at Level 1, 2 or 3 will, if not resolved, prevent certification of the TOE. Such ORs require a response from the Sponsor. The existence of unresolved Level 4 ORs will not prevent certification (unless an unacceptably high number of Level 4 ORs has resulted in a Level 2 OR), but a response is desirable.

71. The Scheme requires that ORs, released to the Sponsor and the CB separately from the ETR, be authorised by a named Qualified Evaluator. However, this requirement should also comply with any requirements defined within the CLEF Quality Manual.

72. The OR title page, provides the following information:

- Task Identification;
- OR Severity Level;
- OR Identification - Sequence Number, Issue Number and Date;
- OR Summary;
- Deliverables Affected;
- OR Authorisation - Author and Task Quality Assurance.

73. The main body of an OR comprises a written report in three sections as follows:

- Observation;
- Implications;
- Recommended Action.

74. The *Observation* section should describe the problem being reported in sufficient detail to enable the nature of the problem and its implications to be understood. It should reference sections of deliverables and areas of functionality and criteria, where relevant.

⁶ Alternatively, clarification can be requested by email or phone provided that the response and the final resolution will be completed *efficiently* (e.g. within 5 working days). However, the decision to raise either a Level 2 OR or a Level 4 OR still remains, although the information provided by the Sponsor or Developer may be sufficient to completely resolve the associated problem(s) and then an OR will not be necessary.

⁷ Note that the confirmation that is provided will enable the Level 3 OR to be formally *withdrawn* and an appropriate new Level 2 OR or Level 4 OR will be issued, if necessary. Equivalently, the Level 3 OR can be *reclassified* as a Level 2 OR or a Level 4 OR, if necessary.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

75. Where the OR has been raised as a result of the findings of tests, sufficient information must be provided to enable the documentary evidence of the tests to be traced, e.g. to penetration test records.

76. The observation should be reported objectively, and without offering advice or design updates as recommended actions. The text should state clearly what the Evaluators analysed and what they observed during their activities. The Evaluators should take care to preserve independence in reporting observations.

77. The *Implications* section should identify the implications, security or otherwise, for the evaluation, caused by the problem identified in the observation section, including for example:

- how the problem constitutes an exploitable vulnerability or potential vulnerability;
- the possible threats to the implemented TOE which may result in a violation of the security requirements;
- whether the problem could constitute a fail verdict or inconclusive verdict against a given evaluation criterion;
- whether the problem may have an impact on some later aspect of the evaluation work;
- any possible impact on the evaluation itself, e.g. evaluation timescales.

78. The *Recommended Action* section should identify options for how the problem can be resolved. If no specific action is recommended by the Evaluators, this should be stated.

79. Any recommended action specified by the Evaluators should normally be aimed at the Sponsor or the Developer of the TOE, as appropriate, and should be stated in general terms, e.g. the document to be updated. Care should be taken as the Scheme precludes Evaluators from contributing to the development of a TOE.

Observation Report Status Register

80. The Observation Report Status Register (ORSR) is maintained by the Evaluators during the active life of an evaluation task and is used to communicate progress to the Sponsor and CB. The ORSR is split into four sections, one for each severity level.

81. The ORSR for a specific task should detail the following information for each OR:

- its unique sequence number;
- severity level;
- issue number of OR;

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

- date when OR status came into effect;
- summary of observation;
- status of OR (see below).

82. The status assigned to each OR should be selected from the table below:

| Key | Status |
|-----|------------------------------|
| REL | Released to Sponsor and CB |
| PRO | Corrective action proposed |
| REJ | Corrective action rejected |
| AGR | Corrective action agreed |
| FIX | Fix to be evaluated by CLEF |
| CAP | Certification action pending |
| CLR | Cleared |
| WDN | Withdrawn |
| NAR | No Action Required |

83. The CB may rule on the status of ORs where the CLEF and Sponsor disagree.

84. For an ORSR to function effectively, an individual OR must refer only to a single observation or to a single set of closely related observations. Observations in sets should be individually numbered, listed and tracked in the ORSR. In order for the history of an OR to be evident in the ORSR, old entries should not be deleted from the ORSR when their status changes.

