



**UK IT SECURITY EVALUATION
AND CERTIFICATION SCHEME**

UK Scheme Publication No 2

CLEF REQUIREMENTS

Part I

START UP AND OPERATION

**Issue 4.3
October 2010**

© Crown Copyright 2010 – All Rights Reserved

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

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

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

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.

UK Scheme Publication 02 defines the set of requirements on Commercial Evaluation Facilities (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, please consult the Certification Body.

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

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

Facsimile: +44 (0)1242 709194

Email: iacs@cesg.gsi.gov.uk

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

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

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. (including changes to: - restructure document into two parts - reflect current status of CC - incorporate relevant SINS up to SIN 88 - change paragraph formatting)	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

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

ABBREVIATIONS AND REFERENCES

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

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

CONTENTS

I. INTRODUCTION.....	1
CLEF Appointment.....	1
Criteria	1
Terminology	2
Fees	2
II. SETTING UP A CLEF.....	3
Basic Requirements and Criteria.....	3
Quality and Management	4
Security and Confidentiality.....	5
Staff Qualifications and Training	7
The Trial Evaluation	8
III. APPOINTMENT AND ASSESSMENT FOR NEW CLEFS	9
Introduction	9
Point of Contact.....	9
Award of Provisional Appointment	9
The Preliminary Meeting	9
Initial Training.....	10
UKAS Accreditation.....	10
Granting of a Full Appointment.....	12
Summary of the Application and Appointment Process	12
IV. CLEF OPERATION	13
Introduction	13
Interaction with the Certification Body	13
Meetings.....	13
The Conduct of Evaluations	15
CLEF Staff Changes	19
UKAS Surveillance and Reassessment	19
Certification Body Surveillance and Reassessment	20
Termination of Appointment	20
Disputes	20
APPENDIX A TRIAL EVALUATION	22
Purpose.....	22
Objectives	22
Conduct.....	22
Assessment.....	23
Completion	23
APPENDIX B TRAINING	25
Evaluator Training Course.....	25
On-The-Job Training of Trainee Evaluators	27
Maintenance of Evaluator Status	28
APPENDIX C CLEF PROGRESS REPORTS AND MEETINGS.....	30
CLEF Progress Meeting.....	30
CLEF Progress Report.....	31
APPENDIX D ASSESSMENT AND OTHER FEES.....	34

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

Introduction	34
Fee For Help With Setting Up A New CLEF	34
Annual Fees	34
Certification Fees	34
UKAS Fees	34
Training Fees	34
APPENDIX E SUGGESTED CLEF MANAGEMENT STRUCTURE & TERMS OF REFERENCE	35
Terms of Reference	35
CLEF Controller	35
Technical Manager.....	35
Quality Manager.....	36
Business Manager	36
Security Manager	36
Administration Manager	36
Computer Manager	36
Methods Advisor	36
Task Leaders	36
Evaluators	36
APPENDIX F CHECKLIST FOR USE WITH THE APPLICATION AND SET-UP PROCESS	37
Meeting Basic Requirements	37
Quality Manual	37
Management Roles	37
Security and Confidentiality.....	37
Evaluator Status and Training.....	38
Provisional Appointment.....	38
Preliminary Meeting	38
Initial Training.....	38
UKAS Accreditation.....	38
Trial Evaluation	38
APPENDIX G SUMMARY OF CLEF OBLIGATIONS	39

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

I. INTRODUCTION

CLEF Appointment

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 Certification Body (CB) of the Scheme.
2. This 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. 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 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.
4. 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]).
5. CLEFs are subject to basic requirements and rules of operation specified in detail in this document, which form part of the conditions of appointment. These rules govern:
 - a) Quality and Management;
 - b) Security and Confidentiality;
 - c) Staff Qualifications and Training.
6. It is assumed that the reader of this document is familiar with the principles of security evaluation and certification as described in UK Scheme Publication No. 1 (UKSP 01 – Description of the Scheme) [UKSP01]; Common Criteria for Information Technology Security Evaluation (CC) [CC]; or the IT Security Evaluation Criteria (ITSEC) [ITSEC].

Criteria

7. Evaluations are carried out according to one of the CB recognised IT security evaluation criteria using the criteria's associated evaluation methodology. These include the CC [CC] using its associated Common Evaluation Methodology (CEM) [CEM] and [VLAC]; and ITSEC [ITSEC] using its associated methodology as specified in the IT Security Evaluation Manual (ITSEM) [ITSEM] and UK Scheme Publication Number 05 [UKSP05-III]. The criteria are subject to the relevant International Interpretations, UK Interpretations and Scheme Information Notices (SINs).

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

8. As far as possible, UKSP 02 (of which this is Part I) has been written to be independent of any particular IT security evaluation criteria.

