UKSP 02

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No 2

THE APPOINTMENT OF COMMERCIAL EVALUATION FACILITIES

Issue 3.0

3 February 1997

Issued by:-

UK IT Security Evaluation & Certification Scheme

Certification Body

This page is intentionally left blank.

FOREWORD

This document was prepared by the Certification Body of the UK IT Security Evaluation and Certification Scheme (the Scheme).

Evaluations under the Scheme are performed by CommerciaL Evaluation Facilities (CLEFs). CLEFs are managed and staffed by commercial organisations which have been appointed under the Scheme. This document specifies the rules for appointing new CLEFs and their continuing operations.

P.M.Seeviour
Senior Executive
UK IT Security Evaluation and Certification Scheme

Correspondence in connection with this document, including requests for additional copies, should be addressed to:

Certification Body Secretary
UK IT Security Evaluation & Certification Scheme
PO Box 152
Cheltenham
Glos GL52 5UF
United Kingdom

Telephone: +44 1242 238739

Facsimile: +44 1242 235233

AMENDMENT RECORD

Amendments to this document will be published as and when required. The amendment record shall be maintained so that it indicates all changes made to the latest issue of the document.

Amendment Instruction Number	Pages Affected (SINs incorporated)	Incorporated by NAME Signature	Date

CONTENTS

REFERENCES

A. Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 3.0, 2nd December 1996

B. ITSEC - Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria, Version 1.2, 28 June 1991.

C. ITSEM - IT Security Evaluation Manual, V1.0, September 1993.

D. NAMAS Accreditation Standard, General Criteria of Competence for Calibration and Testing Laboratories; M10, Edition 1, March 1989, and Supplement Edition 1, February 1993, NAMAS Executive, NPL, Teddington.

E. NAMAS Regulations, Regulations to be met by Calibration and Testing Laboratories, M11, Edition 1, April 1989, NAMAS Executive, NPL Teddington.

F. The Conduct of NAMAS Assessments, A Guide for Laboratories; M22, Edition 1, December 1992, NAMAS Executive, NPL, Teddington.

G. NAMAS - The Quality Manual: Guidance for Preparation; M16, July 1989, NAMAS Executive, NPL, Teddington.

H. Accreditation for Site Calibration and Site Testing, M18, Edition 1, NAMAS Executive, June 1996, NAMAS Executive, NPL, Teddington.

I. Interpretation of Accreditation Requirements for IT Test Laboratories for Software and Communications Testing Services, NIS35, November 1990, NAMAS Executive, NPL Teddington.

J. Manual of Protective Security, Cabinet Office (Protectively Marked).

K. Manual of Computer Security Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 05, Part I, Evaluation Procedures, Issue 3.0, October 1994.

L. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general Guide, CCEB-96/011, Version 1.0, January 1996.

M. UKSP 06 -UK Scheme Publication Number 6, UK Certified Product List.

ABBREVIATIONS

CB	Certification Body
CESG	Communications-Electronics Security Group
CLEF	CommerciaL Evaluation Facility (formerly Commercial Licensed Evaluation Facility)
CMS	Certificate Maintenance Scheme
CPM	CLEF Progress Meeting
Compusec	Computer Security
DSA	Developer Security Analyst
DTI	Department of Trade and Industry
ECM	Evaluation Control Meeting
EPM	Evaluation Progress Meeting
HMG	Her Majesty's Government
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
ITSEM	Information Technology Security Evaluation Manual
NAMAS	National Measurement Accreditation Service (former name of UKAS)
OJT	On-the-Job Training
POC	Point of Contact
Schedule	UKAS Schedule of Accreditation
Scheme	UK IT Security Evaluation & Certification Scheme
SEISP	System Electronic Information Security Policy
SIN	Scheme Information Notice
SISP	System Interconnection Security Policy
SOR	Scheme Observation Report
SSP	System Security Policy

TOE	**Target of Evaluation**
UK	**United Kingdom**
UKAS	**United Kingdom Accreditation Service**
UKSP	**UK Scheme Publication (UK IT Security Evaluation and Certification Scheme)**

This page is left intentionally blank.

Chapter 1. INTRODUCTION

CLEF Appointment

1.1. Evaluations under the UK IT Security Evaluation and Certification Scheme (the Scheme) must be 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.

1.2. 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 Assurance Level falls within the scope of UKAS accreditation.

1.3. 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.

1.4. This document sets out the objectives, assessment criteria and requirements for evidence for a Company wishing to be appointed as a Commercial Evaluation Facility (CLEF).

1.5. 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) [A] and the IT Security Evaluation Criteria (ITSEC) [B].

Criteria

1.6. Evaluations are currently carried out according to the criteria defined in the ITSEC [B], using the methodology specified in the IT Security Evaluation Manual (ITSEM) [C] and UK Scheme Publication Number 05 [K].

1.7. Evaluations to the Common Criteria [L] are expected to commence towards the latter half of 1997 following the anticipated successful completion of its trial. The Common Criteria represents the outcome of international efforts to develop and align both European and North American criteria. This alignment has ensured a broad correspondence between ITSEC and Common Criteria concepts thus protecting current investment in ITSEC evaluations. Given sufficient effort during the evaluation, it is expected that the Certification Body will be able to issue

certificates against both ITSEC and Common Criteria.

1.8. As a consequence of the development and alignment of criteria, the Common Criteria does not always use the same terminology as the ITSEC to describe similar concepts. UKSP 02 (this document) has been written on the basis of CLEF appointments granted to allow UKAS accreditation for evaluations to ITSEC. These ITSEC concepts should be taken to extend to the broadly corresponding Common Criteria concepts.

Terminology

1.9. The terminology used in relation to the appointment process follows that of "The Conduct of NAMAS Assessments" [F], although throughout Scheme documents the term 'Sponsor' refers to the person or organisation that requests an evaluation. This equates to the 'client' in United Kingdom Accreditation Service (UKAS) terms.

1.10. Within the ITSEM [C] the term ITSEF (IT Security Evaluation Facility) is used, and is defined as being 'an organisation accredited in accordance with some agreed rules (eg EN45001) and licensed by the Certification Body to perform ITSEC security evaluations'. Within the UK, the accreditation authority for EN45001 is UKAS and the term CLEF is used instead of ITSEF. For legal reasons connected with charging for Certification Body services, the word appointment is used instead of license. CLEFs must meet the requirements specified below.

Fees

1.11. As from 1 April 1997, the Certification Body is required to charge for its services which hitherto have been provided free to CLEFs and Sponsors. Areas where fees will be 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.

