UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No 4

DEVELOPERS' GUIDE

Part I

ROLES OF DEVELOPERS IN ITSEC

Issue 1.0

July 1996

Issued by:-

UK IT Security Evaluation & Certification Scheme

This Guide does not replace or supersede the ITSEC requirements and method as specified by the ITSEC and ITSEM. While the Certification Body and the authors believe that the information and guidance given in this document is correct, all parties must rely on their own skill and judgement when making use of it. The Certification Body and the authors do not assume liability to anyone for any failure to achieve certification or for any loss or damage arising from advice or guidance given within this document.

Parties using this Guide are recommended to check any ITSEC criteria repeated in this Guide against the latest version of the ITSEC.

FOREWORD

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

The Developers' Guide provides guidance to developers and sponsors on how to ensure that the development of secure products and systems meet the evaluation and certification requirements of the IT Security Evaluation Criteria (ITSEC).

This document (Part I of the Developers' Guide) provides an introduction for developers and sponsors to the concept of evaluation, the ITSEC, the roles of the bodies involved in the development of ITSEC secure products and systems, and the practical issues involved in preparing for an evaluation.

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

Correspondence concerning this Guide, including requests for additional copies, should be addressed to:

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

Telephone: +44 1242 238739

Facsimile: +44 1242 235233

E-mail: CBSec@itsec.gov.uk

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	Incorporated by Name Signature	Date

CONTENTS

FIGURES

REFERENCES

A ITSEC - Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria, Version 1.2, Commission of the European Communities, 28 June 1991

B ITSEM - IT Security Evaluation Manual, Version 1.0, Commission of the European Communities, 10 September 1993

C UKSP 01 - UK IT Security Evaluation and Certification Scheme, UK Scheme Publication No 1, Description of the Scheme, Issue 2.0, 29 April 1994

D UKSP 06 - UK IT Security Evaluation and Certification Scheme, UK Scheme Publication No 6, UK Certified Product List, latest issue

ABBREVIATIONS

CCTA	Central Computer and Telecommunications Agency
CESG	Communications-Electronics Security Group
CLEF	Commercial Licensed Evaluation Facility
CMS	Certificate Maintenance Scheme
COTS	Commercial-Off-The-Shelf
CR	Certification Report
DMR	Development Methods Review
DTI	Department of Trade and Industry
ECM	Evaluation Control Meeting
EMR	Evaluation Methods Review
EN	European Norm
EOR	Evaluation Observation Report
EPM	Evaluation Progress Meeting
ESR	Evaluation Summary Report
ETR	Evaluation Technical Report
EWP	Evaluation Work Programme
ISO	International Standards Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
	Information Technology Security Evaluation and Certification (see Scheme)
ITSEM	Information Technology Security Evaluation Manual
MoD	Ministry of Defence
PRSR	Problem Report Status Register
Scheme	UK IT Security Evaluation and Certification Scheme
SEF	Security Enforcing Function
SFN	Security Fault Notification
TCM	Task Closedown Meeting
TCSEC	Trusted Computer System Evaluation Criteria (known as the "Orange Book")
TOE	Target of Evaluation
TSM	Task Startup Meeting
UK	United Kingdom
UKAS	UK Accreditation Service
UKSP	UK Scheme Publication
US	United States of America

Chapter 1 Introduction to the Developers' Guide

How to use this Guide

1.1 The Developers' Guide has been produced to assist developers intending to submit their products or systems for evaluation under the UK IT Security Evaluation and Certification Scheme ('the Scheme').

1.2 The Guide is divided into three parts:

a) Part I - Roles of Developers in ITSEC

b) Part II - Reference for Developers

c) Part III - Advice to Developers.

1.3 Part I (i.e. this document) provides an introduction to the ITSEC for developers. It emphasises the roles and responsibilities of developers and their interactions with other organisations within the Scheme. Readers of this Guide who are familiar with the evaluation process under the Scheme and the basic requirements placed upon developers may wish to concentrate on Parts II and III.

1.4 Part II provides a detailed guide to the ITSEC criteria which are relevant to developers.

1.5 Part III gives advice to developers on how to tackle development issues which are specific to the ITSEC criteria.

1.6 In addition, a Developers' Guide Roadmap provides an explanation of the Guide, with suggested reading plans.

Objectives of Part I

1.7 This Part of the Developers' Guide provides an overview of the UK ITSEC Scheme to developers of IT products and systems who are new to security evaluation procedures. It describes how developers become involved in the evaluation process so that they may produce products or systems suitable for independent evaluation and certification.

