UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No. 2

CLEF REQUIREMENTS

Part I

START UP AND OPERATION

Issue 4.5
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 CLEFs appointed to operate under the Scheme.

This document (UKSP 02 Part I) describes the requirements on the start-up and operation of 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. All changes made since the last major update of the document will be outlined in the amendment record and marked in the document itself.

Issue Number	Major Changes	Date
4.0	Major update.	April 2003
4.1	Refinements and clarifications.	October 2008
4.2	Refinements and clarifications, especially regarding specialist penetration testers.	December 2009
4.3	Refinements and clarifications regarding Basic Requirements.	October 2010
4.4	Refinements for consistency with CGOR, GPG55 and other CESG services; and minor changes for clarification.	January 2013
4.5	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

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 (this document) sets out the objectives, assessment criteria and requirements for evidence for a company wishing to be appointed as a CLEF.

   b) Part II 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 startup and operation of a CLEF.

5. To satisfy the accreditation criteria of the United Kingdom Accreditation Service (UKAS), it is necessary that established procedures are used to establish a CLEF 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.

CLEF Appointment[2]

6. Appointments are either Provisional or Full. The former is granted to allow evaluations to be performed and monitored so as to enable the appropriate UKAS Accreditation to be awarded; a Full Appointment is granted to cover future evaluations whose criteria and assurance package/level fall within the scope of UKAS Accreditation (see http://www.ukas.com/ for further details). A copy of the Appointment Agreement to be made between a CLEF and the CB is available from the CB.

7. The Appointment Process will give due consideration to any requirements for specialist skill sets and equipment that the CLEF may need, e.g. for evaluating hardware tamper resistance claims, or specialised technologies such as biometric devices. It may be noted that precise requirements for hardware CLEFs are being developed at an international level and (when agreed) will be adopted by the Scheme (see [RICE]).

---

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

[2] With reference to the CCRA, Article 5 *Conditions for Recognition*, part (a): the requirement for the Evaluation Facility to be "*licensed* or *approved*" is satisfied by the term "appointed" in this document.

8. CLEFs are subject to basic requirements and rules of operation specified in detail in this document and CESG Test Laboratory General Operational Requirements [CGOR], which form part of the conditions of appointment. These rules govern:

a) Quality and Management;

b) Security and Confidentiality;

c) Staff Qualifications and Training;

d) Test Methodology.

9. It is assumed that the reader of this document is familiar with the principles of security evaluation and certification as described in UKSP 01 [UKSP01] and the Common Criteria for Information Technology Security Evaluation (CC) [CC].

Criteria

10. Evaluations are carried out according to one of the CB recognised IT security evaluation criteria using the criteria's evaluation methodology, for example the CC [CC] using its Common Evaluation Methodology (CEM) [CEM]. The criteria are subject to the relevant International Interpretations, UK Interpretations and Scheme Information Notices (SINs).

11. As far as possible, UKSP 02 is written to be independent of any particular IT security evaluation criteria. Note that ITSEC/ITSEM is now obsolescent, having been replaced by CC/CEM. Guidance for ITSEC is available from the CB if required.

Terminology

12. The terminology used in this document follows that of "The Conduct of UKAS Laboratory Assessments"[3], although throughout Scheme documents the term "Sponsor" refers to the person or organisation that funds an evaluation. This equates to the "customer" in United Kingdom Accreditation Service (UKAS) terms or "consumer" in CC terms.

13. The term "CLEF" is used for Commercial Evaluation Facilities appointed by the CB to perform the set of CC security evaluations for which the facility is accredited by UKAS. For legal reasons connected with charging for CB services, the word "appoint" is used instead of "license" or "approve".

14. 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.

15. 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).

[3] This document is available at http://www.ukas.com/

Fees

16. Since 1 April 1997, the CB has been required to charge for its services, which had previously been provided free to CLEFs and Sponsors. Areas where fees are levied in respect to CLEF appointment are identified in Annex D. UKAS Accreditation and Assessment is subject to the payment of fees to UKAS, details of which are available from the UKAS Executive.

17. The contracting model for CC evaluations is currently under review and, in due course, is likely to be made consistent with that for other AAS services provided by CESG.

II. SETTING UP A CLEF

Basic Requirements and Criteria

18. For Government work involving Protectively Marked information, a CLEF (and its parent company where applicable) will normally be located and autonomously managed in the UK (the CB may consider exceptions on a case-by-case basis).

19. The primary business objective of a CLEF should be security evaluation under the Scheme and it should aim to become a stable community with minimum staff turbulence.

20. A CLEF must be able to operate as an autonomous unit within the parent company in all day-to-day operational and administrative aspects.

21. To this end a CLEF must be in a secure area of the parent company's premises and it should have:

a) sufficient office furniture and fitments;

b) sufficient administrative and clerical support to ensure the smooth operation of the CLEF whilst maintaining task confidentiality;

c) telephone numbers and email addresses for CLEF points of contact;

d) access controls that permit access only to explicitly authorised CLEF staff;

e) sufficient infrastructure to support evaluation tasks in the Lab and at Developer or other premises.

22. In addition, a CLEF should meet the following basic requirements:

a) sufficient suitably qualified and experienced staff, as defined in Chapters II and IV;

b) secure IT facilities whose logical access controls are capable of supporting multiple evaluation tasks whilst maintaining task separation, confidentiality and integrity;

c) a minimal hardware investigation capability, sufficient to satisfy a basic fault finding and correction requirement;

d) office space available for CB staff, when required;

e) communications facilities enabling secure delivery of information to and from the CB and Sponsor;

f) archive facilities capable of meeting UKAS requirements.

23. A CLEF must be accredited as a testing laboratory by UKAS in accordance with the current UKAS Accreditation Standard, General Requirements for the Competence of Testing and Calibration Laboratories [17025], and the CESG Test Laboratory General Operational Requirements [CGOR].

24. See the *UKAS Accreditation* section of Chapter III for more information.

25. A CLEF must meet all applicable security requirements specified in the *Security and Confidentiality* section below.

26. All new CLEFs must complete a trial evaluation to demonstrate to the CB that:

a) the Evaluators are technically competent (as defined in the *Staff Qualifications and Training* section below*)*;

b) the management and administration of the CLEF is competent to fulfil its role in supporting evaluations.

Quality and Management

Management Objectives

27. The organisational structure of a CLEF must be such as to achieve and maintain:

a) a sufficiently high standard of quality in all aspects of its work, including a Quality Manual to UKAS requirements;

b) security;

c) task confidentiality.

The Quality Manual

28. A CLEF must possess its own Quality Manual that conforms to UKAS requirements.

29. Particular attention must be paid to the maintenance of commercial confidentiality, especially in relation to remote or virtual working. See the *Security Requirements* section below.

Specific Management Roles

30. A suggested structure for a CLEF is described here and illustrated in Appendix E. Other structures will be acceptable, provided that they satisfy the management objectives; the following is therefore offered purely as a guide for new CLEFs.

31. In this suggested structure, each CLEF is headed by a CLEF Controller who has overall management responsibility for the CLEF. The CLEF Controller is directly supported by:

a) a Technical Manager;

b) a Quality Manager;

c) a Business Manager;

d) an Administration Manager;

e) a Security Manager.

32. Evaluation tasks are normally performed by small teams of Evaluators (usually 2 or 3 people) each with a nominated Task Leader who reports to the Technical Manager.

33. Other possible roles include a Computer Manager and a Methods Adviser, who also report to the Technical Manager. Also Technical Consultants who provide specialist evaluator advice on particular TOE types.

34. Some of these roles may be undertaken by the same person, provided no conflict of interest exists between the different roles.

Security Requirements

35. All CLEFs must operate in such a way as to preserve strict commercial confidentiality. This includes any CLEF that intends to operate remotely or virtually, in which case the associated security requirements (covering physical, personnel, procedural and information security aspects) should be included in the CLEF Quality Manual and/or the CLEF Security Manual. CLEFs that wish to be capable of performing evaluation tasks for HMG must additionally be set up and operate in accordance with the requirements of the HMG Security Policy Framework [SPF].

36. The requirements of the UK Government Security Policy Framework [SPF] provide for the security of HMG Protectively Marked information. The UK Government Security Policy Framework requires approved companies to appoint a Security Controller and to operate in accordance with documented Company Security Instructions. It places requirements and constraints for example on:

a) the security of premises;

b) the clearance of staff;

c) the movement and handling of documentation;

d) the movement of visitors into, within and out of secure premises.

37. CLEFs that wish to perform solely commercial work will need to demonstrate to the CB that they have the appropriate levels of commercial security and have staff of appropriate trustworthiness.

The Security Manual

38. A CLEF must possess its own Security Manual that sets out the procedures and responsibilities to be undertaken by all CLEF staff to maintain the high degree of security required to protect commercially sensitive information.

39. The Security Manual should specify procedures for:

a) Physical Security;

b) Personnel Security;

c) Procedural Security;

d) Information Security.

Physical Security

40. The basic requirements for physical security are set out in the *Basic Requirements and Criteria* section above.

41. Each task must be organised and managed so that task material is accessible only to authorised members of the task team.

Personnel Security

42. For those CLEFs who wish to do HMG work, CLEF staff will be subject to the Official Secrets Act and are required to be vetted to at least SC level. Special clearances may be required for some tasks and as a consequence some staff may be subject to overseas travel restrictions.

