



**UK IT SECURITY EVALUATION
AND CERTIFICATION SCHEME**

UK Scheme Publication No 1

DESCRIPTION OF THE SCHEME

**Issue 6.3
December 2009**

© Crown Copyright 2009 – All Rights Reserved

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

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

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

FOREWORD

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

This document provides a high level description of the Scheme and the procedures applied under it. Other documents of the Scheme must be referred to for greater detail. It is intended for use by potential customers, i.e. anyone concerned with the development, procurement or accreditation of IT systems or products in which security is a consideration, as well as those already involved in the Scheme, i.e. Scheme employees, current customers, contractors and security consultants.

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 and Certification Scheme
Description of the Scheme**

AMENDMENT RECORD

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

Issue Number	Major Changes	Date
6.0	Version for use with revised certification processes. (Issue 5.0 remains applicable for applications that still use the previous certification processes.)	July 2005
6.1	Clarification of appeals procedure. Note that only documentation related to CC evaluation will be made available on the CESG website.	March 2006
6.2	Refinements and clarifications; including MRA aspects and Task Startup Reviews.	October 2008
6.3	Minor changes for clarification.	December 2009

**UK IT Security Evaluation and Certification Scheme
Description of the Scheme**

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 and Certification Scheme
Description of the Scheme**

CONTENTS

I. OVERVIEW OF THE UK SCHEME	1
Introduction	1
IT Security Evaluation and Certification	2
The Scheme.....	2
Evaluation Criteria and Methodology	3
Security Targets.....	4
Protection Profiles	4
Mutual Recognition	4
II. ORGANISATION AND MANAGEMENT	6
Introduction	6
Senior Management Team.....	6
Certification Body	6
CLEFs	6
Sponsors	7
Developers	7
Vendor	7
Procurement Body	7
Accreditor	7
Evaluation and Certification Processes.....	7
Appeals Procedure.....	8
III. PREPARATION	9
Introduction	9
Task Startup Review	9
TOE Scope Information.....	10
Evaluation Work Programme	10
Certification Work Programme	11
Deliverables	11
Security Target.....	11
Protection Profile.....	12
Formal Acceptance of Evaluation.....	12
IV. EVALUATION AND CERTIFICATION	13
Introduction	13
Evaluation Work.....	13
Evaluation Progress Reviews.....	13
Evaluation Technical Report	14
Certification Report and Certificate	15
V. ASSURANCE MAINTENANCE	16
Introduction	16
Assurance Maintenance.....	16

UK IT Security Evaluation and Certification Scheme Description of the Scheme

(This page is intentionally left blank¹)

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

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

I. OVERVIEW OF THE UK SCHEME

Introduction

1. The UK IT Security Evaluation and Certification Scheme (referred to as 'the Scheme' in this document) was established in December 1989 by Her Majesty's Government (HMG) to evaluate and certify the trustworthiness of security features in Information Technology (IT) products and systems². It also provides a framework for assurance continuity and the international mutual recognition of such certificates.

2. CESG, as the UK's National Technical Authority for Information Assurance, operates the Scheme as part of its Information Assurance (IA) consultancy services. In addition to internationally recognised IT evaluation and consultancy, there are other IA services that are of relevance to HMG and Critical National Infrastructure (CNI) organisations. For further details, please refer to the Formal Documentation section of the CESG website:

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

3. The IA Delivery Office can offer advice to Sponsors to help them determine which assurance and consultancy services are appropriate for their needs.

4. This document describes the Scheme and the procedures applied under it. It is intended for use by potential customers (i.e. anyone concerned with the development, procurement or accreditation of IT products in which security is a consideration) as well as those already involved in the Scheme.

5. This document serves only as an introductory guide. It is expected that readers will also consult other documents, in particular the following:

- Common Criteria For IT Security Evaluation (CC) documentation, or IT Security Evaluation Criteria (ITSEC) documentation, including International Interpretations, UK Interpretations and Scheme Information Notices (SINs);
- related UK Scheme Publications, e.g. CLEF Requirements (UKSP 02) and the Sponsor's Guide (UKSP 03);
- assurance maintenance documentation, e.g. the Assurance Continuity supporting document (for CC) or UKSP 16 (for ITSEC).

6. For further details, please see the *Abbreviations and References* document on the Formal Documentation page of the CESG website at <http://www.cesg.gov.uk>.