1.8 The organisations involved in the Scheme are described and how those organisations interact with developers in order to achieve successful evaluations. In addition, it gives an overview of the roles and responsibilities of developers and sponsors before, during and after an evaluation and describes the requirements placed upon them.

1.9 This document also provides details on how evaluations can be initiated and the contractual issues involved, in order that developers may plan their development programmes to take account of the business factors involved in the evaluation process, such as time and cost.

Scope

1.10 This document covers:

a) the features and benefits of independent security evaluation under the UK ITSEC Scheme

b) an introduction to evaluation for sponsors and developers and why evaluation is required

c) evaluation concepts within the ITSEC, ITSEM and national scheme (UK ITSEC Scheme)

d) an overview of the evaluation process

e) the roles and responsibilities of sponsors and developers within the UK ITSEC Scheme

f) the work involved in the preparation of an evaluation

g) typical evaluation timescales

h) contractual issues of evaluations.

Acknowledgements

1.11 This Guide contains excerpts from the Information Technology Security Evaluation Criteria (ITSEC) [Reference 0] and the IT Security Evaluation Manual (ITSEM) [Reference 0], both published by the Commission of the European Communities.

A Request for Feedback

1.12 Developers play a significant part in the performance and success of the Scheme. It is the UK Certification Body's wish to assist developers with their understanding of the Scheme to enhance the likelihood of successful evaluations and further increase the number of certificates awarded.

1.13 The Certification Body extends an invitation to all developers and sponsors to contact the Certification Body with feedback on this Guide and the Scheme or to obtain further advice on the Scheme.

1.14 Please contact the Certification Body at the address shown in the Foreword (see page 5).

Chapter 2 Features and Benefits of the ITSEC Scheme

Features of the Scheme

2.1 The objectives of the Scheme are to meet the needs of Industry and Government for cost effective and efficient security evaluation and certification of IT products and systems. The Scheme also aims to provide a framework for the international mutual recognition of certificates. This will be based upon the Information Technology Security Evaluation Criteria (ITSEC) [Reference 0] and the IT Security Evaluation Manual (ITSEM) [Reference 0] and any developments to them.

2.2 The Scheme provides independent confirmation that evaluations have been performed in accordance with the approved criteria (the ITSEC), and the methods and procedures (the ITSEM), and that the conclusions of evaluations are consistent with the facts presented. Within the context of the UK ITSEC Scheme, as operated by the Certification Body, this helps to provide grounds for confidence that different evaluation facilities within the Scheme are operating to the same standards and that the conclusions of any two evaluation facilities will be equally reliable. The major features of these grounds for confidence are summed up in four principles:

a) **Impartiality:** All evaluations must be free from bias

b) **Objectivity:** The property of a test whereby the result is obtained with the minimum of subjective judgement or opinion

c) **Repeatability:** The repeated evaluation of the same system or product against the same set of security requirements by the same organisation yields the same overall verdict as the first evaluation

d) **Reproducibility:** The evaluation of the same system or product against the same set of security requirements by a different organisation yields the same overall verdict as the first organisation.

2.3 Further details of the Scheme can be found in the UK Scheme Publication No. 1 entitled *Description of the Scheme* [Reference 0]. This document is obtainable from the Certification Body at the address in the Foreword (see page 5).

Benefits for Developers

2.4 The major benefits of an ITSEC evaluation to developers, sponsors or vendors are:

a) **third party endorsement** - customers are aware that a successful independent third party evaluation has agreed with the security claims made in respect of the product

b) **market expansion** - an appropriate certificate will permit entry and acceptability in specialised markets, especially where certified products are mandated

c) **mutual recognition** - certificates issued in one country can be recognised in another, requiring only one evaluation and promoting international recognition of certified products

d) **competitive advantage** - certified products may be used as building blocks for certified systems

e) **improved product quality** - certification also provides confidence in the quality of a product or system and its development

f) **increased customer confidence** in the product and in the developers' commitment to security.