43. All CLEF staff will need to sign a CLEF-specific confidentiality agreement. Individual agreements may be required in some cases, in addition to or replacing a general CLEF-Sponsor confidentiality agreement.

44. Whilst a CLEF should aim to become a stable unit with minimum turbulence of its staff, the CB accepts that staffing levels may vary according to the CLEF's workload. In the event of insufficient work such staff may perform non-CLEF work for the parent company, subject to rules on commercial confidentiality and impartiality stated in UKSP 01 [UKSP01] and *The Conduct of Evaluations* in Chapter IV of this document.

Procedural Security

45. The Security Manual should define appropriate procedures, including those for:

a) identifying and authenticating staff and visitors;

b) access control to the CLEF premises and the individual rooms within such premises, equipment, cabinets and information;

c) accounting for the movements of CLEF staff and visitors;

d) periodic audit of the procedures;

e) dealing with security incidents and breaches;

f) the security requirements of remote or virtual working;

g) passwords and encryption;

h) secure transmission of information between CLEF and other parties or sites.

46. There must be a nominated person within the CLEF with overall responsibility for the security of the CLEF and the production of the CLEF Security Manual.

47. It is thus necessary for all CLEF staff to maintain records so that adherence to the Security Manual can be audited, as required by the Security Manager and by the CB and UKAS assessors.

Information Security

48. The Security Manual should cover the handling of commercially sensitive information in whatever form it is held.

49. Where CLEFs are involved in processing HMG Protectively Marked information and where this involves the use of IT equipment, that equipment must meet HMG's minimum computer security standards. CLEFs are not required to meet any formal TEMPEST standards (unless required to do so by a Sponsor, in which case the Sponsor may be expected to bear any additional costs). Provision should also be made for processing material at high levels of Protective Marking if required to do so by a Sponsor.

50. Secure communications facilities (approved by CESG) may be needed for some tasks. Media may also be required for transferring sensitive information. The CLEF must ensure that evaluation results and outputs are appropriately protected during transmission between entities (e.g. site to Lab and Lab to another entity.)

51. Provision must be made for the secure storage and archiving of information held on all media and documents.

52. This must take proper account of the requirements for handling Protectively Marked information. As far as practical, CLEFs should ensure that archived data can be retrieved in the future as equipment and technology progress.

53. UKSP 02 Part II [UKSP02-II] describes the requirements pertaining to the disposal of task material at the conclusion of an evaluation.

Task Confidentiality

54. The above measures contribute to the maintenance of task confidentiality. CLEFs may propose arrangements (for example, covering remote or virtual working) to the CB that preserve confidentiality, whilst allowing more efficient management of the work. Such proposals should also be acceptable to Sponsors and/or Developers whose tasks may be involved.

Staff Qualifications and Training

Objectives

55. The training of Evaluators has the aim of producing Qualified Evaluators and Specialist Evaluators who:

a) understand the principles of IT security and information assurance;

b) have a thorough understanding of the principles underlying the evaluation criteria specified in the conditions of appointment;

c) can apply the criteria at any evaluation level specified in the conditions of appointment, consistent with their technical competence or qualification (see below).

Evaluator Status

56. The Scheme recognises three levels of Evaluator qualification:

a) *Trainee Evaluator*, i.e. An Evaluator who has successfully completed an initial training programme;

b) *Qualified Evaluator*, i.e. A Trainee Evaluator who has been assessed by the CB to be capable of contributing to an evaluation without detailed supervision[4];

c) *Specialist Evaluator*, i.e. A Trainee Evaluator who has been assessed by the CB to be capable of contributing to an evaluation without detailed supervision[4] for some subset of the CC Assurance Classes and has extensive knowledge of a specialist security field[5].

57. For the CC Assurance Classes that are within the scope of a Specialist Evaluator, he/she is equivalent to a Qualified Evaluator. For the CC Assurance Classes that are outside the scope of a Specialist Evaluator, he/she is equivalent to a Trainee Evaluator. Appendix B describes how the Qualified Evaluator and Specialist Evaluator statuses are attained and maintained.

[4] See paragraphs 152-155 for further information.

[5] Some (non-exhaustive) examples of specialist security fields are: Anti-Virus, Biometrics, Cryptography, Data Recovery, Formal Methods, Hardware, Intrusion Detection, Penetration Testing, Secure Erasure, Smart Cards, etc.

Training Requirements

58. Trainees new to an existing CLEF must follow a training programme approved by the CB and based on the modules detailed in Appendix B.

59. Evaluator training must be conducted by a Qualified Evaluator, or a Specialist Evaluator if appropriate.

60. The CLEF Technical Manager and any others involved with the technical work, including technical reviews, must have attended all relevant training modules.

61. Senior CLEF staff, such as the CLEF Controller and Business Manager, are normally expected to be familiar with the content of the initial training programme and should have attended all relevant modules.

The Trial Evaluation

62. The purpose of the trial evaluation is to demonstrate to the CB that the CLEF is competent to perform PP and product evaluations to the Common Criteria assurance packages acceptable to the CB and hence to hold a Full Appointment. It is also used as a basis for UKAS assessment. Details are contained in Appendix A.

III. APPOINTMENT AND ASSESSMENT FOR NEW CLEFS

Introduction

63. The appointment of CLEFs is performed by the CB. The award of a Full Appointment will, in part, depend on the CLEF being accredited as a testing laboratory by UKAS. In addition, the CB will need to satisfy itself that the CLEF is competent in areas covered by the Full Appointment, but which fall outside the scope of UKAS Accreditation.

64. Full Appointments are thus awarded to interested commercial companies which have been successfully assessed by both the CB and UKAS. Such appointments confirm that the CLEF is competent to perform security evaluations to specific assurance packages. Any [17025] and [CGOR] Lab may complete a trial evaluation to gain CC on their Scope of Accreditation.

Point of Contact

65. The CB will appoint one of its staff as a Point of Contact (POC) for the candidate CLEF. The POC will have a thorough understanding of the Scheme and be able to discuss any problems that may arise. As far as possible the CB will strive to ensure that the same POC is responsible for processing a CLEF's application through the Trial Evaluation (see paragraph 94 below) to the granting of a Full Appointment and thereafter for dealing with the CLEF during the early years of its membership of the Scheme.

66. The POC will also act as a Training Officer who will provide day-to-day technical support and direction for the duration of the trial evaluation.

Award of Provisional Appointment

67. An applicant company may apply to the CB for a Provisional Appointment at any time on its own initiative, or in response to a general invitation to industry from the CB.

68. The applicant company must submit a proposal to the CB detailing how it proposes to set up and manage a CLEF in accordance with the Scheme rules and the requirements and criteria stated in this document. The applicant company must be accredited to [17025] and [CGOR] prior to submitting their proposal.

69. If this proposal is accepted by the CB, then the applicant company is granted a CLEF Provisional Appointment to undertake a trial evaluation.

The Preliminary Meeting

70. As soon as practical after the granting of a Provisional Appointment, the POC will make a preliminary visit to the applicant company to advise it in its preparation for assessment by the CB and by UKAS.

71. The meeting has the further intention of introducing the various members of the CB who will assist in the setting up of the CLEF and to answer any queries about the appointment and assessment process.

72. The meeting will be chaired by the POC. A typical agenda will include:

a) introductions;

b) an explanation of the set-up phase;

c) the relationship between the CB and UKAS;

d) discussion of the significance of the CLEF Quality Manual and the CLEF Security Manual;

e) a review of the proposed timetable for set-up, training, the trial evaluation, assessment and appointment;

f) information on requirements and services of the Scheme.

73. The POC will take no part in the UKAS assessment, but will be able to advise on the necessary preparations and requirements for evidence towards attaining a Full Appointment. The POC will be accompanied during the preliminary visit by other members of the CB, as required.

74. It is expected that further meetings will be held in order to review progress. These will normally be chaired by the POC.

Initial Training

75. The initial training programme outlined in Appendix B must be undertaken by the relevant personnel as soon as the POC is satisfied that the arrangements with regards to CLEF management, quality management, security and task confidentiality are sufficiently far advanced.

UKAS Accreditation

Categories of Accreditation

76. A CLEF will be assessed for two categories of UKAS Accreditation, namely:

- Permanent laboratory (the CLEF) where the testing facility is in a fixed location.
- On-site testing performed by CLEF staff sent out on site (e.g. Developer site) by the permanent laboratory (CLEF) that is accredited by UKAS.

77. A CLEF's accreditation covering both permanent and on-site work and the test activity accredited will be detailed in their UKAS Schedule of Accreditation.

78. On-site accreditation is a separate accreditation from permanent laboratory accreditation, which is generally granted before the former is awarded. It should be noted that this covers any evaluation work performed on-site (e.g. Development Site Visits) and not just testing.

Schedule of Accreditation

79. The evaluations performed by a CLEF, and the Evaluation Technical Reports they produce, are required to meet the standards of technical competence and quality which fall within the area of UKAS Accreditation. The scope of Accreditation is specified in a Schedule of Accreditation (the Schedule), submitted by the CLEF and prepared under guidance from the CB. This Schedule specifies the tests that a CLEF has been accredited to perform (e.g. assurance packages) and is limited to tests that meet UKAS requirements for objectivity, impartiality, repeatability and reproducibility. It provides traceability to supporting standards and procedures.