Terminology

9. The terminology used in relation to the appointment process follows that of “The Conduct of UKAS Laboratory Assessments”¹, 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.

10. The term “CLEF” is used for those commercial evaluation facilities appointed by the Certification Body to perform the set of security evaluations for which the facility is accredited by UKAS. In some evaluation criteria recognised by the Certification Body, equivalent but different terms may be used. For legal reasons connected with charging for Certification Body services, the word “appointment” is used instead of license.

11. 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. In some cases the word **must** is also used in the context of an interpretation of a more generally stated mandatory requirement, or of a mandatory requirement imposed by other documents. For the sake of clarity and brevity, such instances are not highlighted by the means of text boxes.

12. 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 Certification Body). Occasionally a “preferred approach” may be highlighted by the means of a text box, where it provides a more concise (and memorable) expression of an underlying mandatory requirement.

Fees

13. Since 1 April 1997, the Certification Body 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 a fee, details of which are available from the UKAS Executive.

¹ This document is available at <http://www.ukas.com/>

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

II. SETTING UP A CLEF

Basic Requirements and Criteria

14. For Government work involving Protectively Marked information, a CLEF (and its parent company where applicable) will normally be under predominantly UK control (the Certification Body may consider exceptions on a case by case basis).

15. 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.

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

17. 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.

18. 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 and confidentiality;
- c) a minimal hardware investigation capability, sufficient to satisfy a basic fault finding and correction requirement;
- d) office space available for Certification Body staff, when required;
- e) communications facilities enabling rapid exchange of information with the Certification Body and Sponsor;
- f) archive facilities capable of meeting UKAS requirements.

19. A CLEF must be accredited as a testing laboratory by UKAS in accordance with the current UKAS Accreditation Standard, ISO/IEC 17025.

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

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

22. All new CLEFs are required to 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);

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

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

Quality and Management

Management Objectives

23. 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

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

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

Specific Management Roles

26. A suggested management structure for a CLEF is described here and shown diagrammatically 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.

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

- a) a Technical Manager;
- b) a Quality Assurance Manager;
- c) a Business Manager;
- d) an Administration Manager;
- e) a Security Manager.

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

29. Other possible roles include a Computer Manager and a Methods Adviser, who also report to the Technical Manager.

30. Certain of these roles may be undertaken by the same person, provided no conflict of interest exists between the different roles. For example, as would be the case if the Quality Assurance Manager also performed evaluation tasks and where this does not jeopardise the effective performance of any task or where the burden becomes too great for one individual.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Security and Confidentiality

31. 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 and procedural aspects) should be included in the CLEF Quality Manual and/or the CLEF Security Manual. Those 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 UK Government Security Framework.

32. The requirements of the UK Government Security Framework provide for the security of HMG Protectively Marked information. The UK Government Security 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.

33. 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

34. 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.

35. The Security Manual should specify procedures for:

- a) Physical Security;
- b) Personnel Security;
- c) Information Security.

36. With regard to information security, the Security Manual should cover the handling of commercially sensitive information in whatever form it is held.

37. The Security Manual should further address the means 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 violations;
- f) the physical, personnel and procedural aspects of remote or virtual working.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

38. 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.

39. 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 Certification Body and UKAS assessors.

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 carried out 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 Certification Body 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.

Information Security

45. 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.

46. Secure communications equipment (approved by CESG) may be needed for some tasks. USB memory sticks may also be required for transferring sensitive information.

47. Provision must be made for the secure storage and archiving of information from all media and documents.

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

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

Task Confidentiality

50. The above measures contribute to the maintenance of task confidentiality. CLEFs may propose arrangements (for example, covering remote or virtual working) that preserve confidentiality, whilst allowing more efficient management of the work, to the Certification

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Body. Such proposals should, of course, also be acceptable to any Sponsors whose tasks may be involved.

Staff Qualifications and Training

Objectives

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

- a) understand the notion and principles of computer security;
- 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

52. 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 Certification Body to be capable of contributing to an evaluation without detailed supervision²;
- c) *Specialist Evaluator*, i.e. A Trainee Evaluator who has been assessed by the Certification Body to be capable of contributing to an evaluation without detailed supervision² for some subset of the CC Assurance Classes³ (or some subset of the ITSEC criteria) and has extensive knowledge of a specialist security field⁴.

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

² See paragraphs 132-135 for further information.

³ The Assurance Classes for CC Version 3.1 are: ADV (Development), AGD (Guidance Documents), ALC (Life-Cycle Support), ASE (Security Target Evaluation), ATE (Tests), AVA (Vulnerability Assessment) and APE (Protection Profile Evaluation). The Assurance Classes for CC Version 2.3 are: ASE (Security Target Evaluation), ACM (Configuration Management), ADO (Delivery and Operation), ADV (Development), AGD (Guidance Documents), ALC (Life Cycle Support), ATE (Tests), AVA (Vulnerability Assessment) and APE (Protection Profile Evaluation).