Chapter 3 The Concept of Security Evaluation

The Need for Evaluation

3.1 In today's modern technological society, where information can be easily accessed and manipulated, computer security is of increasing importance. This is true for commercial organisations, national and local government, as well as the private individual. All of these bodies have different motives for being concerned about security.

3.2 Individuals are concerned that any information relevant to themselves is accurate and remains confidential. Commercial and Government organisations are concerned that information relevant to their business or function is accessible when required, that is accurate, and that its confidentiality is maintained. Organisations are concerned that the data they own is protected from deletion or corruption, either accidentally or by malicious individuals. Loss or corruption of data can require expensive reinstatement and can place the future of the organisation at risk.

3.3 As a result of these security concerns, individuals and organisations are looking for effective IT products that will ensure that their systems are protected and available when required. It is with this background that developers are becoming much more aware of the need to produce products and systems that meet recognised criteria.

3.4 The UK ITSEC Scheme provides an independent assessment resulting in a certificate which is recognised by user organisations in the UK and overseas. It is also recognised by UK government departments who are now recommended to construct systems using products certified by the Scheme.

What is Evaluation?

3.5 Evaluation is the assessment of a developer's IT system or product against defined security evaluation criteria. The intention of this process is to obtain a certificate indicating the suitability of the IT system or product for use within a specified environment.

3.6 To ensure that impartiality is maintained, ITSEC evaluations are performed by third parties independent of developers.

The Scope of Evaluation

3.7 IT security aspects of systems and products cover three major areas known as **confidentiality**, **integrity** and **availability**. The objective of a security evaluation is to ensure that the security claims made against one or more of these areas are achieved for the system or product under evaluation. The three IT security areas are defined as follows:

a) confidentiality - prevention of the unauthorised disclosure of information

b) integrity - prevention of the unauthorised modification or destruction of information

c) availability - prevention of the unauthorised withholding of information or resources.

Evaluation and the IT Security Framework

3.8 The IT security framework (shown in Figure 1 below) covers five main processes known as development, evaluation, certification, system accreditation and secure operation. Each process provides input to the next process with the last process being able to provide input back to the first process of development. The processes may be partially interleaved, and their sequence means that iteration may occur. The system accreditation process confirms that the use of an IT system is acceptable within a particular environment and for a particular purpose. In the secure operation process the system or product is operated according to approved procedures.