80. The scope of Accreditation includes not only the use of the evaluation criteria and methodology but also the CESG Generic Test Method described in [CGOR]. The CB manages and controls the set of (objective) tests for which CLEFs may be accredited by UKAS and the larger set of tests for which they are appointed. When appropriate, the CB will agree an extension to the Schedule with UKAS and will require new and existing CLEFs to seek Accreditation to the new Schedule.

81. It is not possible to accredit all tests performed by a CLEF, as some aspects of security testing are not completely objective. The interpretation of these subjective elements is subject to CB approval to ensure uniformity and correctness of evaluation procedures, and consistency and compatibility in the reporting of evaluation results.

82. In performing this role the CB may make an appointment to cover all the tests that a CLEF performs, including those not accredited by UKAS. The CB operates a "rolling" Appointment Programme, through which it controls and manages:

a) the set of tests for which a CLEF may be accredited by UKAS; and

b) the larger set of tests for which a CLEF may be appointed by the CB.

83. Accreditation by UKAS and these additional requirements together constitute appointment by the CB.

84. This Appointment Programme also provides a formal mechanism for change control to take account of the continuing development of the Scheme and its associated documentation: new or modified tests are first used under Provisional Appointment and then later under UKAS Accreditation, once the scope of a new Schedule has been agreed between the CB and UKAS. Consequently, as the evaluation criteria and methods are refined, the residual subjectivity of unaccredited tests will be reduced, allowing the CLEF to extend the scope of its existing Accreditation.

85. It is likely that such changes to the Schedule can be handled as part of extended surveillance or reassessment visits conducted by UKAS (see the *UKAS Surveillance and Reassessment* section in Chapter IV).

Application for UKAS Accreditation

86. A new CLEF must have formally completed UKAS assessment to [17025] and [CGOR] as a testing laboratory before the trial evaluation can commence.

87. UKAS will use the trial evaluation as the basis for the extension to scope to cover CC and therefore needs to be consulted at an early stage so that its formal assessment can be scheduled to take place at suitable points in the trial evaluation.

88. The CLEF must complete the required application forms available from the UKAS website http://www.ukas.com and forward them, together with a copy of the Quality Manual, Security Manual and the application fee, to the UKAS Applications Section. A copy of the CLEF Quality Manual and CLEF Security Manual must be sent to the CB once UKAS Accreditation is requested.

89. Throughout its lifetime, a CLEF will deal directly with UKAS on matters concerning its Accreditation. The CB will be able to advise on this aspect during the early stages, but will take no formal part in UKAS assessment leading to the award of Accreditation. The CB will, however, keep the results of UKAS Accreditation under review for appointment purposes.

Conduct of UKAS Assessments

90. The UKAS assessment and accreditation process is conducted as an independent activity in accordance with its standard procedures; they are described in detail in [LAB], which should be consulted for further information. The process is concerned only with the general procedures of the CLEF and makes no judgement on the product in evaluation at the time of the assessment.

91. UKAS assessments of CLEFs will be conducted by fully trained UKAS assessors, who will be tasked by UKAS specifically for the purpose and have appropriate security clearances and security knowledge. An assessor may be selected from the members of the CB but, if so, he/she will not be engaged on certification work related to any evaluation which was used for the purposes of the UKAS assessment. Also, the POC will not be involved in the assessment.

92. Both categories of accreditation are necessary for a full CLEF appointment and it is therefore necessary for this to be completed before the CB can make its final decision whether to grant the Full Appointment. In practice, the CB's appointment activities continue in parallel with the UKAS assessment, with the objective of reducing duplication of effort as far as possible.

93. Formal UKAS assessment is expected to take place during the latter stages of the trial evaluation; each category of Accreditation requires one or two days of assessment visits.

The Trial Evaluation

94. A new CLEF must carry out a trial evaluation in accordance with Appendix A.

95. It may be expected to last between 3 and 6 months and should end with reporting of the results to the CB. The POC will be responsible for liaising with the CLEF to carry out the trial evaluation.

Granting of a Full Appointment

96. A Certifier will be tasked with considering the Evaluation Technical Report from the trial evaluation in detail and whether the conduct and conclusions of the evaluation were in accordance with the rules of the Scheme and the relevant evaluation criteria and methodology. Assuming UKAS Accreditation is granted, a Full Appointment will only be given on the positive recommendation of the Certifier, the CB Technical Director and the Head of the CB. The Head of the CB will notify the CLEF of the outcome of the CB's decision and any conditions affecting the appointment.

Summary of the Application and Appointment Process

97. A checklist for use with the above procedures is provided in Appendix F.

IV. CLEF OPERATION

Introduction

98. This chapter defines rules which address the CLEF's day-to-day interaction with the CB, the conduct of evaluations and the further training of Evaluators, after the award of a Full Appointment.

99. Each CLEF should have a close working relationship with the CB to ensure that the interactive processes of evaluation and certification proceed smoothly. This relationship will be fostered by informal contacts with the CB, through the POC, through day-to-day work on evaluations and through membership of the CC UK Support Group (CCUKSG).

Interaction with the CB

General

100. It is necessary for the CB to be assured that the activities of any CLEF do not bring the Scheme, other CLEFs or the supporting HMG departments or agencies into disrepute. Consequently, the CB will maintain a close scrutiny of the conduct of the CLEF work, both technically and administratively, in order to safeguard task confidentiality and (where appropriate) compliance with the requirements of the UK Government Security Policy Framework [SPF].

General Liaison

101. The POC deals with non-task-specific queries and general CLEF matters.

Business Liaison

102. To facilitate CB resourcing, each CLEF should provide the CB with regular business reports (including prospective business). Such reports will be treated in the utmost confidence, ensuring fair and equitable dealings with each CLEF. The CLEF Progress Report (CPR) provides the CB with an overview of the CLEF's current and future business and the current status of the CLEF with respect to the Scheme. The CPR also enables the CLEF to formally raise any specific concerns with the CB. The requirements for this forum are specified below.

Advertisements and Publicity

103. It is a condition of the appointment that all proposed adverts and publicity statements intended to make mention of the Scheme or Scheme work, must be submitted to the CB Business Manager for prior approval. The CB Business Manager will give a response as soon as possible.

Evaluation and Certification

Booking Certification Services

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

105. 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 Programme 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 CB's service delivery manager assigned to the task.

Task Initiation

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

107. 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.

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

109. 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

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

111. For more details of the rules of independence, see the 'Constraints on Evaluations' section below.

Task Confidentiality

112. 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.

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

114. 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 (especially via email).

115. Task information must also be stored and handled in accordance with the CLEF's Security Manual (see 'The Security Manual' section in Chapter II) which is required to comply with the requirements for CLEF appointment.

116. 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 marked and protected.

Marking of Evaluation Outputs

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

118. 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.

Meetings

CLEF Progress Meetings (CPM)

119. The CLEF must keep the CB aware of all of the evaluation work in progress under the Scheme.

120. CLEF Progress Meetings (CPMs) will be held at a frequency and location mutually agreed between the CB and the CLEF. These meetings are to enable the CB to review progress of the CLEF on all Scheme issues, including technical issues relating to the current evaluations. They are attended by CLEF staff and representatives of the CB. The CLEF should submit the required softcopies of the CLEF Progress Report (CPR) to the CB at least ten working days before the meeting.

121. It is not the purpose of the CPM to resolve task specific points of detail; the appropriate forum for such discussions is the EPM or a specifically convened technical meeting for that task, between the appropriate members of the CB and the CLEF.

122. The primary input to the CPM is the CLEF Progress Report, which will form the basis for the agenda. An example CPM agenda is given in Appendix C.

123. Details of the format and contents of a CPR are given in Appendix C.

124. Attendees at the CPM should include, as a minimum:

a) from the CB:
   - Head of CB (Chairman);
   - CB Delivery Manager.

b) from the CLEF:
   - CLEF Controller;
   - CLEF Technical Manager;
   - CLEF Business Manager.

125. In addition, other members of the management of the CB and the CLEF may wish to attend.

126. The secretary for the CPM will normally be provided by the CLEF and will be responsible for producing the meeting minutes. The meeting minutes should be issued within fifteen working days of the meeting.

Evaluation Progress Meetings (EPM)

127. Evaluation Progress Meetings are called at the discretion of the Sponsor, CB or the CLEF, for the purpose of reviewing technical progress on a particular evaluation task. See UKSP 02 Part II [UKSP02-II] for more details.

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

Other Meetings

129. The Certifier may attend other meetings between the CLEF and a Sponsor for whom an evaluation contract is in progress, or is about to be let (i.e. signed), and should be given reasonable notice of such meetings wherever possible. The Certifier will not impose any unreasonable constraints upon the holding of such meetings. The Certifier will not be required to be present for financial aspects of such contracts.

CCUKSG Meetings

130. A CCUKSG meeting should be held approximately every 3-4 months, with the following attendees included as a minimum:

a) from the CB:
   - Scheme Technical Director;
   - Lead CC Certifier.

b) from each CLEF:
   - CLEF Technical Manager.