⁴ 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.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Training Requirements

54. Evaluation Staff new to an existing CLEF must follow a training programme approved by the Certification Body and based on the modules detailed in Appendix B.

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

56. 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.

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

The Trial Evaluation

58. The purpose of the trial evaluation is to demonstrate to the Certification Body that the CLEF is competent to perform evaluations to the Common Criteria evaluation levels acceptable to the Certification Body 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

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

60. Full Appointments are thus awarded to interested commercial companies which have been successfully assessed by both the Certification Body and UKAS. Such appointments confirm that the CLEF is competent to perform security evaluations to specific target evaluation levels.

Point of Contact

61. The Certification Body will appoint one of its staff as a Point of Contact (POC) for the 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 Certification Body will strive to ensure that the same POC is responsible for processing a CLEF's application through the Trial Evaluation (see paragraph 90 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.

62. 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

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

64. The applicant company must submit a proposal to the Certification Body 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.

65. If this proposal is accepted by the Certification Body, then the applicant company is granted a Provisional Appointment to undertake a trial evaluation.

The Preliminary Meeting

66. 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 Certification Body and by UKAS.

67. Thus the primary purpose of the preliminary meeting is for the Certification Body to advise the applicant company upon the setting up of the CLEF. The meeting has the further intention of introducing the various members of the Certification Body who will assist in the setting up of the CLEF and to clear up any difficulties or confusion about the appointment and assessment process.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

68. 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 Certification Body 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.
69. The POC will take no part in the UKAS assessment, but will be able to advise on the necessary preparations and on other requirements for evidence in respect of attaining a Full Appointment. The POC will be accompanied during the preliminary visit by other members of the Certification Body, as required.
70. It is expected that further meetings will be held in order to review progress. These will normally be chaired by the POC.

Initial Training

71. 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 assurance, security and task confidentiality are sufficiently far advanced.

UKAS Accreditation

Categories of Accreditation

72. A CLEF will be assessed for two categories of UKAS Test Laboratory Accreditation, namely:
- Permanent laboratory (the CLEF) where the testing facility is on a fixed location.
 - Site testing performed by staff sent out on site by a permanent laboratory that is accredited by UKAS.

73. A CLEF's accreditation covering both permanent and site work and the test accredited will be detailed in their UKAS Schedule of accreditation.

74. 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 environment assessments) and not just testing.

Schedule of Accreditation

75. 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 Certification Body. This Schedule specifies the tests that a CLEF has

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

been accredited to perform and is limited to tests that meet UKAS requirements for objectivity, impartiality, repeatability and reproducibility. It provides traceability to supporting standards and procedures.

76. The scope of Accreditation includes the use of the evaluation criteria and methodology. The Certification Body 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 Certification Body will agree an extension to the Schedule with UKAS and will require new and existing CLEFs to seek Accreditation to the new Schedule.

77. 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 Certification Body approval to ensure uniformity and correctness of evaluation procedures and consistency and compatibility in the reporting of evaluation results.

78. In performing this role the Certification Body may make an appointment to cover all the tests that a CLEF performs, including those not accredited by UKAS. The Certification Body 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 Certification Body.

79. Accreditation by UKAS and these additional requirements together constitute appointment by the Certification Body.

80. 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 Certification Body 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.

81. It is likely that the 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

82. A new CLEF must make a formal application to UKAS for Accreditation as a testing laboratory before the trial evaluation can commence.

83. UKAS will use the trial evaluation as the basis for its assessment 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.

84. 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 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 Certification Body once UKAS Accreditation is requested.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

85. Throughout its lifetime, a CLEF will deal directly with UKAS on matters concerning its own Accreditation. The Certification Body 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 Certification Body will, however, keep the results of UKAS Accreditation under review for appointment purposes.

Conduct of UKAS Assessments

86. The UKAS assessment and accreditation process is conducted as an independent activity in accordance with its standard procedures; they are described in detail in [CULA], 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.

87. 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 Certification Body, but if so, he will not be engaged on certification work related to any evaluation which was used for the purposes of the UKAS assessment, unless agreed by the CLEF. Also, the POC will not be involved in the assessment.

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

89. Formal UKAS assessment is expected to take place during the latter stages of the trial evaluation; each category of Accreditation should be completed in one or two days.

The Trial Evaluation

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

91. It may be expected to last between 3 and 4 months and should end with reporting of the results to the Certification Body. The POC will be responsible for training the CLEF to carry out the trial evaluation.

Granting of a Full Appointment

92. 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 Head of the Certification Body will notify the CLEF of the outcome of the Certification Body's decision and any conditions affecting the appointment.