² The processes described by this document relate to internationally recognised evaluation and certification of products. (Note that the use of the term "product" in this document is intended to cover "product or system" unless the context makes the usage specific.) Some aspects may be more widely applicable to similar IA services; as explained in paragraphs 2 and 3, advice regarding the range of IA services can be obtained where desired.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

IT Security Evaluation and Certification

7. IT security evaluation is an impartial assessment of an IT product by an independent body. This provides the users of such products with confidence in the security functionality provided. It also provides users with a metric to compare the security capabilities of products that they are thinking of purchasing. The IT product to be evaluated is referred to as the Target of Evaluation (TOE).

8. Certification provides independent confirmation of the validity of evaluation results, and thereby ensures comparability of these results across all evaluations under the Scheme and facilitates international mutual recognition of results between national schemes. Certification confirms that the TOE meets its Security Target to the claimed assurance level, and confirms that the evaluation has been conducted in accordance with the standards of the Scheme.

9. Certification does not endorse a TOE in any other respects. Moreover it is not a guarantee that the TOE is completely free of exploitable vulnerabilities. There will remain a small probability that some exploitable vulnerabilities remain undiscovered. This probability decreases as the assurance level increases.

10. Certification applies to a specific version of a TOE. However, the Scheme provides means by which the certified status of a TOE can be maintained, without always requiring a full re-evaluation.

The Scheme

11. The Scheme offers evaluation and certification services to Sponsors, Developers, Vendors, Procurement Bodies and Accreditors.

12. The Scheme established a single UK Certification Body (CB), to certify the results of evaluations of IT products. The CB also deals with other nations regarding the mutual recognition of such certificates; see the Common Criteria Portal website at <http://www.commoncriteriaportal.org>.

13. The Scheme also established an organisational and procedural framework for the conduct of evaluations in the UK. This includes the appointment of Commercial Evaluation Facilities (CLEFs), which carry out the evaluations, and the establishment of approved techniques and procedures.

14. Each CLEF is required by the Scheme to be accredited by the UK Accreditation Service (UKAS) as a testing laboratory, in accordance with ISO/IEC 17025.

15. The scope of CLEF accreditation covers tests that meet UKAS requirements reflecting the following four principles.

- impartiality, i.e. evaluations are demonstrably free from bias;

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

- objectivity, i.e. evaluation results are obtained from the evidence provided, with the minimum of subjective judgement or opinion;
- repeatability, i.e. the same overall result would be obtained by the **same** organization, if it repeated the evaluation of the same product against the same set of security requirements;
- reproducibility, i.e. the same overall result would be obtained by a **different** organization, if it evaluated the same product against the same set of security requirements.

16. Some aspects of security testing may, however, require subjective interpretation, e.g. where the criteria need clarification. In such cases the CB plays an essential role to ensure consistent application of the criteria and reporting of results across all evaluations and CLEFs by:

- agreeing UK interpretations;
- maintaining and improving the UK evaluation methodology in order to reduce subjectivity;
- seeking further agreement, on interpretations and methodology, with its international mutual recognition partners.

17. The CB also plays an active role in the evaluation process by:

- determining whether a TOE will be certifiable in principle before accepting a proposed evaluation into the Scheme;
- monitoring all evaluations conducted under the Scheme in a manner appropriate to their respective assurance levels;
- assessing all evaluation results and issuing certificates as appropriate.

18. Therefore, whilst the conduct of individual evaluations and the quality standards enforced are in general the responsibility of CLEFs, the validity and consistency of evaluation results are endorsed by certification under the Scheme.

Evaluation Criteria and Methodology

19. There are clear benefits to be gained if evaluations are carried out in accordance with procedures and standards that are widely recognised. In the case of IT products, the vendor's market will be enhanced by wider customer recognition of the standards achieved.

20. The evaluation criteria currently recognised by the Scheme, and the methodologies associated with them, are:

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

- Common Criteria (CC) ISO/IEC 15408 and Common Methodology For IT Security Evaluation (CEM) ISO/IEC 18045;
- ITSEC and IT Security Evaluation Manual (ITSEM).

21. CC is the set of criteria recommended by CESG for product evaluations, as CC certificates are recognised more widely than ITSEC. However Sponsors should satisfy themselves as to the suitability or otherwise of CC for their particular purposes.

22. Wherever the CC criteria and CEM methodology are mentioned in this document, the reader is referred to the latest references listed on the CESG website <http://www.cesg.gov.uk/> or directly on the Common Criteria portal website <http://www.commoncriteriaportal.org/>. The IA Delivery Office should be consulted if ITSEC is of interest.