Structure of Document

1.12. The document is organised as follows:

Chapter 1 provides an overview of the Scheme;

Chapter 2 describes the process whereby a commercial organisation can set up a CLEF;

Chapter 3 describes the appointment and assessment process for new CLEFs;

Chapter 4 identifies the rules pertaining to CLEF operation not directly covered by UKSP 01 [A] (such as

training of new staff);

Annexes A-C give details of the training and assessment of evaluators;

Annex D identifies the areas where fees are payable in respect of appointments and the certification of evaluations;

Annex E describes the various roles within the Certification Body;

Annex F contains a diagram of a suggested CLEF management structure;

Annex G contains a checklist for use in the application and set-up phase for a new CLEF;

Annex H contains an outline CLEF annual report.

Chapter 2. SETTING UP A CLEF

Basic Requirements and Criteria

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

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

1.15. A CLEF must be able to operate as an autonomous and self contained unit, separate from its parent company in all day to day operational and administrative aspects. It is thus able to conduct its business without the parent company being able to infer the identity of its Sponsors or their projects (special channels should be established as necessary to allow senior management of the parent company appropriate oversight of the CLEF's activities without compromising this general objective). Any arrangement that may compromise the above principles must be agreed by the Certification Body.

1.16. To this end a CLEF must be housed separately from its parent company, in a separate building or in an isolated wing or floor of the parent company's premises and must have:

a. sufficient office furniture and fitments for it to operate as a self-contained unit: a conference room, and normal office equipment, such as word processing facilities, photocopier etc;

b. its own administrative and clerical support;

c. its own telephone number.

1.17. In addition, a CLEF must meet the following basic requirements; it must have:

a. provision for a minimum of three separate evaluation cells, with room for expansion to at least six;

b. sufficient suitably qualified and experienced staff, as defined in Chapters 2 and 4;

c. its own computing equipment normally capable of supporting several evaluation tasks. Provision must also be made for additional small computers for task work, as required, and also for facilities to run special evaluation tools provided by the Certification Body, as required;

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

e. office space available for Certification Body staff, when required;

f. communications facilities enabling rapid exchange of information with the Certification Body and Sponsor (eg, fax);

g. archive facilities capable of meeting UKAS requirements.

1.18. A CLEF must be accredited as a testing laboratory by UKAS in accordance with the current NAMAS Accreditation Standard, M10 [D], and the NAMAS Regulations, M11 [E] and NIS35 [I], to perform all tests specified in the Schedule. See paragraphs 3.14-3.32 for more information.

1.19. A CLEF must meet the requirements of HMG's security manual "Manual of Protective Security" [J] and must meet all security requirements specified in paragraphs 2.18-2.35 below.

1.20. A CLEF must complete an appropriate level trial evaluation to demonstrate that:

a. the evaluators are technically competent as defined in paragraph 2.36;

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

Quality and Management

Management Objectives

1.21. 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

1.22. A CLEF must possess its own Quality Manual. Detailed guidance for the preparation of an appropriate Quality Manual which conforms to UKAS requirements can be found in

[G].

1.23. Particular attention must be paid to the maintenance of commercial confidentiality. For example, in describing the general arrangements for performing quality audits, the Quality Manual must specify the procedures whereby proprietary information belonging to CLEF Sponsors and the results of evaluation (in particular the nature of any vulnerabilities found during evaluation) are not released to inappropriate or unauthorised individuals or organisations. This aspect of CLEF security is known as "task confidentiality".

Specific Management Roles

1.24. A suggested management structure for a CLEF is described here, and shown diagrammatically in Annex F. Other structures will be acceptable, provided that they satisfy the management objectives; the following is therefore offered purely as a guide for new CLEFs.

1.25. 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.

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

1.27. A Computer Manager and Methods Adviser also report to the Technical Manager.

1.28. All clerical staff, such as receptionists and telephonists report to the Administrative Manager.

1.29. 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.

Security and Confidentiality

1.30. All CLEFs must be capable of performing evaluation tasks for HMG in addition to purely commercial work. They are therefore required to be set up and to operate in accordance with the requirements of HMG's security manual "Manual of Protective Security" [J].

1.31. "Manual of Protective Security" 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.

1.32. The requirements of "Manual of Protective Security" provide for the security of HMG Protectively Marked information.

1.33. All CLEFs must operate in such a way as to preserve strict commercial confidentiality. These security and task confidentiality requirements are specified in the following paragraphs.

The Security Manual

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

1.35. The Security Manual must set 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. It must specify procedures for:

a. Physical Security;

b. Personnel Security;

c. Information Security.

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

1.37. The Manual must 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.

Physical Security

1.38. The basic requirements for physical security are set out in paragraphs 2.1-2.5 and 2.7 above.

1.39. Each task must be carried out so that task material must be accessible only to authorised members of the task team. It is permissible to use the same area for more than one task at a time, provided that the same staff are involved in each task and that strict separation of material between tasks is enforced.

Personnel Security

1.40. CLEF staff will be subject to the Official Secrets Act and must 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. 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.

1.41. A CLEF must aim to become a stable unit with minimum turbulence of its staff. However, the Certification Body accepts that staffing levels may vary according to the CLEF's workload, and in the event of insufficient work such staff will be permitted to perform non-CLEF work for the parent company, subject to rules on commercial confidentiality stated in UKSP 01 [A] and paragraphs 4.16-4.21 of this document.

Information Security

1.42. 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 must also be made for processing material at high levels of Protective Marking if required to do so by a Sponsor.

1.43. Secure communications equipment, approved by CESG, may be needed for some tasks.

1.44. Provision must be made for the secure storage and archiving of magnetic media and documents. 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.

1.45. Certain tools and techniques used in CLEF work may be given a Protective Marking, and thus may not be used outside the CLEF or without the prior approval of the Certification Body.

1.46. At the termination of an evaluation task, all material supplied for that task must be disposed of, as agreed between the CLEF and the Sponsor: it may be retained by the CLEF or destroyed, sent to the Certification Body for their archives, or returned to the Sponsor. However, a record of all information relevant to the tests performed must be retained; under UKAS rules, such records must be retained for a period not less than six years. These records may be based on information contained in the evaluation deliverables list.

Task Confidentiality

1.47. The above measures contribute to the maintenance of task confidentiality. CLEFs may propose arrangements that preserve confidentiality, whilst allowing more efficient management of the work, to the Certification Body. Such proposals should also be acceptable to any Sponsors whose tasks may be involved.

Staff Qualifications and Training

Objectives

1.48. The training of evaluators has the ideal of producing qualified evaluators who:

a. understand the notion and principles of computer

security;

b. have a thorough understanding of the principles underlying the ITSEC [B];

c. can apply all criteria at any evaluation level specified in the conditions of appointment.