Summary of the Application and Appointment Process

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

IV. CLEF OPERATION

Introduction

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

95. Each CLEF should have a close working relationship with the Certification Body to ensure that the interactive processes of evaluation and certification proceed smoothly. This relationship will be fostered by informal contacts with the Certification Body, through the POC and through day-to-day work on evaluations.

Interaction with the Certification Body

General

96. It is necessary for the Certification Body to be assured that the activities of any CLEFs do not bring the Scheme, other evaluation facilities or the supporting HMG departments or agencies into disrepute. Consequently, the Certification Body 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 Framework.

General Liaison

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

Business Liaison

98. 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 provides the Certification Body with an overview of the current CLEF business and the current status of the CLEF with respect to the Scheme and permits the CLEF to raise formally any specific concerns with the Certification Body. The requirements for this forum are specified below.

Advertisements and Publicity

99. 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 normally give a response within ten working days.

Meetings

CLEF Progress Meetings (CPM)

100. The CLEF must keep the Certification Body aware of all of the evaluation work in progress under the Scheme.

101. CLEF Progress Meetings (CPMs) will be held at a frequency and location mutually agreed between the Certification Body and the CLEF. These meetings are to enable the Certification Body 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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

representatives of the Certification Body. The CLEF should submit the required copies of the CLEF Progress Report to the CB Secretary at least ten working days before the meeting.

102. 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 Certification Body and the CLEF.

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

104. The CPR and CPM provide the Certification Body with an overview of the CLEF's current and future business and status with respect to the Scheme. The CPR also enables the CLEF to formally raise any specific concerns with the Certification Body.

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

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

a) from the Certification Body:

- Head of Certification Body (Chairman);
- Business Manager.

b) from the CLEF:

- CLEF Controller;
- CLEF Technical Manager.

107. In addition, other members of the management of the Certification Body and the CLEF may wish to attend.

108. 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)

109. Evaluation Progress Meetings are called at the discretion of the Sponsor, Certification Body 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.

Other Meetings

110. 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 however be required to be present for discussion of financial aspects of such contracts.

CLEF Controllers' and Technical Managers' Meetings

111. Meetings may also be held between the Certification Body and CLEF Controllers, Business Managers, or Technical Managers to discuss administrative, promotional or technical issues.

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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

The Conduct of Evaluations

Commercial Impartiality

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

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

115. 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 Certification Body, 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.

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

- a) both the development of the TOE and performance 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.

117. CLEF staff may not engage in any evaluation activities on which they have previously acted as consultants, unless the CLEF can demonstrate to the Certification Body that the independence of the evaluation will not be compromised.

118. 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 will not be compromised (e.g. by knowledge of the sampling strategy).

119. The CLEF must notify the Certification Body of any change to the role of CLEF staff with respect to an evaluation.

120. Notwithstanding the various statements on Evaluator independence in the evaluation criteria (CC, ITSEC) and methodology (CEM, ITSEM), the CLEF evaluation team may produce the security target, low-level (detailed) design and vulnerability analysis (or effectiveness) deliverables as part of the evaluation process for systems which are for HMG use only and are 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 Certification Body must first be obtained. For example, agreement will not usually be given where such a product has a commercial variant that may make reuse of the evaluation results.

121. 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 115.) 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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

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).

122. These independence requirements are summarised in the following Figure.

CLEF Activities	CLEF Staff Role		
	Evaluator	Developer	Consultant
Evaluation or Re-evaluation	✓		(Para 123)
TOE Development		✓	✓
Consultancy	(Para 118)	✓	✓
Production of security target, low-level design and vulnerability analysis (effectiveness) deliverables	(Para 120)	✓	✓
Activities in respect of TOE developed by group or division within CLEF's parent company	(Para 115)	✓	✓
CLEF management – same immediate technical management for development/consultancy and evaluation	–	–	–

123. The independence rules for CLEF staff performing evaluation activities for CMS tasks are given here and supersede those given in UKSP 16 Part I [UKSP16-I].

124. During any CMS maintenance cycle of a given TOE (i.e. the period between the completion of an evaluation or re-evaluation and the conclusion of the subsequent CMS re-evaluation), a CLEF may not:

- a) participate in any evaluation activity (i.e. Certification Maintenance (CM) Audit, CMS Re-evaluation and the review of the CM Plan and the CM Status Report) for a particular TOE where the CLEF has also provided part or all of the Developer Security Analyst (DSA) function during the same maintenance cycle; or
- b) employ staff on any evaluation activity for a particular TOE who have been concerned with its development or have provided pre-evaluation consultancy for it during the same maintenance-cycle; or
- c) evaluate the work of any group or division within the parent company to which it belongs, or any associate partner who is a TOE developer.

125. These rules may be relaxed at the discretion of the Certification Body, 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. The Certification Body does not anticipate any relaxation of the independence requirements in respect of CM Audits, but a relaxation may otherwise be granted, in accordance with paragraphs 115 and 120, to HMG systems and more rarely to specialised products for use in HMG systems.