131. The meeting will discuss and agree UK Interpretations, and UK and international issues such as the following:

- CESG website, CPA, security characteristics;
- CC portal, CC/CEM, CCRA, ICCC;
- SOGIS, SOGIS portal, SOGIS-MRA;
- JIWG, NATO, JTEMS, CAS, OSeC, ISO;
- CCMC/ES/DB, CCMB, CCUF;
- ISCI-WG1, JHAS (was ISCI-WG2);
- International Technical Communities (iTCs), Collaborative PPs (cPPs) & Supporting Documents.

CLEF Controllers', Business Managers' and Technical Managers' Meetings

132. Meetings may also be held between the CB and CLEF Controllers, Business Managers, or Technical Managers to discuss administrative, promotional, strategic or technical issues.

133. All of the above mentioned meetings are in addition to those associated with UKAS assessment visits.

Constraints on Evaluations

Commercial Impartiality

134. An evaluation can only be said to be independent if it is possible to demonstrate to the CB that neither the CLEF, nor individual CLEF staff concerned with a particular evaluation, has a vested interest in the outcome of the evaluation.

135. The work performed by the Evaluators must be independent of the development of the TOE. Evaluators must always be free from any commercial, financial and other pressures which might influence their technical judgement.

136. A CLEF may not thus evaluate the development work of any group or division within the parent company to which it belongs, or any associate partner who is a TOE developer. This rule may be relaxed at the discretion of the CB, provided the CLEF can satisfactorily demonstrate that the independence of the evaluation can be maintained and that the credibility of the Scheme will not be damaged. The CLEF must submit a written application in each case. Examples where this rule has been relaxed in the past have been confined to HMG systems and more rarely to specialised products for use in HMG systems.

137. In no circumstances, therefore, may the same CLEF team or individual be involved in:

a) both the development of the TOE and the conduct of its evaluation; *or*

b) the provision of consultancy advice to the Sponsor or Developer which would in any way compromise the independence of the evaluation.

138. CLEF staff may not engage in any evaluation activities on which they have previously acted as consultants, unless the CLEF can demonstrate to the CB that the independence of the evaluation will not be compromised. CLEF Staff cannot advise Sponsors or Developers how to resolve problems, but they can comment on the adequacy of a proposed response or suggest possible options for consideration.

139. CLEF staff may provide consultancy on a TOE on which they have previously worked as Evaluators provided that the CLEF can demonstrate that the evaluation or any assurance maintenance activity will not be compromised (e.g. by knowledge of the sampling strategy). CLEF staff cannot guarantee the completion date of an evaluation or the issue date for certification.

140. The CLEF must notify the CB of any change to the role of CLEF staff with respect to an evaluation.

141. Notwithstanding the various statements on Evaluator independence in the evaluation criteria and methodology, the CLEF evaluation team may produce the security target, low-level (detailed) design and vulnerability analysis deliverables as part of the evaluation process for systems which are for UK use only and not subject to any mutual recognition process. This relaxation is permissible where it will help Evaluator understanding of the TOE. This relaxation may also be made for specialised products for use in HMG systems; however the agreement of the CB must first be obtained. For example, agreement will not usually be given where such a product has a commercial variant that may make re-use of the evaluation results.

142. Evaluation teams and individual Evaluators should not have the same immediate manager as the consultancy or development teams. (Note that development is applicable only in the context permitted by paragraph 136.) Independence will be questioned if it is apparent that a manager may be able to influence decisions between development and consultancy on the one hand and evaluation on the other. CLEF staff involved in the technical management of a TOE's evaluation must not be involved in its development. However, CLEF managers dealing with contractual issues may be common to a development team and an evaluation team provided that they have no influence on the conduct of the evaluation (e.g. in terms of allocating effort budgets or providing technical advice).

143. These independence requirements are summarised in the following Figure, where "✓" indicates "is permitted", "×" indicates "is not permitted" and "–" indicates "is not applicable".

	CLEF Staff Role		
CLEF Activities	Evaluator	Developer	Consultant
Evaluation or Re-evaluation	✓	×	×
TOE Development	×	✓	✓
Consultancy	(Para 139)	✓	✓
Production of security target, design and vulnerability analysis deliverables (for UK systems only)	(Para 141)	✓	✓
Activities in respect of TOE developed by group or division within CLEF's parent company	(Para 136)	✓	✓
CLEF management – same immediate technical management for development/consultancy and evaluation	–	–	–

144. These rules may be relaxed at the discretion of the CB, provided the CLEF can satisfactorily demonstrate that the independence of the evaluation can be maintained and that the credibility of the Scheme will not be damaged. A written application from the CLEF is required in each such case.

Supply of Documentation to the CB

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

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

147. Related security aspects of such deliveries are detailed in paragraph 22.

Sanitisation of Evaluation outputs

148. The CLEF must ensure that evaluation output is appropriately sanitised before it is sent to the Sponsor/Developer.

149. As a result of confidentiality requirements of the CLEF and Developer, some evaluation output (e.g. the EWP and the ETR) may need to withhold the following:

a) information proprietary to the Developer (e.g. source code);

b) TOE specific sampling information and test information;

c) effort estimates and/or actuals for the evaluation;

d) commercially sensitive information.

150. To avoid the need for additional work in sanitising an ETR before releasing it to the Sponsor, it is recommended that the Evaluators partition the report in such a way that information which should not be released to the Sponsor, or another CLEF, is contained in either a separate volume, or, more usually, separate annex(es).

151. The non-proprietary parts of the ETR will be released to the Sponsor and CB, whereas any CLEF- or Developer-proprietary annexes will only be released to the CB and marked with the appropriate protective marking to indicate the ownership of the material contained therein.

Evaluator Teams

152. At any given time, the ratio of Trainee Evaluators to Qualified Evaluators (or Specialist Evaluators if appropriate) on any evaluation should not exceed **3:1**.

153. In exceptional circumstances this rule may be relaxed at the discretion of the CB, who may then require additional safeguards to ensure that the following Scheme rules are upheld:

a) the proportion of Trainee Evaluators should not be such as to have an adverse effect on the technical quality of the work;

b) Trainee Evaluators receive sufficient supervision so as to ensure the correct performance of their duties.

154. Evaluations at the Common Criteria EAL4 Assurance Level and higher must have an experienced Qualified or Specialist Evaluator in the team, who should play a significant and active role, preferably as Task Leader.

155. The role of the experienced Qualified or Specialist Evaluator in such evaluations will be considered sufficiently significant and active if it provides confidence in the overall technical quality of evaluation work throughout the evaluation. The Evaluator will be considered sufficiently experienced if he/she has played a significant role in evaluation tasks whilst holding Qualified Evaluator or Specialist Evaluator status (as agreed with the CB). In particular, evaluations at CC EAL7 must have a formal methods expert in the team.

156. However, the CLEF may recommend a Qualified Evaluator or Specialist Evaluator on the basis of other experience, such as involvement in security evaluations performed to other criteria and schemes, development, research or publications. The CLEF must demonstrate to the CB that the proposed Evaluator will play a sufficiently significant and active role in the evaluation and has sufficient experience to ensure the necessary technical quality of evaluation work at the required assurance level or assurance package. In particular, evaluations that require knowledge of a specialist security field must include an appropriate Specialist Evaluator.

157. For enhancing and improving the Penetration Testing activity during an evaluation, the CLEF must justify to the CB whether or not to include in the evaluation team appropriate specialist penetration testers to conduct specific penetration tests. (The justification must be recorded, e.g. in the EWP or in the TSM minutes, for audit purposes.) Such specialists, who must be suitably recognised (see sections 158-159) by the UK National Technical Authority (NTA) for Information Assurance, CESG, are permitted to be part of the CLEF's parent company. Their tests should be conducted in close collaboration with the Evaluation Task Leader, who has the responsibility to ensure that the efforts of the evaluation team, including any specialist penetration testers, are appropriately coordinated and integrated. In particular, any specialist penetration testers should be provided with detailed information about the Evaluated Configuration and IT security environment so that their testing resources are effectively focused and utilised. Specialist penetration testers should also be provided with details defining the specific scope of their tests and this information may be provided in a scoping meeting. The test

results, together with details of the specialist network and vulnerability tools and techniques used by the specialist penetration testers, should be clearly documented in the ETR or in a referenced Penetration Test Report. It is accepted that certain products may not be suitable for testing by specialist penetration testers. Additional advice and recommendations can be provided to the CLEF by request to the CB.

Specialist Penetration Tester Qualifications

158. For assurance levels of EAL3 and higher, any specialist penetration tester included in the evaluation team must be recognised by CESG as holding a current qualification for either a CHECK Team Leader or a CHECK Team Member as appropriate to the evaluation task. For assurance levels of EAL5 and higher, a current qualification of CHECK Team Leader is mandatory for such specialist testers.

159. For assurance levels of EAL2 and lower, the CLEF may propose to the CB the use of specialist penetration testers who hold a current relevant award from a commercial penetration testing qualification body (e.g. Tiger or Crest). The acceptance of such a proposal is at the discretion of the CB.

160. The CLEF must ensure that any specialist penetration tester has sufficient security clearance, in relation to the protective markings of the TOE and its documentation, to be able to perform Penetration Testing for the evaluation.

CLEF Staff Changes

161. The CB should be notified of all CLEF staff changes via the CLEF Progress Report (see Appendix C). The list of CLEF staff should highlight which staff have joined since the last CLEF Progress Meeting and the date of joining. A list of staff who have left the CLEF, together with dates, should also be included.