Evaluation Technical Report

85. The CLEF must produce a final ETR and supply a copy to the CB.

86. The objective of an ETR is to report the Evaluators' findings. It is released to the CB, and all non-proprietary parts released to the Sponsor, by the CLEF.

87. A named Qualified Evaluator should take responsibility for the production of the ETR.

88. For evaluations conducted under the Scheme, the Evaluators' findings may be spread throughout a number of ETRs and ORs. The final ETR must draw together and summarise the results and conclusions of any earlier ETRs. In particular, for a TOE to be certified, there must not be any outstanding ORs at Level 1, 2 or 3 in the final ETR.

89. The CB should previously have been made aware of significant findings, sometimes through use of draft ETR material, in the course of its certification reviews. It will usually perform a brief review of the final ETR to check consistency with its earlier reviews, and will implicitly accept it upon agreement of the Certification Report.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

90. Guidance on the structure and minimum contents of an ETR is provided in the relevant methodology⁸. The ETR will include the following.

- a) An Introduction.
- b) A description of the architecture of the TOE including its security features.
- c) Evaluation methods, with mention of any tools and techniques used during the evaluation, by reference to the Evaluation Work Programme or otherwise.
- d) Summary of the results of the evaluation.
- e) Guidance for Re-evaluation and Impact Analysis. (Optional)
- f) Conclusions and recommendations.
- g) List of evaluation evidence.
- h) List of Acronyms/Glossary of Terms.
- i) The evaluated configuration.
- j) Detailed evaluation results.
- k) The ORSR.
- l) Summary of TOE testing.

| |
|--|
| 91. The ETR must precisely identify the evaluated configuration of the TOE. |
|--|

92. The following items must be specified, with hardware, firmware and software detailed as applicable:

- version numbers of all installation components of the TOE, including patch/release numbers where applicable;
- any configuration options selected when installing the TOE;
- specification of any platforms and other environmental IT components, including version number of all major platform components.

93. These items must be specified for the version, configuration and operational environment for which claims are made for the TOE and those used in testing the TOE. Where those specified for testing are representative of those claimed then supporting

⁸ See the *Write ETR sub-task* section in [CEMv2.3] or [CEMv3.1], as appropriate.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

rationales should be included in the ETR to justify their sufficiency, together with results for representative test configurations on different platform architectures⁹.

94. If any of this information is included in another document, e.g. a configuration list required by the criteria, then the ETR may reference it.

95. The ETR must include a deliverables list.

96. It is permissible for an ETR to refer to a separately supplied deliverables list, which contains a list of those deliverables used as evidence by the Evaluators during the evaluation.

97. The Evaluators must report work performed and the detailed results in the ETR, as required by the evaluation methodology, giving sufficient justifications for verdicts and conclusions.

98. The report for each evaluation activity should comprise the following information:

- the inputs to the work;
- details of techniques and tools used in performing the work;
- details of sampling methods used in performing the work;
- verdicts and supporting justifications, e.g. the work performed and the results obtained, including references to any ORs issued, in accordance with the appropriate methodology and interpretations;
- the Evaluators' conclusions.

99. The question of what constitutes a sufficient verdict justification for a given evaluation activity is typically the subject of a published Scheme Interpretation. For example, for CC version 3.1 it would be UK CC Interpretation UK/3.1/007 and for CC version 2.3 it would be UK CC Interpretation UK/2.3/007.

100. Evaluators must ensure that scripts for penetration tests and additional implementation tests are recorded in sufficient detail to allow repeatability and reproducibility.

101. Completed test records should be included in the ETR; otherwise whichever documents contain them must be referenced by the ETR.

102. When adding to or modifying test scripts, due consideration must be given to the configuration control of the scripts and results. Precise requirements for the storage of additional or modified scripts and their accompanying results, and the updating of configuration control records, will be dependent on the context of the evaluation. It is

⁹ The UK CC Interpretation *Multi-platform TOEs* (UK/2.2/012 or UK/3.1/012) may be useful here.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

envisaged that this will probably be required for a re-evaluation, but probably not for the re-use of a certified component in a composite TOE.