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

126. The permitted CLEF roles in CMS are summarised in the following figure.

CLEF Activities	CLEF Staff Role		
	Evaluator	Developer	Consultant
Review of CM Plan	✓	–	–
CM Audit	✓	–	–
Review of CM Status Report	✓	–	–
CMS Re-evaluation	✓	–	–
TOE Maintenance	–	✓	✓
Consultancy	–	✓	✓

127. The permitted CLEF CMS Evaluation Activities are summarised in the following figure.

CLEF Evaluation Activities	DSA and TOE from external company	DSA provided by CLEF	TOE developed by parent company
CM Audit	✓	–	–
Review of CM Plan	✓	(Para 125)	(Para 125)
Review of CM Status Report	✓	(Para 125)	(Para 125)
CMS Re-evaluations	✓	(Para 125)	(Para 125)

Sanitisation of Evaluation outputs

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

129. 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 for the evaluation;
- d) commercially sensitive information.

130. 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).

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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Evaluator Teams

132. 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**.

133. In exceptional circumstances this rule may be relaxed at the discretion of the Certification Body, who may then require additional safeguards to ensure the following UKAS rules are upheld:

- a) the proportion of Trainee Evaluators should not be such as to have an adverse effect on the quality of the work;
- b) Trainee Evaluators receive sufficient supervision so as to ensure the correct performance of their duties.

134. Evaluations at the Common Criteria EAL5 or ITSEC E4 Assurance Level and higher must have an experienced Evaluator in the team, who should play a significant and active role, preferably as Task Leader.

135. The role of the experienced Evaluator in such evaluations will be considered sufficiently significant if it is such as to give confidence in the overall technical quality of evaluation work throughout the evaluation. The Evaluator will be considered sufficiently experienced if he/she has held Qualified Evaluator or Specialist Evaluator status for at least three years and has played a significant role in evaluation tasks during this time (as agreed with the CB). In particular, evaluations at CC EAL7 must have a formal methods expert in the team.

136. 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. In particular, evaluations that require knowledge of a specialist security field must include an appropriate Specialist Evaluator.

137. 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 TSM minutes, for audit purposes.) Such specialists, who must be suitably recognised (see sections 138-139) by the 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 optimally 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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

testing by specialist penetration testers. Additional advice and recommendations can be provided to the CLEF by request to the CB.

Specialist Penetration Tester Qualifications

138. For assurance levels of EAL3 and higher, any specialist penetration tester included in the evaluation team must be recognised by the NTA for Information Assurance 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.

139. 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.

140. 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

141. The Certification Body 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

142. All evaluation staff who have not previously worked for a CLEF should be notified to the Certification Body 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

143. If the new member of CLEF staff has previous evaluation experience, but currently has no Evaluator status, application may be made to the Certification Body for the (re)award of a status.

UKAS Surveillance and Reassessment

144. UKAS assessors will carry out surveillance visits to the CLEF as specified in [CULA]. 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.

145. 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 and reassessment assesses the CLEF in its conduct of "real life" 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.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

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

147. Surveillance and reassessment visits for accreditation of the permanent laboratory may be carried out on different days from those for the accreditation of site work, which will involve the assessors accompanying the Evaluators on a site visit.

148. 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 Certification Body and UKAS on the scope of the extended Schedule.

149. 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 tests 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 tests without the prior approval of UKAS.

Certification Body Surveillance and Reassessment

150. Independently of UKAS, the Certification Body 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

151. The Certification Body reserves the right at short notice to withdraw the 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 UK Government Security Framework. There will also be an assessment of the impact of the takeover (or merger) with respect to client information confidentiality or other contractual conflicts.

152. Normally, the Certification Body 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.

153. At the termination of a CLEF appointment, the Certification Body 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 Certification Body. 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.

154. The Certification Body also reserves the right to withdraw all CLEF appointments if the Scheme is to be terminated, on six months notice.

Disputes

155. In the event of a dispute between the CLEF and the Certification Body, the CLEF or its parent company has the right of appeal.

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

156. In the first instance the CLEF should strive to resolve the matter directly with the Certification Body via the Head of the Certification Body. 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 security evaluation is to demonstrate to the Certification Body that a CLEF is competent to perform evaluations. It is also used as the basis for the UKAS assessment and must cover both permanent laboratory work and 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 Certification Body, 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 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 POC. The scope of the evaluation will however need to cover all the tests specified in the Schedule (see paragraph 75).

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 Certification Body 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 direction of the POC. 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

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

the 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 Training Officer will not be involved in this assessment.

A.11. Independently of UKAS, the Certification Body 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 evaluation and produce a Certification Report based on a draft provided by the CLEF.