New Entrants

162. All evaluation staff who have not previously worked for a CLEF should be notified to the CB prior to assignment to an evaluation. Notification can be given by letter to the Head of CB or at a CLEF Progress Meeting if such a meeting is imminent.

Staff Rejoining the CLEF

163. If the new member of CLEF staff has previous evaluation experience, but currently has no Evaluator status, application may be made to the CB for the (re)award of a status together with a rationale and evidence for the requested status, based on work in the IA field. See the section on *Maintenance of Evaluator Status* in Appendix B.

UKAS Surveillance and Reassessment

164. UKAS assessors will carry out surveillance visits to the CLEF as specified in [LAB]. The first surveillance visit is normally carried out six months after the date of Accreditation. Subsequent surveillance visits are carried out at yearly intervals. A full reassessment will take place three and a half years after the date of Accreditation and thereafter at four-yearly intervals. Reassessments are similar to initial assessments except that the CLEF's current evaluations replace the need for a trial evaluation.

165. Surveillance visits will normally be undertaken by one or two assessors and each category of Accreditation will be completed within one or two days. Surveillance assesses the CLEF in its conduct of actual evaluations rather than a trial evaluation. Normally assessors will not be expected to check either all the evaluations which are in progress at

the time or the whole of any one evaluation; rather, several surveillance visits are performed over a period of time in order to check all aspects of evaluation.

166. A reassessment visit will provide the opportunity for a more comprehensive examination of a CLEF's performance.

167. Surveillance and reassessment visits for accreditation of the permanent laboratory may be carried out on different days from those for the accreditation of on-site work, which will involve the assessors accompanying the Evaluators to witness an activity on-site.

168. Extensions to the scope of the Accreditation Schedule are normally catered for during extended surveillance and reassessment visits. Such extensions are required to update the Accreditation of an existing CLEF, following prior agreement between the CB and UKAS on the scope of the extended Schedule.

169. In order to demonstrate its ability to perform evaluations against an extended Schedule, a CLEF will need a period of time to apply the new activities or methodology and procedures to real evaluations. When it is ready for assessment, the CLEF must either make arrangements with UKAS to take any extended Schedule into account during the next surveillance or reassessment visit, or make arrangements for a special visit, as required. If successful, the CLEF will receive a corresponding extension to the scope of its Accreditation. A CLEF may not claim Accreditation for these new activities without the prior approval of UKAS.

CB Surveillance and Reassessment

170. Independently of UKAS, the CB will also carry out surveillance through its day-to-day involvement in the certification of evaluations and will formally review conditions of appointment following each UKAS surveillance or reassessment.

Termination of Appointment

171. The CB reserves the right at short notice to withdraw the CLEF's appointment if the UKAS Accreditation lapses, or if the CLEF is found to be in serious breach of the conditions of appointment. The appointment will be reviewed automatically if the CLEF's parent company is taken over. This is to ensure that the CLEF's quality management system does not suffer as a result of such a change and that the CLEF continues to comply (where appropriate) with the provisions of the HMG Security Policy Framework [SPF]. There will also be an assessment of the impact of the takeover (or merger) with respect to client information confidentiality or other contractual conflicts.

172. Normally, the CB provides at least three months notice of withdrawal, non-renewal or intention to vary the terms of the appointment and expects the same notice of a CLEF's intention to withdraw from the Scheme.

173. At the termination of a CLEF appointment, the CB will determine whether any ongoing evaluation work under the Scheme will be allowed to continue in order for the CLEF to fulfil its contractual obligations to its Sponsors. Such work will have the support of the CB. Evaluations will not be allowed to continue if to do so would bring the Scheme into disrepute or would be against the interests of the Sponsor.

174. The CB also reserves the right to withdraw *all* CLEF appointments if the Scheme is to be terminated, on six months notice.

Disputes

175. In the event of a dispute between the CLEF and the CB, the CLEF or its parent company has the right of appeal.

176. In the first instance the CLEF should strive to resolve the matter directly with the CB via the Head of the CB. However, if the CLEF, or its parent company, considers this course of action ineffective, it may lodge an appeal with the Scheme Senior Executive.

Appendix A
TRIAL EVALUATION

Purpose

A.1. The purpose of the trial evaluation is to demonstrate to the CB that a CLEF is competent to perform IT security evaluations. It is also used as the basis for the UKAS assessment and must cover both permanent laboratory work and on-site work.

Objectives

A.2. The trial evaluation is designed to demonstrate that:

a) the individual Evaluators are technically competent;

b) the management and administration of the CLEF is competent to fulfil its role in supporting an evaluation.

A.3. The trial evaluation covers all the areas associated with the on-the-job training of Trainee Evaluators in a newly established CLEF (see Appendix B). The trial evaluation also provides an opportunity for CLEF staff to demonstrate that they are conversant with all aspects of the organisation and management of an evaluation task and that they can deal with the other organisations that are involved in the evaluation process.

Conduct

A.4. The precise details and subject of the trial evaluation will be determined in accordance with the above mentioned objectives and the assessment criteria given below. Wherever possible a real system or product will be used.

A.5. The CLEF may suggest a particular product or system which, with the approval of the CB, may then become the subject of the trial evaluation. It is the responsibility of the CLEF to find this work. However, to satisfy the requirements for on-site accreditation it is essential that the evaluation has an element of on-site work.

A.6. It is intended that a typical trial evaluation will involve a minimum of 3-4 (Trainee) Evaluators and will last for no more than 3-4 months. The objective of the trial evaluation is primarily to “assess” the Evaluators, not the TOE. However, since the evaluation must be completed in order that an assessment of all aspects of the work may be made, it can be expected that certification of the TOE should follow, assuming the satisfactory conduct and outcome of the evaluation task.

A.7. The aspects to be evaluated, and to what depth, will be determined by the CB. The scope of the evaluation will however need to cover all the tests specified in the Schedule (see paragraph 79).

A.8. The duration of the trial evaluation will depend on progress made. It may be necessary to extend it beyond the expected time to provide the CB with additional evidence as to the competence of the Evaluators.

A.9. The trial evaluation will be performed under CLEF management but under the technical guidance of the CB. In its early stages it should be regarded as a practical application of the classroom theory and will be conducted under the close supervision of

the CB's POC who will be permitted to lead by example. As it proceeds, the CLEF will be expected to require significantly less supervision.

A.10. Satisfactory progress and the need for minimal supervision will be taken as an indication of the CLEF's readiness for formal UKAS assessment. The CB's POC will not perform this assessment.

A.11. Independently of UKAS, the CB also assesses the CLEF, paying particular attention to any aspects not covered by the UKAS assessment. A Certifier (usually the POC) will be appointed to monitor the trial evaluation and produce a Certification Report based on a draft provided by the CLEF.

Assessment

A.12. During the trial evaluation the CB will pay particular attention to the following areas:

a) the planning of the evaluation, including production of the EWP (including the Test Plan);

b) the conduct of the evaluation to ensure conformance with the approved UK evaluation technical approach and the extent to which the test methods employed meet the requirements of objectivity, repeatability, reproducibility and impartiality;

c) the reporting of the evaluation, both in terms of its quality and its level of detail;

d) liaison with other organisations, the conduct of meetings and the observation of procedures and protocols relating to such contact;

e) procedures to ensure that task confidentiality is observed.

A.13. While some of these areas will be covered by UKAS assessment, the CB will avoid duplication of effort as far as possible.

A.14. Also during the trial evaluation, the Trainee Evaluators will be assessed via their normal day-to-day contact with the CB's POC to determine whether or not they have demonstrated sufficient competence to be regarded by the CB as Qualified Evaluators[6]. It is a requirement of the granting of the Full Appointment that there should be at least one Qualified Evaluator within the CLEF. It should be noted, however, that the granting of Qualified Evaluator status does not follow automatically from successful completion of the trial evaluation; the CB will require on-the-job training of some Trainee Evaluators before deeming them qualified.

A.15. The UKAS assessment takes place during the latter stages of the trial evaluation but before the evaluation has been completed. The assessors will accompany Evaluators during a site visit so that they can observe that aspect of the work.

Completion

A.16. The evaluation team is required to complete the trial evaluation and produce examples of evaluation outputs for consideration by the CB. Provided that the CLEF has met all other criteria to the satisfaction of the CB, including the granting of Accreditation by

[6] The Specialist Evaluator qualification is not relevant to a Trial Evaluation.

UKAS and reports from the CB's POC and Certifier, these documents represent the final test of the CLEF's capabilities prior to the granting of a Full Appointment.

Appendix B
TRAINING

Evaluator Training Course

Objectives

B.1 The objectives of the Evaluator training course are:

a) to familiarise students with basic security principles, the Scheme and the evaluation criteria and methodology;

b) to introduce the practices of the UK technical approach to evaluation, based on the evaluation methodology approved for use under the Scheme;

c) to describe the procedures to be adopted when conducting evaluations under the Scheme and to describe the underlying principles and activities such as planning, organisation and management of evaluation tasks;

d) to introduce the organisations which are involved in the Sponsorship, Evaluation, Certification and System Accreditation process and to provide the background information needed to ensure efficient and successful evaluation.

Course Structure

B.2 The course is broken down into the following three modules:

M1 – Evaluation Overview

M2 – Assurance

M3 – Scheme Rules and Procedures

B.3 The above modules comprise the UK Evaluator Training Material[7] which is available at the CESG website http://www.cesg.gov.uk. CLEFs may choose the method of presentation of the material, which may be done in formal classroom environments or informal sessions on an ad-hoc basis. The material covered should follow the syllabus below.