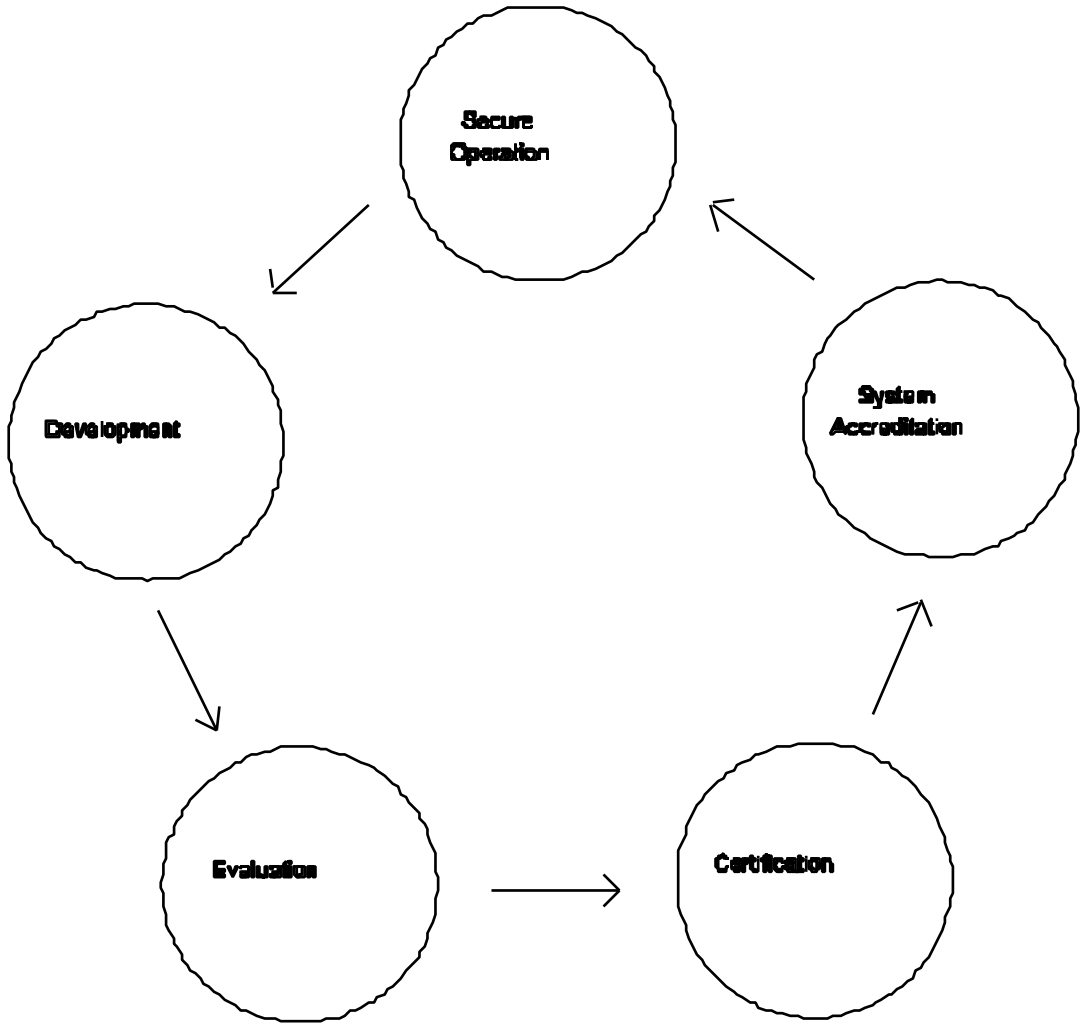

Figure 1 Processes in the IT Security Framework

3.9 In the development process an IT system or product is built to satisfy a set of security claims. The output from this process is assessed in the evaluation process against defined security evaluation criteria. The correct application of evaluation criteria and the validity of the evaluation results are checked in the certification process. The results are then used to produce

the certificate and certification report. Therefore, the evaluation process is fundamental within the IT security framework for a system or product to be able to gain final certification.

3.10 For a system, the process of system accreditation confirms its acceptability for use within a particular environment and for a particular purpose. In the secure operation process an accredited system is operated according to approved procedures, but changes to the environment may require changes which provide input to the development process.

3.11 For a product, the purchaser of the product will either use the product on its own or integrate it within a system. It is the responsibility of the purchaser to ensure that the product's security conditions are followed - for a product integrated within a system this can be provided by a further evaluation which will use the results from the product's original evaluation.

General Philosophy of Evaluation

Assurance

3.12 The goal of evaluation is to gain assurance that a system or product satisfies its security claims. The evaluation provides a particular degree of assurance that the security claims do not suffer from vulnerabilities which can be exploited.

3.13 The degree of assurance provided by an evaluation depends on the chosen evaluation level and the 'strength' of resistance to vulnerabilities for security mechanisms provided. As the evaluation level rises, the amount of relevant information provided increases, and the evaluation effort required increases, resulting in higher degrees of assurance. Thus, the higher the evaluation level and strength of mechanisms, the greater the likelihood that a system or product will behave as expected and adequately counter the identified threats to the system or product.

3.14 Assurance in the security provided by a system or product is derived from examining the system or product and its design and documentation, and from understanding the process by which it was developed. A significant contribution to assurance derives from examination of design and development representations of the system or product.

3.15 Evaluation under the UK Scheme has significant advantages as it provides independent third party confirmation of the security of the TOE. This independent evaluation involves examination of the TOE documentation (as mentioned above), but also includes significant amounts of testing devised and performed by the evaluators to check the correct operation of the TOE and to confirm the absence of exploitable vulnerabilities.

Security Evaluation and Certification

3.16 Users of systems or products need confidence in the security functionality provided. Users also need a yardstick to compare the security capabilities of products they are thinking of purchasing. Although users could rely on trust in the developers of the systems or products in question, or could test them themselves, it is likely that many will prefer to rely on the results of some form of impartial assessment by an independent body. This assessment is called

security evaluation, while the IT system or product being evaluated is referred to as the "Target of Evaluation (TOE)".