Assessment

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

- a) the planning of the evaluation, including production of the EWP;
- 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 Certification Body 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 Training Officer to determine whether or not they have demonstrated sufficient competence to be regarded by the Certification Body as Qualified Evaluators⁵. 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 Certification Body 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 Certification Body. Given that the CLEF has met all other criteria to the satisfaction of the Certification Body, including the

⁵ The Specialist Evaluator qualification is not relevant to a Trial Evaluation.

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

granting of Accreditation by UKAS and reports from the Training Officer 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 Material⁶ 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.

⁶ The training material may be out of date and trainers will need to reflect current practice. It relates to CC (version 2.1) and ITSEC.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

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 Certification Body and the CLEFs.

B.11 Changes to the Methodology are promulgated by means of Interpretations. The CLEF trainers are expected to be aware of these changes and must point these out to students during their presentation of the course modules. Periodically, the Certification Body will carry out a review of the training material in which the effects of all Interpretations and SINs⁷ 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 Certification Body indicating the precise nature of the problem. If the error is seriously misleading then a correction will be issued by the Certification Body; however if the problem is minor then corrective action will be taken during the review and update exercise referred to above.

⁷ SINs that are published on the CESG website have status Open (currently these are SIN 091 and SIN 092). All other SINs are obsolete and therefore have status Closed.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Conduct

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

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

Charges

B.15 Where CLEFs present courses for other CLEFs, they may make an appropriate charge for their 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 Certification Body 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 or ITSEC by their application in a real evaluation;
- b) have experience that includes the following:
 - performance of all Evaluator actions required for a typical Common Criteria evaluation;
 - examination of the development environment of at least one TOE;
 - examination of the operational environment and documentation of at least one TOE;
 - have experience in the planning and conduct of functional and penetration tests;
- c) be able to demonstrate an understanding of the UKAS aspects of the evaluation process, the CLEF Quality Manual and the CLEF Security Manual;

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

- 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 Certification Body, 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 part 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:

- 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 Certification Body 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 reports which are independently produced by the Trainee 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 Certification Body 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 Certification Body within the context of the Scheme; Evaluators must not therefore claim Certification Body 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 six 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 Certification Body 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.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

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 Certification Body.

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

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. Task Overview
 - G. Common Criteria Concerns
 - H. Legacy Scheme Status
 - I. CLEF View On The Strategic Future of CC
 - J. Marketing Issues
 - K. Staffing Issues
 - L. Appointment Issues
 - M. General Scheme Issues
 - N. Administration Issues
 - O. General Technical Issues
 - P. Task Status Reports
 - Q. Any Other Business
 - R. Action Summary
 - S. Date of Next Meeting
- (This should be updated, for each meeting, with current business topics.)*

Figure C.1 – CLEF Progress Meeting - Example Agenda

C.1. The major agenda items are discussed in the following sub-sections.

Item F – Task Overview

C.2. The following topics should be reviewed:

- a) the general workload;

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

- 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.3. The future prospects should be reviewed insofar as they impact upon the Certification Body, subject to commercial concerns.

Item K – Staffing Issues

C.4. 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.5. 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.6. This item should allow attendees to raise any other Scheme related matters e.g. status of SINS and interpretations.

Item N – Administration Issues

C.7. Any organisational matters related to the CLEF should be raised under this item.

Item O – General Technical Issues

C.8. 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.9. Task Status Reports should be considered where there are issues for the CPM attendees to discuss.

CLEF Progress Report

Overview

C.10. The objective of the CPR is to provide the Certification Body 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 Certification Body, for discussion at the next CPM.

Structure

C.11. The structure of a CPR should be as follows:

- a) Title page, including reference, issue, date, distribution and copyright.
- b) Contents page.
- c) Introduction.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

- d) Task Overview, listing all the current tasks within the CLEF and their current status (e.g. active, inactive, cancelled, reported⁸ 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 future inputs to the Certification Body 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 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.12. 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.13. 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.

⁸ The status "reported" indicates that an ETR has been issued to the CB.

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

Protective Markings

C.14. The main body of the CPR and any annexes (i.e. each TSR) should bear its own appropriate protective marking.

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

**Appendix D
ASSESSMENT AND OTHER FEES**

Introduction

D.1 Since 1 April 1997 the Certification Body has been required to cover 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 Certification Body on the granting of a Provisional Appointment to cover the cost of Certification Body 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 Certification Body 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 Certification Body 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 Certification Body services will normally be levied directly on the Sponsor for each evaluation (or re-evaluation) and for assurance maintenance.