Evaluator Status

1.49. In practice, individual evaluators will have differing levels of expertise. The Scheme recognises three levels of qualification:

a. Trainee Evaluators, i.e. evaluators who have successfully completed an initial training programme;

b. Qualified Evaluators, i.e. Trainee Evaluators who have been assessed by the Certification Body to be capable of contributing to an evaluation without detailed supervision (see paragraphs 4.29-4.32);

c. Senior Evaluators, i.e. Qualified Evaluators who have been assessed by the Certification Body to be capable of successfully leading an evaluation targeted at any level of evaluation without supervision (see paragraphs 4.33-4.35);

1.50. In addition, there is a fourth category, Provisional Trainee, for those staff who have begun, but not yet completed, the initial training programme for qualification.

1.51. There are specific requirements on the composition of evaluation teams for them to be permitted to perform certain classes of evaluation work (see paragraphs 4.22-4.24).

1.52. The Certification Body holds a register of all evaluators of any status, including Trainee and Provisional Trainee. It should be noted, however, that the status of any evaluator (Trainee, Qualified or Senior), 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.

Initial Evaluator Training

1.53. Initial evaluation staff training is based on a set of four modules:

M1 - Basic Security Concepts

M2 - Evaluation Technical Approach

M3 - Planning and Tasking

M4 - External Authorities.

1.54. The objective of the initial training is to familiarise the course attendees with the principles of evaluation (both technical and managerial), the Scheme and the ITSEC.

1.55. Further details of the content of each module are given in Annex A. For new CLEFs, the training will be given under the supervision of the Point of Contact (see para 3.3), with assistance from other members of the Certification Body as appropriate. All evaluation staff in a new CLEF will be considered to be Provisional Trainees, unless they can demonstrate otherwise. Once an candidate evaluator has satisfactorily completed modules M1 and M2, he/she is deemed to be a Trainee Evaluator. Satisfactory completion of all four modules, together with relevant OJT experience, is required before a Trainee Evaluator can become a Qualified Evaluator. This will typically be at least six months after achieving Trainee status. Progress of the staff of a new CLEF will be monitored by the POC during the trial evaluation.

1.56. The evaluators who are to conduct the trial evaluation must attend at least the first two modules to attain Trainee Evaluator status.

Training for Senior CLEF Members

1.57. Senior members of a new CLEF (as detailed in paragraph 2.13 above) should also attend all relevant modules, or should have equivalent experience. Those senior managers involved in the technical work, including technical reviews, must attend all training modules.

The Trial Evaluation

1.58. The purpose of the trial evaluation is to demonstrate to the Certification Body that the CLEF is competent to perform evaluations preferably up to ITSEC Assurance Level E3 or Common Criteria EAL4 and hence to hold a Full Appointment. It is also used as a basis for UKAS assessment. Details are contained in Annex B.

This page is intentionally left blank

Chapter 3. APPOINTMENT AND ASSESSMENT FOR NEW CLEFS

Introduction

1.59. 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.

1.60. 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

1.61. 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 to the granting of a Full Appointment, and thereafter for dealing with the CLEF during the early years of its membership of the Scheme.

1.62. 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

1.63. An applicant company applies to the Certification Body for a Provisional Appointment. It may do this at any time on its own initiative or in response to a general invitation to industry from the Certification Body.

1.64. The applicant company submits 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.

1.65. 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

1.66. 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.

1.67. 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.

1.68. 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.

1.69. 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. He will be accompanied during the preliminary visit by other members of the Certification Body, as required.

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

Initial Training

1.71. The initial training programme outlined in paragraphs 2.36 to 2.45 above should 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

1.72. A CLEF will be assessed for two categories of UKAS test laboratory accreditation, namely:

Category 0 Permanent laboratory (the CLEF) where the testing facility is erected on a fixed location for a period expected to exceed three years.

Category 1 Site testing performed by staff sent out on site by a permanent laboratory that is accredited by UKAS.

1.73. A CLEF is required to be accredited to both categories to perform the tests specified in the Schedule. Category 1 accreditation is a separate accreditation from Category 0 accreditation which must be granted before the former is awarded.

1.74. The criteria to be met for Category 0 accreditation is described in [D] and [E]. Category 1 criteria is documented in a further UKAS publication [H]. An interpretation of the accreditation requirements can be found in NIS35 [I].

Schedule of Accreditation

1.75. The evaluations performed by a CLEF, and the evaluation technical reports they produce, must 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 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.

1.76. The scope of accreditation includes the use of the ITSEC [B] and ITSEM [C]. 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.

1.77. It is not possible to accredit all tests performed by a CLEF, as some aspects of security testing are not completely objective. Such aspects mainly arise in the "effectiveness" criteria of the ITSEC [B], which are less mature than other aspects of evaluation. Reducing the subjectivity in testing for these criteria in particular, is addressed in the IT Security Evaluation Manual (ITSEM) [C].

1.78. Any further development of the ITSEC and ITSEM will directly address the issue of objectivity in security testing, but some subjectivity is likely to remain. The interpretation of these subjective elements is carried out by the Certification Body to ensure uniformity and correctness of evaluation procedures and consistency and compatibility in the reporting of evaluation results.

1.79. 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 both

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.

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

1.81. 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.

1.82. It is likely that the changes to the Schedule can be handled as part of extended surveillance or reassessment visits conducted by UKAS (paragraphs 4.41-4.46).

Application for UKAS Accreditation

1.83. Before the trial evaluation can commence, the CLEF should make a formal application to UKAS for accreditation as a testing laboratory. 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.

1.84. The CLEF should complete UKAS form MF101 and forward this, together with a copy of the Quality Manual and the application fee, to the UKAS Executive. A copy of the CLEF Quality Manual and CLEF Security Manual should be sent to

the Certification Body once UKAS accreditation is requested.

1.85. 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

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

1.87. UKAS assessments of CLEFs will be conducted by fully trained UKAS assessors, who will be tasked by UKAS specifically for the purpose. The assessors will be civil servants having 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. Also, the POC will not be involved in the assessment.

1.88. Category 0 and Category 1 accreditation is necessary for a full CLEF appointment and must therefore 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 object of reducing duplication of effort as far as possible.

1.89. 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

1.90. The CLEF should carry out the trial evaluation in accordance with Annex B. 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

1.91. Following the UKAS assessment, the CLEF is required to complete the trial evaluation. In particular a certifier will be tasked with considering the Evaluation Technical Report in detail and whether the conduct and conclusions of the evaluation were in accordance with the rules of the Scheme and ITSEC [B]. 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

1.92. A checklist for use with the above procedures can be found at Annex G.

This page is intentionally left blank

Chapter 4. CLEF OPERATION

Introduction

1.93. 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.