Security Targets

23. A TOE can only be evaluated and certified against an explicit Security Target. The Sponsor is responsible for preparing the Security Target, but may seek advice from a CLEF in order to do so.

24. The Security Target³ specifies:

- the security environment in which the TOE will operate;
- the security functional requirements against which the TOE is evaluated;
- the level of assurance required in the TOE.

Protection Profiles

25. A Protection Profile⁴ is a generic specification of security environment, security functional requirements and assurance level for a particular type of product, prepared by an organisation to define their security needs. A CC Security Target may be evaluated for conformance to a Protection Profile (or more than one, if the requirements do not conflict).

Mutual Recognition

26. It is HMG's aim that the certificates issued under the Scheme should also be recognised as far as possible in the international context. It is intended that such recognition should extend at least to certificates for commercial applications and

³ For a Common Criteria Security Target see CC Part 1 (v3.1 Annex A or v2.3 Annex B). For an ITSEC Security Target see ITSEC (v1.2 Chapter 2).

⁴ For a general definition of a Common Criteria Protection Profile see CC Part 1 (v3.1 Annex B or v2.3 Annex A). Specific examples are listed on the CESG website and Common Criteria Portal websites.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

government non protectively-marked applications. It is also HMG's intention that certificates should be valid for UK national security applications and in the context of NATO requirements.

27. To this end, the UK is a party to the Mutual Recognition Agreement (MRA) by the Senior Officials Group – Information Systems Security (SOGIS) of the European Commission for CC and ITSEC, and also the CC Recognition Arrangement (CCRA). In addition, CESG has signed a Memorandum of Understanding with DSD of Australia and GCSB of New Zealand to recognise each other's ITSEC certificates up to assurance level E6. See <http://www.cesg.gov.uk/> for these documents and further information regarding mutual recognition.

28. See <http://www.cesg.gov.uk/> for those countries that recognise CC and ITSEC certificates issued by the UK CB, and the extent of this recognition in terms of CC Evaluation Assurance Level (EAL n) or ITSEC Evaluation Level (E n). Note that all countries that accept UK CB certificates up to ITSEC E6 will also accept up to CC EAL7, except for Australia and New Zealand who will only accept up to CC EAL4. Countries that do not accept ITSEC at all will only accept up to CC EAL4 by virtue of the CCRA. See <http://www.commoncriteriaportal.org> for the definitive list of current CCRA members.

29. For CC recognition, the following notes apply:

- recognition to a given EAL includes recognition of evaluations against all of the assurance components included in that level, or in levels below it;
- countries party to the CCRA also recognise evaluation against the CC Flaw Remediation assurance components;
- countries party to the CCRA also recognise CC Assurance Continuity results based on assurance components included in the EAL4 level, or in levels below it.

30. See <http://www.commoncriteriaportal.org> for the current list of CC Schemes. The current certificates that are recognised by the UK CB are detailed at <http://www.commoncriteriaportal.org>.

31. The above international agreements include the caveat that certificates issued by other countries will not necessarily be recognised where national security is involved.

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

II. ORGANISATION AND MANAGEMENT

Introduction

32. This chapter describes the roles of the principal stakeholders in the process of IT security evaluation and certification. It also describes associated policy and approach. The principal stakeholders in evaluations under the Scheme are the Scheme Senior Executive, the Certification Body, CLEFs, Sponsors, Developers, Vendors, Procurement Bodies and Accreditors.

Senior Management Team

33. The Scheme operates as part of CESG and its affairs are overseen by the CESG Senior Management Team. The CESG Senior Management Team provides the CB with top level direction, setting and reviewing policy and monitoring the performance of the Scheme overall. Policy is set following extensive interaction with HMG and CNI organisations, and other stakeholders, to ensure that their needs are addressed.

34. Responsibility for the day-to-day running of the Scheme resides with the Head of the CB and its Technical Director, with oversight provided by the Scheme Senior Executive.

Certification Body

35. Terms of reference for the CB include the following:

- appointing CLEFs and keeping their appointment under review;
- confirming the suitability of each TOE, certifying the results of evaluations conducted under the Scheme, and providing details of certified products in the Directory of Infosec Assured Products and on the CESG website;
- liaising with the appropriate national and international agencies regarding the mutual recognition of certificates;
- developing, improving and maintaining the UK evaluation methodology described in UK Scheme Publications and relevant interpretations, and ensuring consistency with evolving international criteria and methods.