Syllabus

B.4 This outline indicates the general areas to be addressed in order to meet the objectives set out above.

M1 – EVALUATION OVERVIEW

B.5 This module provides a background to IT security concepts and evaluation and introduces both assurance and scheme rules and procedures.

B.6 M1 should normally be given before any other module.

[7] The training material relates to CC version 2.1. Trainers will need to reflect current practice.

M2 - ASSURANCE

B.7 This module comprises nine modules, including an introductory module (M2.0) that relates the various assurance aspects covered by the remaining modules. These modules are:

M2.1 – Security Requirements

M2.2 – Development Representations

M2.3 – Functional Testing

M2.4 – Development Environment

M2.5 – Operational Environment

M2.6 – Vulnerability Analysis

M2.7 – Penetration Testing

M2.8 – Assurance Maintenance and Composition

M3 – SCHEME RULES AND PROCEDURES

B.8 M3 comprises two modules, intended to reinforce and supplement the awareness of Scheme rules and procedures from module M1 and the OJT element of the training programme (see below):

M3.1 – Evaluation Process

M3.2 – Evaluation Management

B.9 Module M3.1 covers the roles and responsibilities of interested parties. It also describes the inputs, activities and outputs associated with each evaluation process phase. M3.2 revisits the evaluation process from a task management perspective.

Maintenance of Course Material

B.10 With the passage of time and changes to the Scheme, the training material inevitably becomes out of date. The mechanism for ensuring that the courses reflect current practice depends on cooperation between the CB and the CLEFs.

B.11 Clarifications to the Methodology are promulgated by means of Interpretations. The CLEF trainers are expected to be aware of these clarifications and must point these out to students during their presentation of the course modules. Periodically, the CB will carry out a review of the training material in which the effects of all Interpretations and SINs[8] will be considered.

B.12 Despite the best endeavours of the reviewer(s) there may still be some inconsistencies or inaccuracies in the training material. Should an inconsistency or inaccuracy be noticed, other than that which is the subject of a recent or impending SIN, then an email should be sent to the CB indicating the precise nature of the problem. If the error is seriously misleading then a correction will be issued by the CB; however if the problem is minor then corrective action will be taken during the review and update exercise referred to above.

[8] SINs that are published on the CESG website have status Open (currently SIN 092). All other SINs are obsolete and therefore have status Closed.

Conduct

B.13 CLEFs may develop their own training programmes. However these must be approved by the CB and include at least the same material as provided in the current M1-M3 kernel available from the CB.

B.14 Normally, CLEFs will only present training material to their own staff. There is, however, no objection to staff of other CLEFs and/or the CB attending a formal course run by any CLEF, subject to the agreement of the presenting CLEF.

Charges

B.15 Where a CLEF presents a course to staff of other CLEFs, it may make an appropriate charge for its services.

On-The-Job Training of Trainee Evaluators

Introduction

B.16 On-the-job training is the primary means by which Evaluators acquire their skills.

B.17 Following completion of an initial training programme, Trainee Evaluators undergo on-the-job training on real evaluations under the direction of Qualified Evaluators (or Specialist Evaluators, if appropriate). They need to be given experience of all relevant aspects of evaluation before they can be recommended to the CB for consideration as Qualified Evaluators or Specialist Evaluators. Their work on these evaluations will be offered in support of such a recommendation.

Scope of Training

B.18 There is no specific number of evaluations or a specific time period required as a prerequisite to becoming a Qualified or Specialist Evaluator. Trainee Evaluators are required to demonstrate competence in all relevant aspects of evaluation. They should, therefore, be given sufficient opportunity to allow them to gain experience and to demonstrate their competence.

B.19 In particular, it is expected that when a Trainee Evaluator is recommended for Qualified Evaluator status he/she will:

a) be able to demonstrate understanding of the Common Criteria by their application in a real evaluation;

b) have experience that includes performance of all Evaluator actions required for a Common Criteria evaluation:

c) be able to demonstrate an understanding of the UKAS aspects of the evaluation process, the CLEF Quality Manual and the CLEF Security Manual;

d) demonstrate that he/she is able to document the evaluation results of his/her work objectively, precisely, unambiguously and at the level of detail required by the CB, Scheme and Methodology.

B.20 A Trainee Evaluator intending to become a Specialist Evaluator will have items a), c) and d) above and the relevant subsets of item b). A Trainee Evaluator may need to work on more than one evaluation in order to gain the required experience.

Assessment

B.21 Assessment will be performed by the CB:

a) following a positive recommendation by the CLEF management; and

b) by consideration of written reports produced by the Trainee Evaluator as part of his/her on-the-job training.

B.22 In addition, the CB may subject the Trainee Evaluator to an oral examination and may monitor his/her progress as necessary in order to determine his/her fitness to be a Qualified Evaluator or a Specialist Evaluator.

Written Reports

B.23 The CLEF must identify written Work Package Reports which are clearly produced by the Trainee Evaluator and peer reviewed by a Qualified Evaluator. These reports should demonstrate the Trainee Evaluator's understanding of the relevant evaluation criteria, methodology and Scheme documents and that he/she is able to apply them in practice. The reports should cover practical experience of all aspects of the evaluation process as identified in paragraph B.19 above.

B.24 Written reports should normally be part of the Evaluation Technical Report though, if necessary, the CB *may* be prepared to consider reports written specifically for the purpose of Trainee Evaluator assessment. In this case there must be clear indication that the Trainee Evaluator understands how the work that he/she has described fits into the overall work of the evaluation.

Maintenance of Evaluator Status

B.25 The CLEF holds a list of all Evaluators of any status (Trainee, Qualified and Specialist). It should be noted, however, that the status of any Evaluator is only recognised by the CB within the context of the Scheme; Evaluators must not therefore claim CB endorsement of their qualification to perform work outside the Scheme.

B.26 The status of an Evaluator is to be maintained by continuing practice as an Evaluator. Such status is only relevant for the performance of evaluation duties. If an Evaluator is temporarily moved within the parent company to do non-CLEF work he/she may retain his/her status as a Qualified Evaluator or Specialist Evaluator if he/she returns to evaluation duties within a period of twelve months. Thereafter the CLEF is required to make a case for the reinstatement of the individual Evaluator. Such reinstatement is at the discretion of the CB and will take into account the candidate's length of service as an Evaluator and the period of absence from evaluation work. It should also take into account any IT security or evaluation consultancy that may have been part of the candidate's work in the intervening period of absence. If regaining of status is not granted then he/she will be required to re-attend part or all of the training described above.

B.27 If an Evaluator transfers to another CLEF, he/she does not automatically retain his/her status and the new CLEF has to make a case for the status of the Evaluator. The status granted shall be at the discretion of the CB.

Technical Competence of Evaluators

B.28 In addition to the requirement to maintain evidence to support Evaluator status, the CLEF should also maintain evidence of ongoing technical competence of Evaluators, sufficient to support UKAS Accreditation.

B.29 Evaluators should undertake personal development training appropriate to their skills or specialisms enabling them to keep abreast of technology changes appropriate to their scope of activities. CLEF procedures for identifying training needs and providing Evaluator training should be relevant to current and anticipated tasks. The procedures should also provide a method for assessing the effectiveness of the received training.

B.30 The CLEF should ensure that the effectiveness of Evaluator training is appropriately assessed in accordance with such procedures and that appropriate evidence of such assessments is also maintained.

Appendix C
CLEF PROGRESS REPORTS AND MEETINGS

CLEF Progress Meeting

Agenda

C.1. The objective of a CPM is to discuss issues relating to the CLEF business and the operation of the Scheme and to review progress and problems on current tasks. An example CPM agenda is shown in Figure C.1.

A. Chairman's Introduction
B. Agree The Agenda
C. Minutes Of Last Meeting
D. Actions Arising
E. Contract Extensions
F. CLEF Progress Report
   - Task Overview
   - Marketing Issues
   - Staffing Issues
   - Appointment Issues
   - General Scheme Issues
   - Administration Issues
   - General Technical Issues
   - Task Status Reports
G. Any Other Business
   - Common Criteria Concerns
   - Legacy Scheme Status
   - CLEF View On The Strategic Future of CC
H. Action Summary
I. Date of Next Meeting

(This should be updated, for each meeting, with current business topics.)

Figure C.1 – CLEF Progress Meeting - Example Agenda

C.2. The major agenda items are discussed in the following sub-sections.

Item F – Task Overview

C.3. The following topics should be reviewed:

a) the general workload;

b) any tasking items that are not task specific;

c) any other work being performed in the CLEF that may impact upon the current workload.

Item J – Marketing Issues

C.4. The future prospects should be reviewed insofar as they impact upon the CB, subject to commercial concerns.

Item K – Staffing Issues

C.5. This item should review changes in the CLEF staffing, changes in Evaluator status and specific staff related issues such as training.

Item L – Appointment Issues

C.6. This item should review current and future appointment and accreditation status and allow attendees to raise any appointment related matters.

Item M – General Scheme Issues

C.7. This item should allow attendees to raise any other Scheme related matters e.g. status of SINs and interpretations.

Item N – Administration Issues

C.8. Any organisational matters related to the CLEF should be raised under this item.