UKAS Fees

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

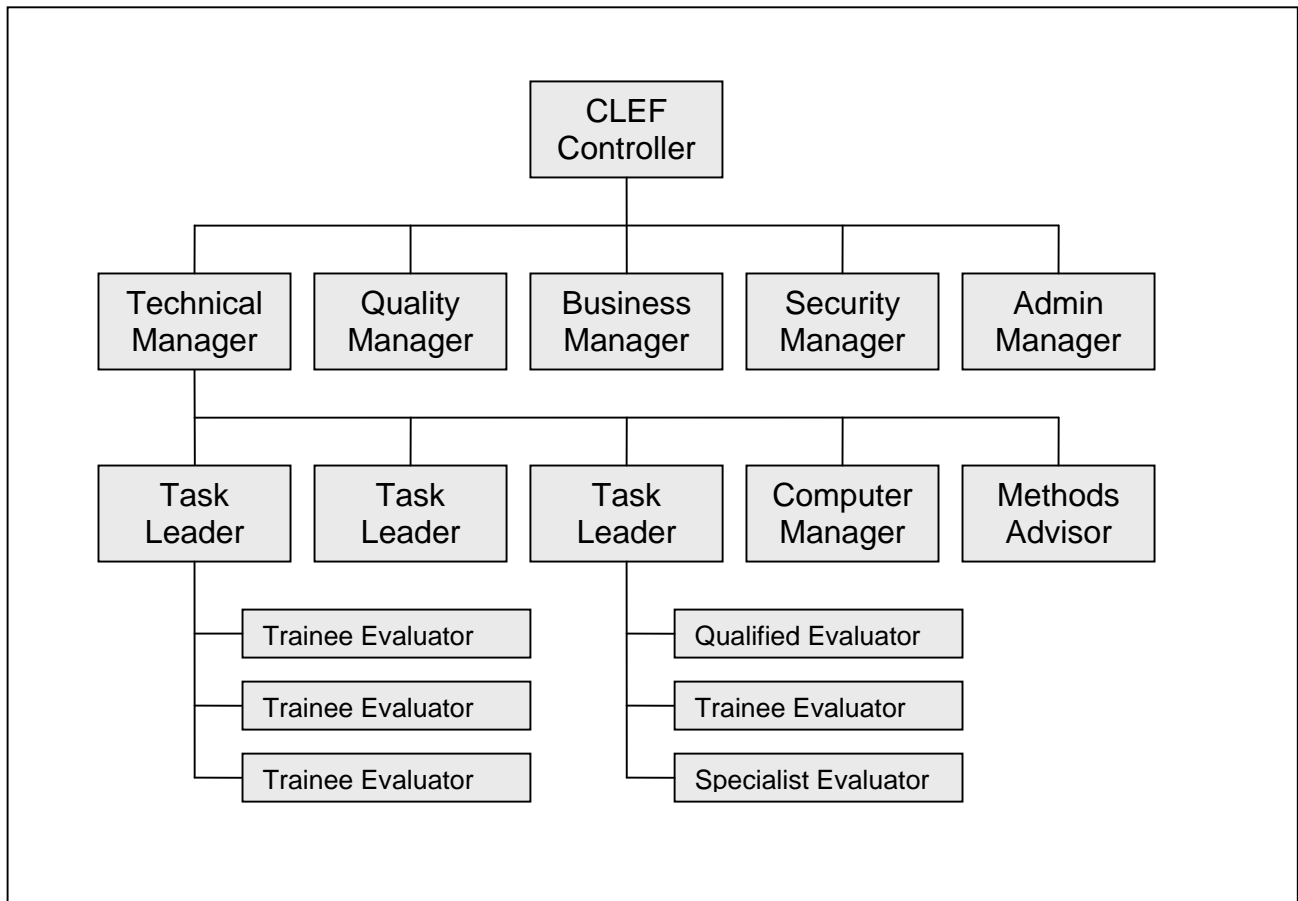
Training Fees

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

Appendix E

SUGGESTED CLEF MANAGEMENT STRUCTURE & TERMS OF REFERENCE

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 Certification Body on matters concerning the evaluation methodology.

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

Quality Manager

E.5 The Quality Manager ensures that the procedures detailed in the CLEF Quality Manual are followed and for taking any remedial action that may be required as a result of either internal or UKAS quality audits.

Business Manager

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

Security Manager

E.7 The Security Manager is responsible for the physical, personnel and information security aspects of CLEF operation. This post liaises with the Government Departments responsible for overseeing compliance with the UK Government Security Framework. Any CLEF Security Guards report to the Security Manager.

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 provides advice and guidance on the use of the evaluation methodology and its interpretations within the CLEF. This post will liaise with the Certification Body on methodology aspects of the CLEF's operations.

Task Leaders

E.11 Evaluation Task Leaders are responsible for the correct conduct of the evaluations that they lead, ensuring compliance with the evaluation methodology and current Certification Body 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.12 Covered by the constraints on "The Conduct of Evaluations" in Chapter IV.

Appendix F

CHECKLIST FOR USE WITH THE APPLICATION AND SET-UP PROCESS

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 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?