CLEFs

36. CLEFs are contracted with CESG to operate under the Scheme. Each CLEF is obliged as a condition of its appointment to:

- observe all rules of the Scheme;

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

- be accredited as a testing laboratory by UKAS, against ISO/IEC 17025;
- follow the appropriate evaluation methodology and interpretations;
- observe the highest standards of commercial confidentiality;
- have the status of its individual Evaluators recognised by the CB.

37. Each CLEF is subject to scrutiny, by both the CB and UKAS as appropriate, to ensure that it meets its obligations.

Sponsors

38. The term 'Sponsor' refers to the person or organisation that requests and funds an evaluation and is entitled to receive the reports produced. Further details and guidance is provided by the Sponsor's Guide (UKSP 03).

39. The Sponsor has the option of engaging a security consultant, which may be a CLEF, to assist them to prepare for evaluation. However such consultancy should not impair the independence of the evaluation; i.e. an individual cannot evaluate his or her own work.

Developers

40. The term 'Developer' refers to the organisation that has produced (or is producing) the TOE. Where the Developer is not the Sponsor, it will usually be necessary for the Sponsor to ensure the co-operation of the Developer in supporting the evaluation, e.g. by providing technical evaluation deliverables to the CLEF.

Vendor

41. The term 'Vendor' refers to the organisation that sells the TOE.

Procurement Body

42. The term 'Procurement Body' refers to the person or organisation that purchases and acquires the TOE for use in an operational environment.

Accreditor

43. The term 'Accreditor' refers to the person who is responsible for the overall security of a system in its operational environment and who takes into consideration the conclusions and recommendations of the CLEF that has been chosen to perform the evaluation of the IT security requirements of the TOE, which may be the whole or some well defined part of that system.

Evaluation and Certification Processes

44. The evaluation is divided into 'preparation', 'evaluation and certification' and 'assurance maintenance' phases, which are outlined in the following chapters.

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

45. The CLEF will evaluate the TOE using the appropriate criteria and methodology. It will liaise with the Sponsor and Developer to progress the evaluation and, together with the Sponsor, is responsible for requesting the following certification services at the appropriate points in the evaluation:

- a Task Startup Review (which *may* include a Task Startup Meeting with key stakeholders), to assess the suitability of the proposed TOE for entry into the evaluation process and to agree the scope of the TOE;
- formal approval to accept the TOE into the Scheme;
- an Evaluation Work Programme (EWP) Review;
- a Security Target Review to approve the Security Target;
- any Evaluation Progress Reviews with the CB to review or approve aspects of selected evaluation work and to identify new UK National Interpretations that are required, which will be addressed by the CC UK Support Group (CCUKSG);
- a Certification Review to approve and issue the Certification Report and issue the Certificate;
- a Post Evaluation Review (if required) with the CB to capture any new UK interpretations that may have been required during the evaluation.

46. The objective of each certification service⁵ will be to determine, in a timely manner, whether to give approval to continue and to make appropriate recommendations concerning the evaluation. Where necessary, certification processes may be iterative, with the CB considering inputs which have been revised in response to its previous suggestions.

47. The Sponsor will need to enter into separate contracts with the CLEF and the CB for their respective evaluation and certification services. For further details please refer to UKSP 03.

Appeals Procedure

48. Any dispute concerning the operation of the Scheme may be referred to the CB by any party, e.g. CLEF, Sponsor, Developer, Vendor, Procurement Body or Accreditor. If this course of action is considered to be ineffective, or if the CB itself is involved in the dispute, the party may appeal to the Scheme Senior Executive for resolution.

⁵ The general Certification activities provided by the UK CB for a CC evaluation are summarised in the "UK CB Standard Certification Work Programme" as detailed on the CESG website under "Formal Documentation". Similar activities are provided for other assurance services.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

III. PREPARATION

Introduction

49. The objective of the preparation phase is to determine the suitability of the TOE for evaluation, prior to the evaluation and certification phase. This is a risk reduction exercise which is supported by the following activities:

- discussion and agreement of the scope of the TOE based on an understanding of the TOE Scope Information;
- discussion and agreement of the Evaluation Work Programme (EWP) and the Certification Work Programme (CWP), based on the agreed scope of the TOE;
- identification of the deliverables needed to support the evaluation;
- production and approval of the Security Target;
- formal acceptance of the evaluation into the Scheme;
- discussion of any assurance maintenance aspects.