Item O – General Technical Issues

C.9. Any general technical issues (criteria or methodology) which are relevant across different tasks should be raised. The status of known and potential vulnerabilities should be discussed, together with proposals for risk management.

Item P – Task Status Reports

C.10. Task Status Reports should be considered where there are issues for the CPM attendees to discuss.

Item Q – CLEF Progress Report

C.11. See next section for full details.

CLEF Progress Report

Overview

C.12. The objective of the CPR is to provide the CB with an overview of the CLEF's current business and status with respect to the Scheme and to permit the CLEF to raise formally any specific issues with the CB, for discussion at the next CPM.

Structure

C.13. The structure of a CPR should be as follows:

a) Title page, including reference, issue, date, distribution and copyright.

b) Contents page.

c) Introduction.

d) Task Overview, listing all the current tasks within the CLEF and their current status (e.g. active, inactive, cancelled, reported[9] and complete). Timescales should show the start date, initial planned ETR date and current best estimate of ETR date. Outstanding Certification commitments and timescales should be highlighted. In addition, brief details of any work being undertaken in the CLEF which might impact upon evaluation tasks should be covered.

e) Marketing Issues. Specific references to business prospects are desirable, but if not possible for commercial reasons, some notice of the scale of future inputs to the CB is required.

f) Staffing Issues, listing the CLEF's current staff, with their roles and status under the Scheme (including an indication of staff trainers). The list should also highlight any change of role, status, additions/deletions since the previous CPR, with dates of joining/leaving the CLEF.

g) Appointment Issues, stating the current appointment and accreditation status of the CLEF and highlighting any changes to these since the previous CPR. The issue number and date of the current UKAS Accreditation Schedule should be included, as should the date of the previous and next UKAS Accreditation visits.

h) General Scheme Issues, enabling the CLEF to raise any other issues pertaining to the Scheme.

i) Administration Issues, covering any general administration matters.

j) General Technical Issues, covering any technical issues of a general nature. This should include a list of any TOE-specific interpretations raised by the CLEF in the period.

k) Task Status Reports (TSRs), giving further details for specific tasks, may be included as separate annexes.

Task Status Reports

C.14. TSRs need only be included where there are specific issues for the CPM to discuss. In such cases a TSR need only give the information that is needed to understand the issues.

C.15. Issues warranting TSRs include:

a) Changes to anticipated evaluation timescales (since the previous CPR or EWP) unless already known to the CB.

b) Problems encountered in accommodating the evaluation requirements of the Sponsor (or Developer).

c) TOE-specific interpretations of evaluation criteria which might usefully be circulated within the Scheme.

[9] The status "reported" indicates that an ETR has been issued to the CB.

Protective Markings

C.16. The main body of the CPR and any annexes (i.e. each TSR) should bear its own appropriate protective marking.

Appendix D
ASSESSMENT AND OTHER FEES

Introduction

D.1 Since 1 April 1997 the CB has been required to recover its costs. The paragraphs below indicate areas where fees are raised. Fees will not be refundable.

Fee for Help with Setting Up a New CLEF

D.2 A fee is payable to the CB on the granting of a Provisional Appointment to cover the cost of CB advice and training of the CLEF staff prior to the trial evaluation.

D.3 There is a further fee which covers the services of the CB during the trial evaluation. The fee would be charged irrespective of whether the applicant company is successful in obtaining a Full Appointment or not.

Annual Fees

D.4 The CB reserves the right to levy an annual subscription fee on the initial granting of a Full Appointment and on each anniversary of that occasion. The fee would amongst other things cover all documentation updates.

Certification Fees

D.5 A fee for CB certification services will normally be levied directly on the Sponsor for each evaluation (or re-evaluation) and on the Sponsor for any assurance maintenance activity.

UKAS Fees

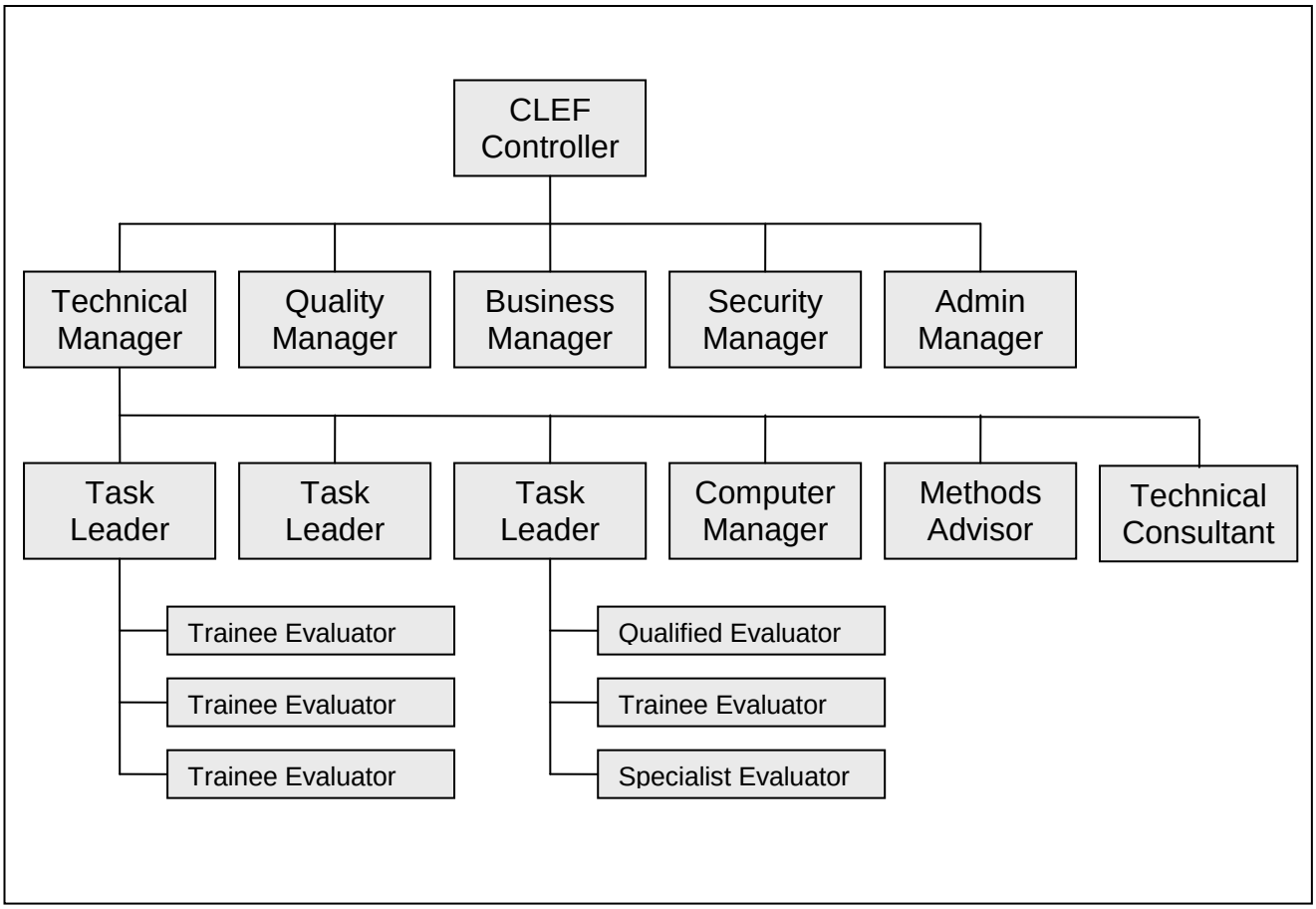
D.6 UKAS charges a fee for its Accreditation services, details of which are available from the UKAS Executive.

Training Fees

D.7 Training courses which are approved by the CB may be run on a commercial basis. Any fees are the subject of negotiation between the relevant parties.

Appendix E
SUGGESTED CLEF STRUCTURE

E.1 The following diagram illustrates the organisational structure described in Chapter II.



Terms of Reference

E.2 Whilst the precise terms of reference for each of the above roles is a matter for the CLEFs, the following notes indicate the general areas of responsibility involved.

CLEF Controller

E.3 The CLEF Controller has overall management responsibility for the operation of the CLEF, ensuring that both Scheme and UKAS requirements are met.

Technical Manager

E.4 The Technical Manager is responsible for the provision of evaluation technical advice and guidance and for liaison with the CB on matters concerning the criteria and evaluation methodology.

Quality Manager

E.5 The Quality Manager ensures that the procedures detailed in the CLEF Quality Manual are followed and is responsible for taking any remedial action that may be required as a result of either internal audits or UKAS (re)assessment/surveillance visits.

Business Manager

E.6 The Business Manager is responsible for pre-contract and tender negotiations with potential clients and for liaison with the CB on administrative issues connected with potential or current evaluation tasks.

Security Manager

E.7 The Security Manager is responsible for the physical, personnel, procedural, and information security aspects of CLEF operation. This post liaises with the Government Departments responsible for overseeing compliance with the HMG Security Policy Framework [SPF]. Any CLEF Security Guards report to the Security Manager who is responsible for logging, reporting, escalating and resolving all security incidents and breaches.

Administration Manager

E.8 The Administration Manager is concerned with provision of administrative support to the CLEF. All clerical staff, such as receptionists and telephonists (where these services are not provided by the parent company) report to this Manager.