1.94. Each CLEF must 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

1.95. A CLEF works under appointment from the Certification Body, and thereby has access to certain Protectively Marked tools, techniques, and information, as well as considerable technical and other support from the latter. Because of this, it is necessary to maintain very close cooperation between the Certification Body and each CLEF, to ensure that the evaluation tools, techniques and information are confined to proper and controlled use within the evaluation community and are appropriately protected. Equally 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 compliance with the requirements of "Manual of Protective Security" [J].

Certification Body Roles

1.96. In order to facilitate management of contacts with CLEFs, roles have been defined within the Certification Body, to which particular types of contact can be directed. These roles are specified in Annex E.

General Liaison

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

Business Liaison

1.98. The Deputy Head of the Certification Body provides a link between prospective CLEF customers and the CLEFs. To

facilitate this, each CLEF must provide him with regular business reports (including prospective business). Such reports will be treated in the utmost confidence, and which will ensure 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 in UKSP 05 [K].

Advertisements and Publicity

1.99. 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 Certification Body's Publicity Officer for prior approval. The Publicity Officer will normally give a response within ten working days.

Meetings

CLEF Progress Meetings (CPM)

1.100. CLEF Progress Meetings will be held at agreed regular intervals. 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 representatives of the Certification Body. The CLEF will submit the required copies of the CLEF Progress Report to the CB Secretary at least ten working days before the meeting.

Evaluation Progress Meetings (EPM)

1.101. Evaluation Progress Meetings are called at the discretion of the Certification Body, the CLEF or the Sponsor, for the purpose of reviewing progress on a particular evaluation task; prior to the meeting the CLEF will issue the meeting agenda. The Certifier may comment on the agenda and may attend the meeting.

Evaluation Control Meetings (ECM)

1.102. Evaluation Control Meetings are called at the discretion of the Certification Body or the CLEF for the purpose of discussing detailed technical work relating to a particular evaluation. In exceptional circumstances, the Sponsor may be invited to attend.

Other Meetings

1.103. 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, 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 require to be present for discussion of financial aspects of such contracts.

Annual Meetings

1.104. Annual Meetings are held to review the year's work in the CLEF. The CLEF will submit an Annual Report to the Head of the Certification Body at least 10 working days before the meeting.

CLEF Controllers' and Technical Managers' Meetings

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

Joint Technical Reviews

1.106. In addition to those meetings already described, which relate to the business and organisation of the CLEF and to specific evaluations, the Certification Body will arrange, periodically, Joint Technical Reviews. These meetings provide a forum for the exchange of information and views on any aspects of evaluation. They contain presentations both from evaluators and from members of the Certification Body on topics of general interest to the evaluation community. They may be attended by staff from any CLEF. The agenda for each meeting is the responsibility of the Certification Body but CLEFs are invited to contribute both in suggesting topics of interest and in making presentations.

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

The Conduct of Evaluations

Commercial Impartiality

1.108. It must be 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 an evaluation.

1.109. In no circumstances 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.

1.110. Subject to the above, CLEF staff may provide consultancy advice about ITSEC deliverables to the Sponsor and the Developer. Notwithstanding the wording in the ITSEC (paragraphs 0.11, 1.29, 3.12, 3.29, etc.) and ITSEM (paragraphs 4.2.23 etc.) the CLEF evaluation team may produce the detailed design and effectiveness deliverables as part of the evaluation process, where this will help their understanding of the TOE, for systems which are for HMG use only and are not subject to any mutual recognition process.

1.111. In particular, teams and individuals should not have the same immediate manager as the development team. Independence will be questioned if it is apparent that a manager may be able to influence decisions between development on the one hand and evaluation on the other.

1.112. 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 for a particular TOE where the CLEF has also provided part or all of the Developer Security Analyst 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.

1.113. In general, a CLEF may not evaluate the work of any group or division within the parent company to which it belongs. This rule may be relaxed at the discretion of the Certification Body where the CLEF can satisfactorily demonstrate that the independence of the evaluation can be maintained and the creditability of the Scheme will not be harmed. The CLEF must submit a formal application in each case. Examples where this rule has been relaxed in the past have been confined to Government Systems and more rarely to specialised products for use in Government Systems.

Evaluator Teams

1.114. The ratio of Trainee Evaluators to Qualified or Senior Evaluators on any evaluation should not exceed 3:1.

1.115. Evaluations at the ITSEC E4 Assurance Level or Common Criteria EAL5 and higher must have a Senior Evaluator in the team; preferably this Senior Evaluator should be the Task Leader.

1.116. In exceptional circumstances these rules may be relaxed at the discretion of the Certification Body who may then require additional safeguards to maintain the appropriate standards of work. However, with respect to paragraph 4.22, the CLEF must ensure that it upholds UKAS rules regarding the use of Trainee Evaluators, namely:

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.

Other CLEF Work

1.117. The primary purpose of a CLEF is to perform security evaluations in accordance with the Scheme. However, the Certification Body may authorise the parent company of the CLEF to do similar work, such as safety evaluations or other security work not directly related to the Scheme, which may employ CLEF staff or make use of CLEF resources. The parent company may do this, but only with prior written authorisation of the Certification Body. As a minimum the identity of the client and an outline of the proposed work should be provided.

1.118. Such authorisation will not be unreasonably withheld.

Training

Status of Evaluators

1.119. 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 regain his/her status as a qualified or senior 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 Compusec 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 below (Paragraphs 4.29. to 4.36.).

1.120. 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.

Attaining Qualified Evaluator Status

1.121. Evaluation Staff new to an existing CLEF must follow a training programme approved by the Certification Body, and based on the modules detailed in Annex A. The training will normally be supervised by the CLEF Technical Manager, who will provide a statement to the Certification Body in support of any request for a change of evaluator status.

1.122. This semi-formal training programme is supported by on-the-job training, which involves the Trainee Evaluator or Provisional Trainee participating in a real evaluation. Trainee Evaluators who are put forward as being suitable for Qualified status are assessed by the Certification Body to determine if they have reached the necessary standard. Assessment is performed:

a. following positive recommendation by the CLEF management (normally the Technical Manager);

b. by consideration of written reports produced by the candidate as part of his/her on-the-job training (Annex C).

1.123. At its discretion, the Certification Body may subject the Trainee Evaluator to an oral examination. It is also possible that the Trainee Evaluator will come into contact with representatives of the Certification Body through the normal course of evaluation work. In such cases, any impression of the Trainee Evaluator's technical abilities formed, for example by the certifiers, may also be taken into account.

1.124. More than one evaluation is likely to be needed to successfully complete the OJT element of the training programme.

