UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No. 2

CLEF REQUIREMENTS

Part II

CONDUCT OF AN EVALUATION

Issue 3.1
August 2013

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 (IT) products and systems using methodologies and procedures that facilitate international mutual recognition of certification results (certificates) between national schemes.

The Scheme is operated by the CESG Certification Body (CB), which appoints Commercial Evaluation Facilities (CLEFs) to conduct secure product and system evaluations which are overseen by the CB. The results of successful evaluations are certified and published for use by consumers.

Scheme Publication UKSP 02 defines the set of requirements on the 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 or feedback, please consult the CESG Certification Body.

Address: CESG Certification Body
UK IT Security Evaluation and Certification Scheme
IA Service Management
CESG, Room A2j
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Email: cc@cesg.gsi.gov.uk
Facsimile: +44 (0)1242 709052
Website: http://www.cesg.gov.uk

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
3.0	Refinements for consistency with CGOR, GPG55 and other CESG services; and minor changes for clarification.	January 2013
3.1	Minor updates as a result of internal reviews.	August 2013

ABBREVIATIONS AND REFERENCES

Please refer to the *Abbreviations and References* document [UKSP00], for the definition of all standard Scheme terms and UK Scheme Publications, on the Formal Documentation page of the CESG website at http://www.cesg.gov.uk.

CONTENTS

UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part II – Conduct of an Evaluation

I. INTRODUCTION

General

1. Evaluations under the UK IT Security Evaluation and Certification Scheme ('the Scheme') are performed by Commercial Evaluation Facilities (CLEFs) which are managed and staffed by commercial organisations and are appointed by the CESG Certification Body (CB[1]) of the Scheme.

2. Scheme Publication UKSP 02 defines the requirements on the start-up and day-to-day operation of a 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.

3. This document should be read in conjunction with UKSP 01 *Description of the Scheme* and UKSP 03 (Parts I & II) *Sponsor's Guide*. For a list of abbreviations and references, see UKSP 00 *Abbreviations and References.*

Objectives

4. 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.

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 a CLEF.

Scope

6. The evaluation procedures defined here are applicable to the Information Technology (IT) security evaluations of products[2] against the criteria laid down in the Common Criteria (CC), subject to the relevant Protection Profiles (PPs) and supporting documents, International Interpretations, UK Interpretations and Scheme Information Notices (SINs). These procedures cover the following phases of an evaluation task:

- Preparation;
- Evaluation and Certification.

---

[1] In this document, 'CB' always refers to the CESG Certification Body.

[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.

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.

Terminology

8. All mandatory requirements on a CLEF are highlighted in this document by the use of shaded text boxes and are also relisted in Appendix G. As a general rule, the word **must** is used to indicate a mandatory requirement on a CLEF.

9. The word **should** is used to indicate a preferred approach, where deviation may be permitted under certain circumstances (e.g. if supported by a rationale approved by the CB).

II. CLEF ORGANISATION

Introduction

10. A CLEF has a number of obligations placed on it by the Scheme and UKAS. The fundamental aim of these obligations is that each CLEF organises its work in a way that allows the CB to ensure the Scheme is adhered to and provides certificates and certification reports in a timely, repeatable, manner.

11. This chapter provides a technical framework for the organisation of a CLEF conducting evaluations under the Scheme. For general organisational procedures addressing topics such as booking services, task initiation, security requirements, task confidentiality and independence, and CLEF progress reports and meetings, see UKSP 02 Part I.

Evaluation Tasks

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

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

14. 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.

CB Oversight

15. The activities performed by the CB to monitor CLEF activities on a specific evaluation task are detailed in the Certification Work Programme (CWP). The CWP states the documentation required to support these activities, which are summarised as:

- Task Startup Review;
- Security Target Review;
- Evaluation Progress Reviews;
- Certification Review.

16. These activities and related CLEF requirements and obligations, are described in more detail in the following chapters.

III. PREPARATION PHASE

Introduction

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

18. The CLEF is required to:

a) produce an Evaluation Work Programme (EWP) and participate in the Task Startup Review (TSR), which may involve attending a Task Startup Meeting (TSM);

b) check on the availability of deliverables for evaluation;

c) review the Security Target (ST).

Evaluation Work Programme

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

20. 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.

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

- Reference to applicable criteria, methodology, 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.

- Test Plan (or a reference to it), including test configurations, IT environment, strategy, objectives, scripts, and security functional test ideas.

- 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.

- Team composition including Task Leader and Trainee/Qualified/Specialist Evaluators (see Chapter IV of UKSP 01 Part I).

22. 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

23. 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.

24. 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.