Computer Manager

E.9 The Computer Manager is responsible for all aspects of CLEF computing, including operation and security of any internal computers or systems. The post may also be involved in configuring and operating any computer equipment housed in the CLEF as part of an evaluation task.

Methods Advisor

E.10 The Methods Advisor promulgates advice and guidance on the use of the evaluation methodology and its interpretations within the CLEF. This post will liaise with the CB on methodology aspects of the CLEF's operations as required by the Technical Manager.

Technical Consultant

E.11 The Technical Consultant provides specialist advice to evaluators on specific TOE types.

Task Leaders

E.12 Evaluation Task Leaders are responsible for the correct conduct of the evaluations that they lead, ensuring compliance with the evaluation methodology and current CB guidance. They should ensure that their team members (consisting of Trainee, Qualified

or Specialist Evaluators) are adequately trained for the work involved. They are responsible for all reports produced as a result of the evaluation.

Evaluators

E.13 Covered by the constraints on “The Conduct of Evaluations” in Chapter IV.

Appendix F
CHECKLIST FOR CLEF START UP

F.1 The following may be used as a checklist during an application for a CLEF Appointment and until a Full Appointment has been awarded.

Meeting Basic Requirements

F.2 Is the CLEF an autonomous unit within the Company?

F.3 What is the Company's management structure?

F.4 Has it sufficient furniture and fitments, etc. to operate?

F.5 Has it its own administrative and clerical support?

F.6 Have full contact details (including telephone, email, fax and postal address) been made available for all CLEF POCs?

F.7 Has it sufficient infrastructure to support evaluation tasks?

(If appropriate:)

F.8 Are the requirements of the HMG Security Policy Framework [SPF] met?

F.9 When was its security status granted?

F.10 When was it last reviewed?

F.11 Does the company have an existing accreditation to [17025] and [CGOR]?

Quality Manual

F.12 Is there a Quality Manual?

F.13 Does it conform to UKAS requirements?

F.14 Has it been reviewed by UKAS? If so, when, and with what result?

Management Roles

F.15 Who is the CLEF Controller?

F.16 Who is the Technical Manager?

F.17 Who is the Quality Manager?

F.18 Who is the Business Manager?

F.19 Who is the Administration Manager?

F.20 Who is the Security Manager?

F.21 Is there a Computer Manager?

F.22 Is there a Methods Adviser?

F.23 Is there a Technical Consultant?

F.24 Does any individual undertake more than one role? If so, is there any possibility that the effective performance of these roles could suffer as a result?

Security and Confidentiality

F.25 Who has overall responsibility for the security of the CLEF and production of the Security Manual?

F.26 Does the Security Manual adequately cover the areas of concern laid down in UKSP 02 Part I?

F.27 Are CLEF staff adequately cleared? To what level?

F.28 What facilities exist for secure storage of media and documents?

F.29 What are the arrangements for maintaining task confidentiality?

F.30 How are CLEF computing facilities separated from those of the parent company?

F.31 Have the responsibilities and procedures for reporting and managing security incidents and breaches been established?

F.32 Is there adequate experience of management and resolution of security incidents and breaches that have occurred?

Evaluator Status and Training

F.33 What is the Evaluator status of CLEF staff?

F.34 What Initial Training is required and how will it be arranged?

Provisional Appointment

F.35 Has a formal application been made for a Provisional Appointment?

F.36 Has a proposal been submitted to the CB detailing how the applicant company plans to set up and manage the CLEF?

Preliminary Meeting

F.37 Has the Preliminary Meeting been held?

Initial Training

F.38 What Initial Training has been arranged? Who will give it and when? What will be covered?

UKAS Accreditation

F.39 Has formal application been made to UKAS for Accreditation as a CC testing laboratory?

F.40 Have copies of the CLEF Quality and Security Manuals been sent to the CB?

Trial Evaluation

F.41 Has a TOE been identified for use in the trial evaluation?

F.42 Has this been agreed by the CB?

F.43 How far has the trial evaluation progressed?

Appendix G
SUMMARY OF MANDATORY REQUIREMENTS ON CLEFS

G.1 This Appendix contains a summary of CLEF Requirements, in the context of their start-up and operation, as required by the Scheme and/or UKAS. The main body of this document marks these with shaded text boxes.

Para	CLEF Requirement	Scheme/ UKAS
20	A CLEF must be able to operate as an autonomous unit within the parent company in all day-to-day operational and administrative aspects.	Scheme
23	A CLEF must be accredited as a testing laboratory by UKAS in accordance with the current UKAS Accreditation Standard, General Requirements for the Competence of Testing and Calibration Laboratories [17025], and the CESG Test Laboratory General Operational Requirements [CGOR].	Scheme
28	A CLEF must possess its own Quality Manual that conforms to UKAS requirements.	UKAS
35	All CLEFs must operate in such a way as to preserve strict commercial confidentiality. This includes any CLEF that intends to operate remotely or virtually, in which case the associated security requirements (covering physical, personnel, procedural and information security aspects) should be included in the CLEF Quality Manual and/or the CLEF Security Manual. CLEFs that wish to be capable of performing evaluation tasks for HMG must additionally be set up and operate in accordance with the requirements of the HMG Security Policy Framework [SPF].	Scheme
38	A CLEF must possess its own Security Manual that sets out the procedures and responsibilities to be undertaken by all CLEF staff to maintain the high degree of security required to protect commercially sensitive information.	Scheme
41	Each task must be organised and managed so that task material is accessible only to authorised members of the task team.	
46	There must be a nominated person within the CLEF with overall responsibility for the security of the CLEF and the production of the CLEF Security Manual.	Scheme
51	Provision must be made for the secure storage and archiving of information held on all media and documents.	Scheme
58	Trainees new to an existing CLEF must follow a training programme approved by the CB and based on the modules detailed in Appendix B.	Scheme

Para	CLEF Requirement	Scheme/ UKAS
59	Evaluator training must be conducted by a Qualified Evaluator, or a Specialist Evaluator if appropriate.	Scheme
60	The CLEF Technical Manager and any others involved with the technical work, including technical reviews, must have attended all relevant training modules.	Scheme
68	The applicant company must submit a proposal to the CB detailing how it proposes to set up and manage a CLEF in accordance with the Scheme rules and the requirements and criteria stated in this document. The applicant company must be accredited to [17025] and [CGOR] prior to submitting their proposal.	Scheme
75	The initial training programme outlined in Appendix B must be undertaken by the relevant personnel as soon as the POC is satisfied that the arrangements with regards to CLEF management, quality management, security and task confidentiality are sufficiently far advanced.	Scheme
77	A CLEF's accreditation covering both permanent and on-site work and the test activity accredited will be detailed in their UKAS Schedule of Accreditation.	UKAS/ Scheme
86	A new CLEF must have formally completed UKAS assessment to [17025] and [CGOR] as a testing laboratory before the trial evaluation can commence.	UKAS/ Scheme
88	The CLEF must complete the required application forms available from the UKAS website http://www.ukas.com and forward them, together with a copy of the Quality Manual, Security Manual and the application fee, to the UKAS Applications Section. A copy of the CLEF Quality Manual and CLEF Security Manual must be sent to the CB once UKAS Accreditation is requested.	UKAS/ Scheme
94	A new CLEF must carry out a trial evaluation in accordance with Appendix A.	Scheme
103	It is a condition of the appointment that all proposed adverts and publicity statements intended to make mention of the Scheme or Scheme work, must be submitted to the CB Business Manager for prior approval. The CB Business Manager will give a response as soon as possible.	Scheme
104	The CLEF and Sponsor must ensure that the necessary certification services are booked.	Scheme
106	The CLEF must notify the CB when it is ready to perform an evaluation task, naming the assigned task leader.	Scheme
108	The CLEF's contract with the Sponsor must ensure adequate provision for technical support from the Sponsor during the evaluation.	Scheme

Para	CLEF Requirement	Scheme/ UKAS
110	The work performed by the Evaluators must be independent of the development of the TOE.	Scheme
112	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.	Scheme
117	All evaluation outputs must be marked "<LF_/T___> EVALUATION IN CONFIDENCE" (unless not required).	Scheme
119	The CLEF must keep the CB aware of all of the evaluation work in progress under the Scheme.	Scheme
128	The CLEF must produce a formal record (e.g. in the form of Meeting Minutes) of any required EPM and distribute the record appropriately.	Scheme
135	The work performed by the Evaluators must be independent of the development of the TOE. Evaluators must always be free from any commercial, financial and other pressures which might influence their technical judgement.	Scheme
140	The CLEF must notify the CB of any change to the role of CLEF staff with respect to an evaluation.	Scheme
145	All documentation supplied by the CLEF to the CB must be in a suitable softcopy format, either on media or via email.	Scheme
148	The CLEF must ensure that evaluation output is appropriately sanitised before it is sent to the Sponsor/Developer.	Scheme
152	At any given time, the ratio of Trainee Evaluators to Qualified Evaluators (or Specialist Evaluators if appropriate) on any evaluation should not exceed **3:1.**	Scheme
154	Evaluations at the Common Criteria EAL4 Assurance Level and higher must have an experienced Qualified or Specialist Evaluator in the team, who should play a significant and active role, preferably as Task Leader.	Scheme

Figure G.1 – Summary of Mandatory Requirements on CLEFs