F.8 (If appropriate:) Are the requirements of the UK Government Security Framework met? When was its security status granted? When was it last reviewed?

Quality Manual

F.9 Is there a Quality Manual?

F.10 Does it conform to UKAS requirements?

F.11 Has it been reviewed by UKAS? If so, when, and with what result?

Management Roles

F.12 Who is the CLEF Controller?

F.13 Who is the Technical Manager?

F.14 Who is the Quality Manager?

F.15 Who is the Business Manager?

F.16 Who is the Administration Manager?

F.17 Who is the Security Manager?

F.18 Is there a Computer Manager?

F.19 Is there a Methods Adviser?

F.20 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.21 Who has overall responsibility for the security of the CLEF and production of the Security Manual?

F.22 Does the Security Manual adequately cover the areas of concern laid down in UKSP 02?

UK IT Security Evaluation & Certification Scheme CLEF Requirements Part I – Start Up and Operation

F.23 Are CLEF staff cleared? To what level?

F.24 What facilities exist for secure storage of media and documents?

F.25 What are the arrangements for maintaining task confidentiality?

F.26 How are CLEF computing facilities separated from those of the parent company?

Evaluator Status and Training

F.27 What is the Evaluator status of CLEF staff?

F.28 What Initial Training is required and how will it be arranged?

Provisional Appointment

F.29 Has a formal application been made for a Provisional Appointment?

F.30 Has a proposal been submitted to the Certification Body detailing how the applicant company plans to set up and manage the CLEF?

Preliminary Meeting

F.31 Has the Preliminary Meeting been held?

Initial Training

F.32 What Initial Training has been arranged? Who will give it and when? What will be covered?

UKAS Accreditation

F.33 Has formal application been made to UKAS for Accreditation as a testing laboratory?

F.34 Have copies of the CLEF Quality and Security Manuals been sent to the Certification Body?

Trial Evaluation

F.35 Has a TOE been identified for use as the trial evaluation?

F.36 Has this been agreed by the Certification Body?

F.37 How far has the trial evaluation progressed?

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

**Appendix G
SUMMARY OF CLEF OBLIGATIONS**

F.38 G.1 This Appendix contains a summary of CLEF responsibilities in the context of their start-up and operation as required by the UK Scheme. The main body of this document marks these with text boxes.

CLEF obligation	UKAS/Scheme
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
A CLEF must be accredited as a testing laboratory by UKAS in accordance with the current UKAS Accreditation Standard, ISO/IEC 17025.	Scheme
A CLEF must possess its own Quality Manual that conforms to UKAS requirements.	UKAS
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 and procedural aspects) should be included in the CLEF Quality Manual and/or the CLEF Security Manual. Those 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 UK Government Security Framework.	Scheme
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
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
Each task must be carried out so that task material is accessible only to authorised members of the task team.	Scheme
Provision must be made for the secure storage and archiving of information from all media and documents.	Scheme
Evaluation Staff new to an existing CLEF must follow a training programme approved by the Certification Body and based on the modules detailed in Appendix B.	Scheme
Evaluator training must be conducted by a Qualified Evaluator, or a Specialist Evaluator if appropriate.	Scheme

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**

CLEF obligation	UKAS/Scheme
The CLEF Technical Manager and any others involved with the technical work, including technical reviews, must have attended all relevant training modules.	Scheme
The applicant company must submit a proposal to the Certification Body 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.	Scheme
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 assurance, security and task confidentiality are sufficiently far advanced.	Scheme
A CLEF's accreditation covering both permanent and site work and the test accredited will be detailed in their UKAS Schedule of accreditation.	UKAS/Scheme
A new CLEF must make a formal application to UKAS for Accreditation as a testing laboratory before the trial evaluation can commence.	UKAS/Scheme
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 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 Certification Body once UKAS Accreditation is requested.	UKAS/Scheme
A new CLEF must carry out a trial evaluation in accordance with Appendix A.	Scheme
The CLEF must keep the Certification Body aware of all of the evaluation work in progress under the Scheme.	Scheme
The work performed by the Evaluators must be independent of the development of the TOE. Evaluators must be free from any commercial, financial and other pressures which might influence their technical judgement.	Scheme
The CLEF must notify the Certification Body of any change to the role of CLEF staff with respect to an evaluation.	Scheme
The CLEF must ensure that evaluation output is appropriately sanitised before it is sent to the Sponsor/Developer.	Scheme
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
Evaluations at the Common Criteria EAL5 or ITSEC E4 Assurance Level and higher must have an experienced Evaluator in the team, who should play a significant and active role, preferably as Task Leader.	Scheme

Figure G.1 – CLEF Responsibilities

**UK IT Security Evaluation & Certification Scheme
CLEF Requirements Part I – Start Up and Operation**