Task Startup Review

50. The aim of the Task Startup Review (which normally requires a Task Startup Meeting) is to agree the suitability of the proposed TOE for evaluation, and to discuss the evaluation and certification process for that TOE. It involves the Developer, the Sponsor, the CLEF, the CB and any other interested parties as appropriate.

51. The main areas covered in the Task Startup Meeting are as follows.

- a. the Sponsor presents the TOE Scope Information, as summarised below;
- b. the Evaluator presents an outline Evaluation Work Programme based on the TOE Scope Information;
- c. the CB discusses the suitability of the proposed TOE, the outline Evaluation Work Programme, and its standard Certification Work Programme.

52. The CB will usually require that sufficient TOE Scope Information is available at least ten working days in advance of the Task Startup Meeting.

53. During or following the Task Startup Meeting, the CB will confirm whether the proposed TOE is suitable for evaluation. As a result of this meeting, the CB will formally approve the continued production of the Security Target and the continued stages of evaluation based on the agreed scope of TOE. The CB may also make

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

recommendations about the further conduct of the evaluation, including initial test ideas from their technical experts.

54. In some cases, e.g. for re-evaluations, a Task Startup Meeting may not be required by the CB. When a Task Startup Meeting is not required, a Task Startup Review will still be required, but it may use other means of communication and discussion, e.g. email or phone. The reason for omitting the TSM should be documented.

TOE Scope Information

55. The TOE Scope Information is a required input for the Task Startup Review and the Task Startup Meeting. It is prepared by the Sponsor to enable the CB to assess the suitability of the proposed TOE for evaluation. It is based on the product architecture and it should include enough detail about the proposed TOE and its scope to enable the CB to make this decision. The Sponsor should be prepared to discuss all aspects of the TOE at the Task Startup Meeting. There are some cases where a separate document will *not* be needed for the TOE Scope Information requirement. For example:

- If a TOE is being submitted for re-evaluation, then the previous Security Target (updated to indicate changes, e.g. using *Track Changes*) will normally be sufficient;
- If a Security Target is already in production then a draft copy may be suitable to satisfy the TOE Scope Information requirement, provided that the TOE Description and Evaluated Configuration are specified in sufficient detail, even if the chapters describing the TOE Summary Specification and Rationale are still to be completed.
- If the TOE is a Protection Profile then there will not be any product architecture information and a draft copy of the Protection Profile may be suitable to satisfy the TOE Scope Information requirement.

56. Further details of the requirements for TOE Scope Information are provided in the Sponsor's Guide (UKSP 03).

Evaluation Work Programme

57. The Evaluation Work Programme outlines the work to be undertaken by the CLEF. Where relevant, it will highlight issues concerning application of the criteria, methodology and interpretations, to the evaluation of the TOE.

58. The outline Evaluation Work Programme discussed at the Task Startup Meeting and approved during the Task Startup Review may subsequently be refined and updated as the evaluation progresses.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

Certification Work Programme

59. The Certification Work Programme identifies all of the reviews and activities required by the CB to complete the certification process. A UK CB Standard Certification Work Programme is available on the Formal Documentation page at the CESG website <http://www.cesg.gov.uk/>. The Certification Work Programme is an input to the Task Startup Meeting, and may be refined and updated during the evaluation.

Deliverables

60. Evaluation deliverables are inputs to the evaluation process, as prescribed by the assurance level specified by the Security Target. They may include:

- items of hardware, firmware or software which constitute the TOE itself;
- supporting TOE documentation;
- guidance documentation;
- access to the development site;
- technical support;
- Items of hardware, firmware or software which constitute the TOE platform(s).

61. The Sponsor, CLEF and other interested parties should agree the full set of deliverables that will be required for the evaluation, and the Sponsor should ensure the supply of all evaluation deliverables in a timely manner to the CLEF.

Security Target

62. After establishing the **suitability of the proposed TOE for evaluation** following the Task Startup Review and Task Startup Meeting, the Sponsor is responsible for provision of a complete Security Target, which is a formal document defined within CC or ITSEC⁶. Much of the information required for the Security Target will have been agreed already as part of the TOE Scope Information.