3.17 It is important that such evaluation should be carried out in accordance with widely recognised procedures and standards. In the case of IT products, the vendor's market will be limited by customer recognition of the standards achieved. In the case of systems, universal recognition may not be so important, but, for example, where two separately evaluated systems are to be interconnected, the users of each system will need to recognise the validity of the other's evaluation.

3.18 The objective of certification is to independently confirm the validity of evaluation results and thereby to ensure comparability of these results across all evaluations and all evaluation facilities.

Chapter 4 ITSEC Concepts

4.1 This chapter outlines the main concepts of the ITSEC Scheme. Definitions of ITSEC terms are provided in the Glossary. Items highlighted in bold within the text of this chapter indicate that the items are discussed more fully elsewhere in the chapter. The diagram provided in Figure 2 illustrates the relationships between many of these items.

System

4.2 A system is a specific IT installation or configuration, with a particular purpose and operational environment. An example of a system would be a networked set of office computers at several sites.

4.3 A system is evaluated against the security requirements of the specific circumstances of its installation and manner of use.

Product

4.4 A product is a package of IT software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems. An example of a product would be a database sold to a variety of customers for use at the customers' different sites.

4.5 A product is evaluated against the security requirements chosen by the sponsor commissioning the evaluation to cover all the likely circumstances of the product's installation and use by its purchasers.

4.6 It is possible for certain products to be considered as systems, if no alteration is necessary to the product and the specific circumstances of its installation and manner of use exactly match those assumed by the product's sponsor.

Target of Evaluation (TOE)

4.7 Target of Evaluation (TOE) is the term used to refer to an IT system or product which is subjected to security evaluation.

4.8 A TOE may consist of a number of components; for example:

a) newly developed components

b) modified Commercial-Off-The-Shelf (COTS) products

c) unevaluated COTS products

d) COTS products previously evaluated under the ITSEC Scheme

e) COTS products previously evaluated under other schemes, such as the US TCSEC.

4.9 The variety and nature of the components comprising the TOE can greatly affect the extent of the evaluation and the effort required.

Developer

4.10 A developer is the organisation (or group of organisations) which produces the TOE (or component parts of the TOE).

4.11 A developer may also take the role of sponsor to commission an evaluation. Where the developer is not sponsoring an evaluation, he must be prepared to cooperate with the sponsor and agree to assist in the evaluation, e.g. by providing technical support to the organisation performing the evaluation.

Sponsor

4.12 The sponsor of an evaluation is typically the vendor of a product, or the user or supplier of a system who wishes to demonstrate that the TOE meets the specified security target.

4.13 The sponsor is responsible for initiating the evaluation of a TOE by defining the security target and commissioning a Commercial Licensed Evaluation Facility (CLEF) to perform the evaluation.

4.14 The sponsor will receive the Evaluation Technical Report (ETR), and is also entitled to a certification report even if the TOE is awarded **Assurance Level** E0 (i.e. the TOE has failed to achieve certification). TOEs which fail usually have an accompanying certification report which identifies the reasons for failure and required corrective action; this is provided so that the evaluation results can be reused in any future evaluation. (The evaluation may have been halted for reasons unrelated to the TOE, and some aspects may have achieved a successful result, or partially successful result, which can be reused.) In any event, the certification report will provide feedback to the sponsor on the adequacy of deliverables, and can be used to minimise the costs of any future work.

CLEF

4.15 Evaluations are performed by independent, third-party evaluation facilities which are accredited in accordance with agreed rules and licensed by the national Certification Bodies to perform security evaluations. The UK evaluation facilities are known as Commercial Licensed Evaluation Facilities (CLEFs). A list of currently licensed UK CLEFs is available from the UK Certification Body.

4.16 Each CLEF is separately accredited by UKAS to undertake evaluations for a range of ITSEC **assurance levels**, and must meet the requirements of ISO Guide 25 and EN 45001. CLEFs are also permitted by the Certification Body to undertake evaluations for a range of assurance levels. These two ranges can be different. While CLEFs must only carry out evaluations within the range of assurance levels permitted for that CLEF by the Certification Body, a CLEF can

undertake an evaluation for a level unaccredited by UKAS provided that it is within the scope of its licence; this would allow the CLEF to apply for an extension to its UKAS accreditation. It is important to note that the UKAS requirement is a mandatory element of the UK Scheme and dictates the schedule of documentation to be used.