25. The CLEF must attend a Task Startup Meeting, if it is held. 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.

26. The TSM Standard Agenda and the TSM Template Agenda are available at:

http://www.cesg.gov.uk/servicecatalogue/CCITSEC/Pages/Formal-Documentation.aspx

Also available is the UK CB Standard Certification Work Programme, which may be used either as provided or as a template to incorporate contract specific details.

27. At the TSM, the CB may accept the TOE Scope Information (or draft ST) and the EWP as suitable for the evaluation, or may defer its decision for a few days.

28. The CLEF must produce a formal record (e.g. in the form of Meeting Minutes) of any required TSM and distribute the record appropriately.

29. If the TSM is not required then the reason must 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

30. 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 (e.g. PP-centric assurance level).

31. 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

32. 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 PP(s) and supporting documents, criteria, methodology and interpretations; 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.

33. The CB confirms 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.

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

IV. EVALUATION AND CERTIFICATION PHASE

Introduction

35. 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 (in the ETR);

d) drafting the Certification Report (CR);

e) maintaining adequate technical records.

Evaluation Process

36. During the Evaluation and Certification phase, the Evaluators perform the technical evaluation work as defined by the Evaluation Work Programme (including Test Plan) and relevant PP(s) and supporting documents, evaluation criteria, methodology, interpretations and SINs. This will result in the task records, ORs and ETR discussed later in this chapter.

37. The Evaluators must consider public domain vulnerability information relevant to the TOE, in accordance with the EAL requirements (including PP-centric EAL(s)), and record in the ETR the relevant websites that were referenced.

38. 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.

39. Evaluators must produce a detailed Test Plan that is approved by the CB before starting any formal security tests. The Test Plan may be included in the EWP and should provide the following information:

- Test configurations;
- IT Environment;
- Strategy;
- Objectives;
- Scripts;
- Security functional test ideas;
- Penetration test ideas.

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

41. 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:

a) The Developer will host a Development Site Visit (DSV), if required by the evaluation assurance level including PP-centric EALs[3], and may be consulted on other issues associated with the evaluation of the deliverables.

b) The Developer or Sponsor will need to be consulted if they will be providing facilities for Evaluator testing.

c) The Sponsor will be informed of evaluation progress and made aware of significant issues which arise in the course of the evaluation.

d) The CB's Evaluation Progress Reviews (EPRs) will be supported.

e) For a system evaluation, the Accreditor and/or Procurement Bodies may need to be consulted with regard to operational aspects.

Evaluation Progress Reviews

42. Evaluators must participate in Evaluation Progress Reviews[4], 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.

43. 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 is informed of 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 is informed of 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.

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

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

46. The CLEF must produce a formal record of any decisions made that affect the evaluation or certification outcome and distribute the record appropriately. Decisions regarding resolution of CB review comments should be incorporated in review responses.

---

[3] The CB may waive the requirement if there has been a recent, relevant and successful DSV.

[4] EPRs can be conducted by email, phonecalls or meetings. EPRs can include reviews of EWP, ST, Test Plan, ETR, etc.

47. 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. the 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 (e.g. Test Plan).

48. 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

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

50. The records must include adequate cross referencing to enable correlation between, for example, ORs and deliverables affected, tests and ORs raised, tests and Security Functional Requirements (SFRs).

51. 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.

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

53. Where computer based tools are used, it is not necessary to retain all output generated, but as a minimum the information 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

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

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

56. 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.
- *Level 3* – For requesting clarification[5] from the Sponsor or Developer, in order to confirm whether a Level 2 or Level 4 OR is required[6].
- *Level 4* – For reporting any inability to comply with the assurance requirements that does not warrant a Level 2 OR.

57. 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.

58. 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.

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

- Task Identification;
- OR Severity Level;
- OR Identification - Sequence Number, Issue Number and Date;

---

[5] 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.

[6] 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.

- OR Summary;
- Deliverables Affected;
- OR Authorisation - Author and Task Quality Assurance.

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

- Observation;
- Implications;
- Recommended Action.

61. 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.

62. 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.

63. The CLEF must report each OR objectively, accurately and impartially. Each OR must be reported without offering advice or design updates as recommended actions. The Evaluators must take care to preserve independence in reporting observations.

64. The Observation section should state clearly what the Evaluators analysed and what they observed during their activities.

65. 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.

66. 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.

67. 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

68. 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.

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

- its unique sequence number;
- severity level;
- issue number of OR;
- status of OR (see below).
- date when OR status came into effect;
- summary of observation;

70. 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

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

72. 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

73. The CLEF must produce a final ETR and supply a softcopy to the CB.

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

75. A named Qualified Evaluator should be responsible for production of the ETR.

76. 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 and all verdicts must be "Pass".

77. The CB should previously have been made aware of any significant findings, sometimes through use of draft ETR material, in the course of its Evaluation Progress Reviews. It will usually perform a review of the final ETR during the Certification Review, to check consistency with its earlier reviews, and will approve it upon agreement of the draft Certification Report produced by the CLEF.