103. When a tool is used to assess one or more test items this must be recorded in sufficient detail to allow repeatability or reproducibility.

104. Information allowing the tool to be identified and a broad description of how the tool was used must be provided. For example, for a software tool, the ETR should state:

- the software version number;
- the environment in which the software was run, e.g. hardware platform, operating system, other dependent software, environment variable settings;
- the functionality of the tool, e.g. by menu options;
- how the tool was applied to test items, including configuration, parameters and mode of use;
- details of any sampling, using the tool;
- details of any test data.

105. The details of tools should appear either in the ETR or in a separate document, referenced by the ETR.

Certification Report

106. The Certification Report is drafted by the CLEF and formally issued by the CB, with the Sponsor providing any additional clarification.

107. The CLEF must produce the draft Certification Report for the evaluation.

108. The following procedures apply for drafting the Certification Report.

- a) The Certification Report is first drafted by the Evaluators, based on a template format provided by the CB.
- b) The CLEF circulates the draft Certification Report to the CB and the Sponsor for comments. It should ensure that the CB sees any comments made by the Sponsor.
- c) The CLEF produces an updated version to incorporate any comments returned.
- d) The CB remains the signatory of the Certification Report and formally issues the final agreed version together with the associated Certificate.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

Task Closedown

109. When the CLEF has completed the evaluation work that it has been contracted to perform and the Certification Report and Certificate (if any) have been agreed and issued by the Certification Body, the CLEF can close down the task. It archives, returns or destroys, as appropriate, all material which relates to the task.

110. The following checklist may be used for task closedown.

- Archive Baseline produced and distributed?
- ETR produced and agreed by all parties?
- Certification Report and Certificate agreed and issued?
- Softcopy files provided for CB?
- Task material disposed of - archived, returned to originators or destroyed?
- Task specific computer accounts archived and deleted?
- Task specific magnetic media archived or erased?
- All material not archived or returned has been destroyed?
- All evaluation and certification issues have been suitably addressed.

Disposal of Task Material

111. Archived material must be kept for a period of not less than six years from the end of the evaluation, with sufficient test records archived to ensure the repeatability and reproducibility of tests and results or to resolve potential disputes.

112. Throughout an evaluation, material should be organised in such a way as to make the actual task closedown as simple as possible. A task closedown can also be simplified by returning and/or destroying superseded documents throughout the evaluation.

113. Where files have been retained in softcopy formats, there is no requirement to maintain hardcopy versions of the files. Softcopy files should be suitably protected, for example by making them read only and having offsite backups.

114. For the task closedown, the CLEF must produce an Archive Baseline. This must list all the task material and must detail how the material has been disposed of, i.e. whether it has been archived, returned or destroyed.

115. The Archive Baseline must give sufficient details for each individual item to enable the item to be identified in future, if necessary. One copy of the Archive Baseline should be held by the CLEF.

UK IT Security Evaluation & Certification Scheme Conduct of an Evaluation

116. In general, material that is received from Sponsors or Developers will not be archived, but will be returned to them or destroyed, as agreed between the CLEF and the Sponsor.

117. The CLEF's Quality Manual will indicate the requirements for archiving. As a minimum, the following task material should normally be archived by the CLEF:

- quality records, e.g. document review histories;
- task logbooks and Evaluator test/review notebooks;
- the Archive Baseline;
- the Security Target, the deliverables list if produced, and the Evaluation Work Programme;
- identification of evaluation tools and associated outputs relevant to the reported results;
- evaluation correspondence (such as letters and emails) that has a direct bearing on the outcome of the evaluation;
- ETR(s), including issued drafts, related test scripts and unresolved ORs.

118. The CLEF must inform the CB if a Sponsor or a Developer, to whom it is intended to return material for archiving, is unable to ensure the continued availability of that material to assist the process of maintaining the certification.

119. In such circumstances the CB will wish to determine how best to maintain the certification, e.g. to enable resolution of any dispute.