Attaining Senior Evaluator Status

1.125. Qualified Evaluators will continue to gain experience as a natural consequence of their evaluation work; accumulation of such experience will contribute towards their eventual recognition as Senior Evaluators.

1.126. Following positive recommendation by the CLEF management, the Certification Body will, at its discretion, admit the evaluator to its register of Senior Evaluators. The Certification Body must be satisfied that the

evaluator can personally apply all evaluation criteria as defined by the ITSEC E4 or Common Criteria EAL5 Assurance Level. This will normally mean that he/she has led, or played a significant role in, at least three evaluation tasks (preferably at E3 or EAL4 and above), one of which should, if possible, have been a system.

1.127. In making its assessments, the Certification Body may take account of the candidate's involvement in security evaluations performed to other criteria and schemes, development, research, publications and other such work as it deems relevant.

Training of Senior CLEF Staff

1.128. Senior CLEF staff, such as the CLEF Controller, and Business Manager are normally expected to be familiar with the content of the initial training programme, and should have attended all relevant modules. The Technical Manager, and any others involved with the technical work, including technical reviews, must have attended all training modules.

Trainers

1.129. Staff experienced in security evaluations may be nominated as trainers who are qualified to present and maintain the CLEF training courses. Trainers shall be registered with and approved by the Certification Body.

CLEF Staff Changes

1.130. The Certification Body should be notified of all CLEF staff changes via the CLEF Progress Report (see paragraph 4.6). 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

1.131. All evaluation staff who have not previously worked for a CLEF should be notified to the Certification Body prior to assignment to an evaluation and preferably prior to recruitment into the CLEF. Notification can be given by letter to the CB Technical Officer or at a CLEF Progress Meeting if such a meeting is imminent.

Staff Rejoining the CLEF

1.132. 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

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

1.134. 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.

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

1.136. Surveillance and reassessment visits for Category 1 accreditation may be carried out on different days from that for Category 0, and will involve the assessors accompanying the evaluators on a site visit.

1.137. 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 agreement between the Certification Body and UKAS on the scope of the extended Schedule.

1.138. 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 may make arrangements with UKAS to take the 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

1.139. 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

1.140. 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 with the provisions of "Manual of Protective Security" [J].

1.141. Normally, the Certification Body provides at least 6 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.

1.142. 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 fulfill 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.

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

Disputes

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

1.145. 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 Management Board.

1.146. An appeal hearing will be held by the Management Board that will consist of the joint Chairmen and at least three members. In attendance will be the Senior Executive, the Head of the Certification Body and representatives of the CLEF.

This page is intentionally left blank

Annex A. INITIAL TRAINING PROGRAMME

Objectives

1.1. The objectives of the initial training programme are:

a. to familiarise students with basic security principles, the Scheme and the ITSEC [B];

b. to introduce the practices of the UK technical approach to evaluation, as interpreted from the ITSEM [C] and approved for use under the Scheme;

c. to describe the procedures to be adopted when conducting evaluations under the Scheme and to describe the 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.

Scope of the Programme

1.2. The initial training programme must cover all aspects of the evaluator's activities. CLEFs may choose the method of presentation of the material, which may be done in formal classroom environments, and informal sessions. The material covered should follow the syllabus below. For formal sessions, a modular approach may be best. To assist this, and to provide a basic training framework, four such modules have been identified:

M1 - Basic Security Concepts

M2 - Evaluation Technical Approach

M3 - Planning and Tasking

M4 - External Authorities.

CLEF Training Staff

1.3. The staff used by CLEFs for the delivery of training material must be approved by the Certification Body.

1.4. A CB-agreed basic subset of M1 and M2 should be presented to new evaluation staff on entry. The CLEF should submit evidence of this training for each new entrant to enable the Certification Body Technical Officer to grant Provisional Trainee status. Further evidence is required to show that the remainder of M1 and M2 has been provided within 3 months of the start of training. Satisfactory

evidence will result in the confirmation of Trainee status, which in turn means that they can be used on commercial evaluation work subject to the conditions given in paragraphs 4.22-4.24.

1.5. M3 and M4 (or equivalent) may be delayed until the Trainee Evaluator has gained some experience through on-the-job training (see Annex C) or, in the case of a new CLEF, until the Trainee Evaluator has gained some experience through his/her involvement with the trial evaluation (see Annex B). A Trainee Evaluator must, however, receive training on all aspects of the programme before he/she can be put forward for consideration as a Qualified Evaluator.

Syllabus

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

M1 - BASIC SECURITY CONCEPTS

1.7. This module addresses objective (a): basic security concepts, the Scheme, the ITSEC, and the Common Criteria. This module comprises:

a. the requirement for secure systems and products, and their general characteristics;

b. assurance, confidence, evaluation levels, correctness and effectiveness, the ITSEC, the Common Criteria and other criteria;

c. the Scheme;

d. evaluation facilities, security procedures, confidentiality;

e. protection profiles, security targets, security policies (SSP, SEISP, SISP), security policy models, security enforcing functions, claims language documents.

M2 - EVALUATION TECHNICAL APPROACH

1.8. This module addresses objective (b): the practices of the UK technical approach to evaluation. This module comprises:

a. evaluation philosophy, test method suitability (objectivity, repeatability, reproducibility, impartiality);

b. systems and products;

c. evaluator actions, application of criteria, assigning

verdicts.

M3 - PLANNING AND TASKING

1.9. This module addresses objective (c): the procedures to be adopted when conducting evaluations under the Scheme and the planning, organisation and management of evaluation tasks. This module comprises:

a. CB organisation, evaluation management, document control, report handling;

b. tasks, evaluation jobs, work packages, reporting of results.

M4 - EXTERNAL AUTHORITIES

1.10. This module addresses objective (d): the organisations which are involved in the sponsorship, evaluation, certification, and system accreditation process and background information needed to ensure efficient and successful evaluation. This module comprises:

a. sponsorship process as seen and contrasted for HMG procurement and commercial sponsorship;

b. HMG procurement process, roles of developer and project office, accreditor, consultancy;
c. commercial evaluation process for products and systems;

d. relationship with other Certification Bodies;

e. the role of UKAS, significance of UKAS accreditation, obligations of CLEF staff.

1.11. Training material, in the form of viewfoils and notes, is promulgated by the Certification Body from time to time. There may thus be some slight variation from the above syllabus.

1.12. 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.

1.13. Where changes to the Scheme a promulgated by means of a SIN then 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. As an approximately annual exercise, there will be a review of the training material in which the effects of all SINs will be considered.

1.14. 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 a SOR should be raised 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 in the form of a SIN; however if the problem is minor then corrective action will be taken during the review and update exercise referred to above.