63. The CLEF will check as appropriate that the Security Target corresponds to the agreed TOE Scope Information and will evaluate the Security Target under the relevant CC (or ITSEC) criteria. The CB will then review the Security Target and the CLEF's report on the Security Target.

⁶ For a Common Criteria Security Target see CC Part 1 (v3.1 Annex A or v2.3 Annex B). For an ITSEC Security Target see ITSEC (v1.2 Chapter 2).

UK IT Security Evaluation and Certification Scheme Description of the Scheme

Protection Profile

64. For a Protection Profile (PP) a Task Startup Review is required, but a Task Startup Meeting is not necessary. The PP will be evaluated by the CLEF with respect to the relevant CC criteria⁷. The CB will review the CLEF's report and issue the Certificate if appropriate.

65. The CB will ensure that the PP is suitable for use by the intended consumers, who may include Security Target authors.

Formal Acceptance of Evaluation

66. Following the CB's approval of the Security Target, the evaluation will be formally accepted into the Scheme. In accepting the TOE, the CB indicates that it is satisfied that the TOE will be certifiable in principle under the Scheme, and that the Security Target is an acceptable document describing the TOE.

67. When the TOE is formally accepted and the EWP is approved, an entry showing the TOE as 'In Evaluation' will be placed on the CESG website. The wording of this entry will be proposed by the Sponsor, using about 100 words, and agreed by the CB. The continuation and maintenance of this entry depends on the ongoing progress of the evaluation.

⁷ Note that there is no concept of an ITSEC Protection Profile.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

IV. EVALUATION AND CERTIFICATION

Introduction

68. The objective of the evaluation and certification phase is to determine, to the required assurance level, whether the TOE meets its Security Target and is suitably free from exploitable vulnerabilities⁸. This involves the following activities.

- evaluation of the TOE, including analysis and testing;
- interaction between the parties involved, to ensure effective co-operation between the development and evaluation processes;
- production of any Observation Reports (ORs);
- production of the Evaluation Technical Report (ETR) by the CLEF;
- publication of the Certification Report (CR) and Certificate by the CB.

Evaluation Work

69. The Evaluators perform the technical work against the defined evaluation criteria. This comprises a series of analysis and testing activities as prescribed by the relevant evaluation methodology, and outlined in the Evaluation Work Programme (EWP).

70. During the course of an evaluation, the CLEF often needs to interact directly with the Developer, but will, where appropriate, seek the agreement of the Sponsor before doing so.

71. The results of the evaluation are documented as the evaluation proceeds. If, in the course of performing the evaluation work, errors or vulnerabilities are discovered, then ORs will be raised that will normally require some corrective/improvement action by the Sponsor and/or the Developer.

72. The CLEF will discuss such ORs with the Sponsor and/or Developer as appropriate, to ensure early resolution. It will also bring any significant issues to the attention of the CB.

Evaluation Progress Reviews

73. During this phase of the evaluation, the CB conducts Evaluation Progress Reviews, which may be in the form of documentation reviews or Evaluation Progress Meetings with the CLEF. Evaluation Progress Meetings may also involve the Sponsor and other interested parties.

⁸ This is subject to the conditions in paragraph 9.

UK IT Security Evaluation and Certification Scheme

Description of the Scheme

74. Evaluation Progress Reviews may result from issues raised in the evaluation or from requirements raised earlier by the CB in the Certification Work Programme.

75. An Evaluation Progress Review can include one or more of the following:

- detailed technical review of the TOE architecture;
- review of preliminary evaluation outputs which form some or all of the ETR;
- review of evaluation deliverables, e.g. design, guidance documentation, delivery processes;
- review of Observation Reports or other issues raised by the CLEF or the Sponsor;
- clarification of details to be included in the Certification Report.

76. Although some Evaluation Progress Reviews will be based partly on meetings, often such issues can be dealt with by normal communications such as email or telephone/teleconference.

77. For some evaluations there will be a specific requirement for a Test Strategy Review (both for functional testing and penetration testing), which can be seen as a special case of an Evaluation Progress Review.

78. A Test Strategy Review will include some or all of the following:

- review of vulnerability analysis;
- review of parts of the Evaluation Work Programme concerning test strategy and sampling strategy;
- review of the planned test configurations;
- review of the planned Test Scripts.

79. As part of this review, the CB may attend and witness some or all of the Evaluators' security testing and may seek advice from CESG's technical experts.