78. Guidance on the structure and minimum contents of an ETR is provided in the relevant methodology[7]. The ETR will include the following (but not necessarily in the order given):

a) An Introduction.

b) A description of the architecture of the TOE including its security features.

c) Referenced PP(s) and supporting documents, evaluation criteria, methodologies and interpretations, 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.

[7] See the *Write ETR sub-task* section in [CEMv3.1], as appropriate.

k) The ORSR.

l) Summary of TOE testing.

79. The ETR must precisely identify the evaluated configuration of the TOE.

80. 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 numbers of all major components of platforms.

81. 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 rationales should be included in the ETR to justify their sufficiency, together with results for representative test configurations on different platform architectures[8].

82. 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.

83. The ETR must include or reference evaluation deliverables pertinent to the evaluation evidence.

84. 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.

85. 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.

86. 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 any sampling methods used in performing the work;

[8] The UK CC Interpretation *Multi-platform TOEs* (UK/3.1/012) may be useful here.

- 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.

87. 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 is UK CC Interpretation UK/3.1/007.

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

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

90. 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 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.

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

92. 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.

93. The details of tools should appear either in the ETR or in a separate document, referenced by the ETR. For the task records, logs from automatic tool runs must be maintained and linked to the relevant tests.

Certification Report

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

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

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

a) The Certification Report is first drafted by the Evaluators, based on the latest 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, if necessary, 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.

Task Closedown

97. 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 CB, the CLEF can closedown the task. The CLEF archives, returns or destroys, as appropriate, all material which relates to the task.

98. 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?
- CESG and commoncriteriaportal website entries updated, if required?
- 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 or optical media archived or erased?
- All archived records adequately and securely protected?
- All material not archived or returned has been destroyed?

- All evaluation and certification issues have been suitably addressed.

Disposal of Task Material

99. 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.

100. 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.

101. 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.

102. 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.

103. 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 archived by the CLEF.

104. 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.

105. 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.

106. 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.

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

Appendix A
SUMMARY OF MANDATORY REQUIREMENTS ON CLEFS

This Appendix contains a summary of CLEF Requirements, in the context of their conduct of evaluations, as required by the UKAS or UK Scheme. The main body of this document marks these with shaded text boxes.

Para	CLEF Requirement	Scheme/ UKAS
12	The CLEF must partition its work into discrete tasks.	Scheme/ UKAS
19	The Evaluators must present their outline Evaluation Work Programme before or during the Task Startup Review, or Task Startup Meeting, to communicate task specific details of the evaluation process to the CB.	Scheme
25	The CLEF must attend a Task Startup Meeting, if it is held. 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.	Scheme
28	The CLEF must produce a formal record (e.g. in the form of Meeting Minutes) of any required TSM and distribute the record appropriately.	UKAS
30	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 (e.g. PP-centric assurance level).	Scheme
32	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 PP(s) and supporting documents, criteria, methodology and interpretations; 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.	Scheme
37	The Evaluators must consider public domain vulnerability information relevant to the TOE, in accordance with the EAL requirements (including PP-centric EAL(s)), and record in the ETR the relevant websites that were referenced.	Scheme
40	The Evaluators must keep a record of all significant evaluation decisions made with the CB, the Developer and the Sponsor that influence the evaluation results.	UKAS

Para	CLEF Requirement	Scheme/ UKAS
42	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.	Scheme
49	For each task, the Evaluators must ensure that a systematic record of all information is maintained in accordance with the CLEF's Quality Manual.	UKAS
54	Evaluators must raise ORs to draw attention to vulnerabilities and other significant problems, as and when they are discovered, during an evaluation.	Scheme
62	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.	Scheme
63	The CLEF must report each OR objectively, accurately and impartially. Each OR must be reported without offering advice or design updates as recommended actions. The Evaluators must take care to preserve independence in reporting observations.	UKAS
73	The CLEF must produce a final ETR and supply a softcopy to the CB.	Scheme
79	The ETR must precisely identify the evaluated configuration of the TOE.	Scheme
83	The ETR must include or reference evaluation deliverables pertinent to the evaluation evidence.	Scheme
85	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.	Scheme
88	Evaluators must ensure that scripts for penetration tests and additional security functional tests are recorded in sufficient detail to allow repeatability and reproducibility.	Scheme
91	When a tool is used to assess one or more test items this must be recorded in sufficient detail to allow repeatability or reproducibility.	UKAS
95	The CLEF must produce the draft Certification Report for the evaluation.	Scheme
99	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.	UKAS
102	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.	UKAS

Para	CLEF Requirement	Scheme/ UKAS
106	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.	UKAS

Figure A.1 – Summary of Mandatory Requirements on CLEFs