Conduct

1.15. 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 then current M1-M4 kernel, available from the Certification Body.

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

1.17. CLEFs must notify the Certification Body, no less than one week in advance, of their intention to run training courses. The Certification Body may send staff to such courses, either to monitor their conduct or to receive training.

Charges

1.18. Where CLEFs present courses for other CLEFs, they may make an appropriate charge for their services.

This page is intentionally left blank.

Annex B. TRIAL EVALUATION

Purpose

1.19. 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 the Schedule for Category 0 and Category 1 accreditations.

Objectives

1.20. 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 fulfill its role in supporting an evaluation.

1.21. The trial evaluation covers all the areas associated with the on-the-job training of Trainee evaluators in a newly established CLEF (see Annex C). 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

1.22. 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.

1.23. 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. The preference of the Certification Body is for a product at the ITSEC E3 or Common Criteria EAL4 Assurance Level. However, to satisfy the requirements for Category 1 accreditation it is essential that the evaluation has an element of on-site work.

1.24. 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 used: 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.

1.25. 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 Category 0 and Category 1 Schedule (see paragraphs 3.18-3.20).

1.26. 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.

1.27. The trial evaluation will be performed under CLEF management but under the technical direction of a Certification Body 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 the POC who will be permitted to lead by example. As it proceeds, the CLEF will be expected to require significantly less supervision.

1.28. 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.

1.29. 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.

Assessment

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

a. the planning of the evaluation;

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.

1.31. While some of these areas will be covered by UKAS assessment, the Certification Body will avoid duplication of effort as far as possible.

1.32. 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 Evaluators. 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.

1.33. 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

1.34. 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 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.

Annex C. ON-THE-JOB TRAINING OF TRAINEE EVALUATORS

Introduction

1.35. On-the-job training is the primary means by which evaluators acquire their skills.

1.36. Following completion of an initial training programme, Trainee Evaluators and Provisional Trainees undergo on-the-job training on real evaluations under the direction of Qualified Evaluators. They need to be given experience of all aspects of evaluation before they can be recommended to the Certification Body for consideration as Qualified Evaluators. Their work on these evaluations will be offered in support of such a recommendation.

Scope of Training

1.37. There is no specific number of evaluations, nor specific time period for qualification as evaluator. Trainee Evaluators are required to demonstrate competence in all aspects of evaluation. They should, therefore, be given sufficient opportunity to allow them to gain experience and to demonstrate their competence.

1.38. 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 ITSEC or Common Criteria by their application in a real evaluation;

b. have experience of the following:

i. examination of documentation including "requirements" documents such as SSPs, SEISPs, SISPs and Product Security Targets;

ii. performance of all evaluator actions required for an E3 or EAL4 evaluation. This may be as a result of involvement in several evaluations;

iii. examination of the development environment of at least one product or system;

iv. examination of the operational environment and documentation of at least one product or system;

v. have experience in the planning and conduct of 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;

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.

1.39. If a single evaluation cannot provide a trainee with timely experience of all these aspects of evaluation then that trainee may be assigned to work on two or more different evaluations in order to gain the required experience.

Assessment

1.40. Assessment will be performed:

a. following a positive recommendation by the CLEF management and

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

1.41. In addition, the Certification Body may subject the trainee to an oral examination and may monitor the progress of the trainee as necessary to determine his/her fitness to be a Qualified Evaluator.

Written Reports

1.42. The CLEF must identify written reports which are independently produced by the trainee. These reports should demonstrate the trainee's understanding of the ITSEC, Common Criteria or ITSEM 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 C.4 above.

1.43. 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 assessment. In this case there must be clear indication that the trainee understands how the work that he/she has described fits into the overall work of the evaluation.

Annex D. ASSESSMENT AND OTHER FEES

Introduction

1.44. From 1 April 1997 the Certification Body is required to cover its costs. The paragraphs below indicate areas where fees will be raised. Such fees will apply to all Certification Body work undertaken from 1 April 1997. Certification Body work completed by 31 March 1997 will not attract a fee. Fees will not be refundable.

Fee For Help With Setting Up a New CLEF

1.45. 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.

1.46. 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

1.47. 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 but will not implement this on 1 April 1997. The fee would amongst other things cover all documentation updates.

Certification Fees

1.48. A fee for Certification Body services will normally be levied directly on the sponsor for each evaluation (or re-evaluation) and for certificate maintenance.

UKAS Fees

1.49. UKAS charges a fee for its accreditation services, details of which are available from the UKAS Executive.

Training Fees

1.50. 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.

This page is intentionally left blank

Annex E. CERTIFICATION BODY ROLES

Introduction

1.51. A number of roles exist within the Certification Body to assist in the appointment and operation of CLEFs. These are detailed below.

Senior Executive

1.52. The Senior Executive reports to the Management Board and is responsible for:

a. directing and coordinating all management policies and actions of the Certification Body;

b. making efficient and effective use of resources (staff, material and financial);

c. ensuring the smooth running of the Certification Body;

d. allocating appropriate responsibilities and authorities for all Quality Management System matters;

e. reporting on the progress of the Scheme and Certification Body to the Management Board and its constituent members;

f. keeping abreast of changes of UK policy, and of the policies and methodologies of the Scheme's European and international partners, so that the impact upon the Scheme can be correctly assessed;

g. maintaining liaison at a high level with major users, vendors and those who influence the Scheme so that their views can properly be reflected in its development.

Head of the Certification Body

1.53. The Head of the Certification Body reports to the Senior Executive and is responsible for:

a. management of Certifiers, the Appointment Officer and administrative staff;

b. liaison with Technical Officer and Deputy Head of Certification Body to ensure smooth running of the Certification Body;

c. co-ordination of speedy handling of time-sensitive reports and documents from the CLEFs and the Certification Body;

d. provision of certification advice to evaluators and

other customers;

e. assignment of Certifiers to evaluation tasks and review panels;

f. monitoring and supervision of the conduct of CLEF work to ensure consistency of methodology and procedures, including attendance at regular CLEF Progress Meetings;

g. support the Quality Manager in the provision and maintenance of the Quality Management System;

h. co-ordination of Mutual Recognition with other Certification Bodies;

i. collection of information to permit the raising of certification fees.

Deputy Head of the Certification Body

1.54. The Deputy Head of the Certification Body reports to the Senior Executive and is responsible for:

a. management of publicity staff;

b. liaison with Head of the Certification Body and Technical Officer to ensure smooth running of the Certification Body;

c. liaison with CLEFs to provide business contacts from industry and HMG projects;

d. maintenance of Certification Body awareness of CLEF business, including attendance at regular CLEF Progress Meetings;

e. authorisation of proposed press releases by Sponsors, articles by CLEF staff which relate to the Scheme and entries for the Certified Products List, UKSP 06 [M];

f. co-ordination of Scheme promotion or certificate presentation matters;

g. providing first point of contact for press enquiries;

h. support the Quality Manager in the provision and maintenance of the Quality Management System.