4.17 CLEFs are also required to operate as autonomous and self contained units, separate from their parent companies in all day-to-day operational and administrative aspects, and provide certain basic facilities.

4.18 CLEFs must observe high standards of impartiality and integrity. CLEFs must also maintain rigorous commercial confidentiality of the identity of their clients and the TOEs. This information is given only to those CLEF staff directly involved with an evaluation. CLEF staff must be impartial and are not permitted to combine evaluation, development or consultancy work on the same aspect, or a related aspect, of a TOE.

4.19 Each CLEF is headed by a CLEF Controller who has overall management responsibility for the CLEF. The CLEF Controller is supported by other staff roles, including Business Manager and Technical Manager. These roles and their function are explained in UKSP 02.

4.20 Each evaluator must receive appropriate qualification from the Certification Body before being permitted to perform evaluations. New evaluators are required to undertake a formal training programme and appropriate supervised evaluation experience.

Certification Body

4.21 Certification Bodies are independent and impartial national organisations that perform certification. The Certification Body in the UK is jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI) under the direction of a Management Board.

4.22 The Certification Body is based at CESG in Cheltenham, England. The Certification Body is responsible for the day-to-day running of the Scheme, certifying the results of evaluations, and licensing CLEFs.

4.23 The Management Board is responsible for setting policy for the Scheme and for overseeing its implementation. The Management Board is composed of representatives from CESG, DTI, MoD and CCTA.

4.24 The full responsibilities of the Certification Body and the Management Board are set out in Chapter 2 of UKSP 01 [Reference 0].

Assurance

4.25 Assurance is the degree of confidence that may be placed in the security of a TOE. As the evaluation level increases, more relevant information must be provided by the sponsor and developer and the greater the effort required for evaluation. Therefore, higher evaluation levels

result in increased assurance.

4.26 Assurance in the security provided by a TOE is derived from examining the TOE and its design and development representations, and from understanding the process by which it was developed. A significant contribution to assurance is derived from examination of the TOE deliverables.

4.27 A fundamental concept of assurance within the ITSEC is the split of assurance into confidence in the **correctness** of the functionality enforcing the security, and confidence in the **effectiveness** of that functionality. Correctness concerns whether the TOE correctly implements the security requirements expressed in the **security target**. Effectiveness concerns whether the security functionality implemented in the TOE is adequate to protect against identified threats and is free from exploitable vulnerabilities.

4.28 The two main issues covered by correctness are whether there is an adequate description of the **Security Enforcing Functions** (SEFs) in the security target and whether a disciplined development approach has been followed. The deliverables must provide evidence that the SEFs are correctly implemented in the TOE. The development approach must instil an adequate level of confidence that the correct refinement of the requirements can be established.

4.29 The effectiveness criteria concern the following aspects:

a) Suitability of Functionality - this concerns whether the SEFs are able to protect the specified assets from the specified threats in the security target.

b) Binding of Functionality - this concerns whether the whole TOE will be secure under the conditions stated in the security target if the design and implementation of the SEFs is appropriate and correct.

c) Strength of Mechanisms - this defines the TOE's resistance to direct attack.

d) Construction and Operational Vulnerability Assessments - these concern whether the TOE as a whole and in its operational environment has any exploitable vulnerabilities.

e) Ease of Use - this concerns whether the TOE could be unknowingly used insecurely.

Assurance Level

4.30 Seven assurance levels are defined in respect of the confidence in the correctness of a TOE. E0 designates the lowest level and E6 the highest.

4.31 E0 represents inadequate assurance and is reserved for TOEs which fail to achieve higher assurance levels.

4.32 The criteria for levels E1 to E6 are covered in Part II of this Guide.

4.33 Note that, in the ITSEC, the terms 'assurance level', 'level of assurance', and 'evaluation level' are equivalent.

Security Target

4.34 The security target identifies the security required of a TOE and is used as the basis for evaluation. The security target specifies the **security enforcing functions** of the TOE, the **security objectives**, the **threats** to those objectives and any specific **mechanisms** employed.