Evaluation Technical Report

80. The Evaluators document their findings in an ETR, which represents the final output from the evaluation. The conclusions documented in the ETR state whether the evaluation criteria and security functionality have been met, with supporting evidence. The ETR content shall conform to the requirements of the evaluation methodology and the Scheme.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

Certification Report and Certificate

81. Following their review of the ETR, the CB publishes the findings of the evaluation in the Certification Report.

82. The CLEF assists the CB in the production of the Certification Report by producing a draft version. This is circulated to the Sponsor and the CB for comments and the CLEF produces any revised versions required. The CB will approve and formally issue the Certification Report, in consultation with the CLEF and the Sponsor.

83. The purpose of the Certification Report is to:

- provide a statement confirming whether the TOE conforms to its Security Target;
- confirm the assurance level achieved;
- confirm the evaluated configuration;
- recommend any appropriate measures to improve the secure usage of the TOE, such as countermeasures to potential vulnerabilities discovered during the evaluation;
- provide any security relevant guidance to potential customers, procurement bodies and end users, as recommended by the Evaluators;
- confirm that the evaluation has been conducted in accordance with the Scheme and that the conclusions drawn from the evaluation are consistent with the facts presented.

84. When the Certification Report has been successfully finalised, a Certificate will also be issued by the CB. Also the status of the TOE's entry on the CESG website will be changed to 'Certified' and, for a CC TOE, the CB will inform the CC portal website so that an entry will be made on that website. It is a requirement of the Common Criteria Recognition Arrangement that the Security Target, excluding proprietary information if necessary, and the Certification Report are published on the CESG and CC portal websites. Details of the TOE will then also appear in the next issue of the Directory of Infosec Assured Products.

85. Certification Reports and Certificates are Crown Copyright. Their reproduction and distribution is authorised provided that they are copied in their entirety.

V. ASSURANCE MAINTENANCE

Introduction

86. The certificate initially awarded applies to the specific evaluated version of a TOE in its evaluated configuration. However, most TOEs are subject to post-certification changes that are outside the scope of that certificate, e.g. resulting from security irrelevant patches to products. The Sponsor may choose to contract a CLEF to perform a re-evaluation of the TOE, to ensure that certification extends to the new version. However, it is not normally cost-effective to re-evaluate every new version of a TOE.

87. The processes of assurance maintenance provide a means of establishing confidence that the assurance in a TOE is maintained without always requiring a formal re-evaluation. Under these processes the Sponsor is able to maintain assurance in minor⁹ changes to the TOE without incurring the costs associated with re-evaluating the TOE for each of these changes, and at the same time minimise the cost of any future re-evaluation. The Sponsor should always consider the possibility of assurance maintenance and its costs at the time of the original evaluation. It is particularly suited to TOEs that are expected to be updated on a routine or regular basis for minor security relevant changes.

88. **Flaw Remediation** is an additional CC assurance component for evaluating the adequacy of the Developer's flaw remediation process at the time of the evaluation of the TOE. Assurance is not extended to the change made, just to the processes relevant to changing the TOE and identification/handling of reported flaws.

89. **Re-Evaluation** is required where changes made to the TOE have significant impact on assurance. Re-use of evaluation results may be possible and can reduce the cost and time required for a re-evaluation. Where changes have a wide impact on the security functionality in the TOE, and previous results do not apply, a complete evaluation of the TOE may need to be performed to re-establish assurance.

Assurance Maintenance

90. For CC, the **Assurance Continuity** process is based on an Impact Analysis Report detailing the security impact of changes on the evaluation deliverables. The report is produced by the Developer, issued by the Sponsor and reviewed by the CB. Changes are assessed as having minor or major impact on assurance. If there are *only* minor changes then a Maintenance Report can be awarded as an Addendum to the original Certification Report and Certificate.

91. For ITSEC, the UK **Certificate Maintenance Scheme** (CMS) is also based on an Impact Analysis Report produced by the Sponsor. Initial assessment of the impact of changes on assurance as major or minor is left to a Developer Security Analyst, appointed by the Sponsor, who is permitted to claim CMS approved status where

⁹ Note that major changes would require a re-evaluation of the TOE.

UK IT Security Evaluation and Certification Scheme Description of the Scheme

changes are minor. The work of the Developer Security Analyst is subject to periodic audit by the CLEF, and a successful audit will result in the issue of a maintenance certificate by the CB.

92. The award of a maintenance certificate, through either the Assurance Continuity process or the Certificate Maintenance Scheme, is recognised on the CESG website.