Technical Officer

1.55. The Technical Officer reports to the Senior Executive and is responsible for:

a. management of Methodology Officers, the Tools Advisor and Training Officer;

b. liaison with Head of the Certification Body and Deputy Head of Certification Body to ensure smooth running of Certification Body;

c. provision of technical evaluation advice on methodology, tools and training;

d. confirmation of evaluator status and maintenance of a status register;

e. maintenance of a database containing publicly-known product vulnerabilities in IT products;

f. support the Quality Manager in the provision and maintenance of the Quality Management System.

Quality Manager

1.56. The Quality Manager reports to the Senior Executive and is responsible for:

a. provision and maintenance of the Certification Body Quality Manual;

b. provision and maintenance of Certification Body Quality Procedures and Certification Body Operating Procedures;

c. monitoring the effectiveness of the Certification Body Quality Management System, including making improvements where necessary;

d. organisation of Quality Audits and ensuring the implementation of any necessary remedial action;

e. reporting on the status and performance of the Quality Management System, and advising of any need for change;

f. recording and investigating complaints about the quality of service provided by the Certification Body.

Certifier

1.57. Certifiers report to the Head of the Certification Body and are responsible for:

a. providing Technical Assurance by monitoring the technical conduct and progress of CLEF evaluations;

b. production of Letters of Intent and/or Interim Certification Statements as necessary;

c. production of Certification Reports on completion of an evaluation task;

d. advising sponsors on security and/or Scheme documentation and evaluation/re-evaluation approach;

e. advising sponsors on the Certificate Maintenance Scheme;

f. reviewing Scheme, national and international documentation relating to evaluation and certification issues;

g. producing SORs and SINs as required;

h. reporting of CLEF anomalies to the Appointment Officer.

Deputy Certifiers

1.58. Deputy Certifiers report to the Head of the Certification Body and are responsible for:

a. providing a second independent opinion on the technical conduct and progress of CLEF evaluations;

b. deputising for the Certifier should the need arise.

Appointment Officer

1.59. The Appointment Officer reports to the Head of the Certification Body and is responsible for:

a. liaison with potential CLEFs, and processing of applications for the appointment of a CLEF;

b. monitoring the setup phase of new CLEFs in conjunction with the Methodology Officer, Point of Contact, and Training Officer;

c. issuing of CLEF Appointments (Provisional or Full) prior to or on completion of UKAS assessment;

d. where appropriate, updating CLEF Appointments following UKAS surveillance and reassessment visits;

e. reviewing the scope of CLEF Appointments to ensure currency of methods, techniques, tasks, accreditation schedules and criteria;

f. in conjunction with Certifiers and Points of Contact, monitoring CLEFs to ensure that they operate within the scope of their Appointment;

g. recording and handling of CLEF anomalies, including withdrawal of CLEF Appointments if necessary.

Training Officer

1.60. The Training Officer reports to The Technical Officer and is responsible for:

a. liaison with potential CLEFs until a Provisional Appointment has been appointed, to provide day-to-day technical support for a trial evaluation;

b. maintenance of training material and monitoring CLEF evaluator training.

Point of Contact (POC)

1.61. The CLEF Point of Contact reports to the Head of the Certification Body and is responsible for:

a. liaison with a specific CLEF on general Scheme issues;

b. provision of liaison for task issues in the absence of the Certifier appointed to that task;

c. chairing CLEF Progress Meetings;

d. reporting of CLEF anomalies to the Appointment Officer;

f. production of SORs resulting from CLEF liaison issues.

Scheme Administrator

1.62. The Scheme Administrator reports to the Head of the Certification Body and is responsible for:

a. supervision of Certification Body clerical staff;

b. provision of administrative support to all Certification Body staff;

c. registering new tasks and providing management information on the current status of tasks;

d. ensuring that evaluation deliverables, reports and other Scheme documents are properly handled, forwarded or stored;

e. ensuring that all CLEFs receive Scheme information produced or distributed by the Certification Body;

f. maintenance of databases as specified in Certification Body Quality Procedures;

Publicity Officer

1.63. The Publicity Officer reports to the Deputy Head of the Certification Body and is responsible for:

a. provision of point of contact for all general enquiries about the Scheme and requests for further information;

b. organising venues for Scheme presentations and seminars and provision of administrative backup;

c. represents the Scheme at exhibitions, conferences and other venues;

d. vetting of press releases regarding the Scheme;

e. producing updates to, or re-issues of, the Certified Product List, UKSP 06 [M];

Tools Advisor

1.64. The Tools Advisor reports to the Technical Officer and is responsible for:

a. development and support of tools and other working aids for the evaluation/certification process;

b. management of contracts for the supply of tools and in-house support of Certification Body databases;

c. co-ordination of Certification Body computing facilities.

Methodology Officer

1.65. The Methodology Officer reports to the Technical Officer and is responsible for:

a. management of contracts used to employ CLEFs and other contractors on methodology tasks;

b. production and control of the Scheme Evaluation Manual (UKSP 05);

c. production and control of Scheme Information Notices (SINs);

d. technical involvement in leading edge evaluations;

e. Certification Body lead on national and international changes to criteria and methodology;

f. harmonisation of criteria with North America;

g. organisation of Scheme Joint Technical reviews;

h. technical advisor for Evaluation Induction Course;

i. registering and handling of SORs;

j. methodology advice to CLEFs, including attendance at CLEF Progress Meetings;

k. monitoring trial evaluations during CLEF setup phase in conjunction with the Appointment Officer, providing day-to-day technical support as required.

Internal Quality Auditor

1.66. The Internal Quality Auditor reports to the Quality Manager and is responsible for:

a. performing audits in accordance with defined procedures;

b. assessing each noncompliance as significant or non-significant;

c. documenting the results of the audits and bringing them to the attention of the Quality Manager and the staff having responsibility in the area audited.

Document Controller

1.67. The Document Controller reports to the Deputy Head of the Certification Body and is responsible for:

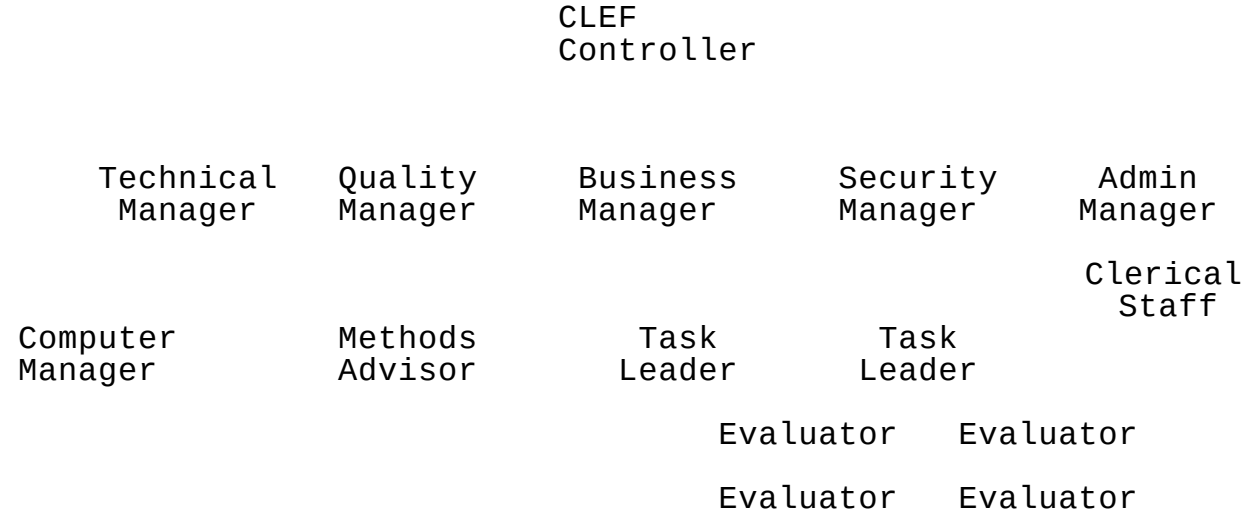
a. maintaining an up to date register of documents;

b. holding master copies of forms, manuals and publications and any other standard documents;

c. issuing and withdrawing all Certification Body specific forms.

ANNEX F. SUGGESTED CLEF MANAGEMENT STRUCTURE & TERMS OF REFERENCE

1.68. The following diagram illustrates the organisational structure described in Chapter 2.



Terms of Reference

1.69. Whilst the precise terms of reference for each of the above roles is a matter for the CLEF's company, the following notes indicate the general areas of responsibility involved.

CLEF Controller

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

Technical Manager

1.71. 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.

Quality Assurance Manager

1.72. The Quality Assurance 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

1.73. 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.

Administration Manager

1.74. 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.

Security Manager

1.75. The Security Manager is responsible for the physical and document security aspects of CLEF operation. This post liaises with the Government Departments responsible for overseeing compliance with "Manual of Protective Security". Any CLEF Security Guards report to the Security Manager.

Computer Manager

1.76. 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

1.77. The Methods Advisor provides advice and guidance on the use of the evaluation methodology within the CLEF. This post will liaise with the Certification Body Technical Officer on methodology aspects of the CLEF's operations.

Task Leaders

1.78. 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 are adequately trained for the work involved. They are responsible for all reports produced as a result of the evaluation.

Annex G. CHECKLIST FOR USE WITH THE APPLICATION AND SET-UP PROCESS

1.79. 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

1.80. Is the CLEF an autonomous unit within the Company ?

1.81. Is it a physically self-contained unit ?

1.82. What is the Company's management structure ?

1.83. Has it sufficient furniture, etc. to operate ?

1.84. Has it its own administrative and clerical support ?

1.85. Has it its own telephone/fax number ?

1.86. Has it provision for separate evaluation cells ?

1.87. Has it sufficient computer equipment to support evaluation tasks ?

1.88. Are the requirements of "Manual of Protective Security" met ? When was its security status granted ? When was it last reviewed ?

Quality Manual

1.89. Is there a Quality Manual ?

1.90. Does it conform to UKAS requirements ?

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

Management Roles

1.92. Who is the CLEF Controller ?

1.93. Who is the Technical Manager ?

1.94. Who is the Quality Assurance Manager ?

1.95. Who is the Business Manager ?

1.96. Who is the Administration Manager ?

1.97. Who is the Security Manager ?

1.98. Is there a Computer Manager ?

1.99. Is there a Methods Adviser ?

1.100. Does any individual undertake more than one role ? Is there any possibility that the effective performance of these roles could suffer as a result ?

Security and Confidentiality

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

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

1.103. Are CLEF staff positively vetted ? To what level ?

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

1.105. What are the arrangements for maintaining task confidentiality ?

Evaluator Status and Training

1.106. What is the Evaluator status of CLEF staff ?

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

Provisional Appointment

1.108. Has a formal application been made for a Provisional Appointment ?

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

Preliminary Meeting

1.110. Has the Preliminary Meeting been held ?

Initial Training

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

UKAS Accreditation

1.112. Has formal application been made to UKAS for accreditation as a testing laboratory ?

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

Trial Evaluation

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

1.115. Has this been agreed by the Certification Body ?

1.116. How far has the trial evaluation progressed ?

Annex H. CLEF ANNUAL REPORT

Introduction

1.117. CLEF Appointments are reviewed by the Certification Body annually. Prior to each annual meeting (see Paragraph 4.12), the CLEF is required to submit an Annual Report to the Head of the Certification Body. This report provides a summary of CLEF activities and significant events over the report period. It also provides the CLEF with an opportunity to outline future plans and to raise any issues and concerns relating to the operation of the Scheme. The content and suggested format of the CLEF annual report is as follows:

Introductory material / document preamble.

MANAGEMENT SUMMARY / HIGHLIGHTS

Summary Report highlighting any key issues contained in the remainder of the report.

TECHNICAL REPORT

General summary of CLEF work and staff allocation
A summary of any pre-evaluation consultancy activities
A summary of any non-Scheme work being conducted by the CLEF

COMMERCIAL / MARKETING

Any issues / concerns the CLEF wishes to highlight concerning commercial and marketing aspects of CLEF business and the Scheme in general.

APPOINTMENT ISSUES

Any issues/concerns that the CLEF wishes to raise concerning CLEF Appointment.

SCHEME ISSUES

Any issues/concerns that the CLEF wishes to raise concerning the Scheme, for example:
- uptake of the Scheme;
- Mutual Recognition;
- new CLEFs;
- Scheme publicity.

UKAS ISSUES

Any issues/concerns that the CLEF wishes to raise concerning UKAS Accreditation.

MANAGEMENT AND ADMINISTRATION

Any future plans or potential problems, for example:
- accommodation;
- security and confidentiality;
- certification Body liaison;
- relationship with parent company;
- any issues that may effect independence and impartiality.