4.35 The security target must contain the following:

a) Either a **System Security Policy** (where the actual environment is known) or a **product rationale** (where the precise environment is not known and a user/purchaser must decide if the TOE is appropriate)

- a System Security Policy is a set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specified system (optionally, the electronic security measures within a System Security Policy can be incorporated into a separate document known as the System Electronic Information Security Policy)

- a Product Rationale is a description of the security capabilities of a product, giving the necessary information for a prospective purchaser to decide whether it will help to satisfy his system security objectives

b) A specification of the required security enforcing functions

c) Optionally, a definition of the required security mechanisms

d) The claimed rating of the minimum strength of mechanisms

e) The target **assurance level**.

4.36 The **security objectives** of a TOE provide the reasoning as to why particular functionality is required. The security objectives describe which actual and perceived security threats to the TOE are to be countered. There must be at least one security objective for each TOE.

4.37 **Security threats** can be either actual or perceived threats that would undermine the secure operation of the TOE. These threats can be either deliberate acts to subvert the TOE or accidental occurrences as a result of an unexpected event.

4.38 Both deliberate and accidental acts which may subvert a TOE give rise to three major categories of threats as follows:

a) the unauthorised disclosure of information (breach of confidentiality)

b) the unauthorised modification or destruction of data (breach of integrity)

c) the inability to continue normal processing due to the withholding of information or resources (breach of availability).

4.39 A **countermeasure** is a security measure, either technical or non technical, which contributes to meeting the security objective(s) of a TOE.

4.40 The TOE's functions can be classed as either security enforcing, security relevant or irrelevant to the secure operation of the TOE. Every item of a TOE's functionality can be assigned to one of these three categories.

4.41 The **security enforcing functions** (SEFs) describe the functionality which is actually provided to counter the security threats to a TOE. The SEFs are related to the security objectives by describing the functionality provided and which ones are required to counter each of the security threats. Security enforcing functions are those functions which directly contribute to upholding the secure operation of a TOE.

4.42 **Security relevant functions** are those functions which indirectly contribute to upholding the secure operation of a TOE by providing services to the security enforcing functions. The security relevant functions may also provide services to the non security related functions.

4.43 **Security irrelevant functions** play no part, either directly or indirectly, in the contribution to the secure operation of a TOE.

4.44 These three types of function form the basis for the implementation of components. For a component that contains at least one security enforcing function, that component is also said to be security enforcing. For a component that contains only security irrelevant functions, that component is also said to be security irrelevant.

4.45 The **separation of functionality** refers to the separation of the security enforcing and security relevant functions from the security irrelevant functions that comprise a TOE. This is addressed at the architectural and detailed design levels (note that the architectural design does not distinguish security relevant functions from security enforcing functions, categorising both as security enforcing).

4.46 These three types of functions are separated to ensure that security irrelevant functionality cannot interfere with the security enforcing and security relevant functionality in the TOE. This means that well defined interfaces are required that can be shown not to allow the security irrelevant functions to interact with security relevant data. A design which incorporates significant (valid) separation will minimise the cost of evaluation, by reducing the work necessary to:

a) check the correct implementation of security enforcing and security relevant code

b) check the effects of security irrelevant code on the security enforcing and security relevant

functions.

4.47 The **security mechanisms** describe how the functionality is provided to counter the security threats to a TOE. The security mechanisms are related to the SEFs by describing how each SEF is implemented in the TOE. A security mechanism is the logic or algorithm that implements a function.

4.48 A **critical mechanism** is a security enforcing mechanism within a TOE whose failure through direct attack would create a vulnerability.

4.49 A **component** is the implementation of one or more functions. Each function is refined through the design into one or more components, each of which may itself be refined through subsequent design levels into other components. The lowest level of specification before implementation defines basic components.

4.50 A **basic component** is an identifiable and self-contained portion of a TOE that is identified at the lowest level of detailed design specification. For example, the design of a single source code module may be considered to be a basic component.

4.51 A **functional unit** is defined as a functionally distinct part of a basic component.

4.52 **Traceability** involves the complete mapping of each security enforcing function from one level of representation to the next level of representation. Depending on the level of assurance required, the appropriate level of traceability must be shown from the security target to the other evaluation deliverables which provide different representations of the TOE. This mainly involves tracing the security enforcing functions and mechanisms through the various levels of design documentation.

Functionality Classes

4.53 A functionality class is a predefined set of complementary **Security Enforcing Functions** capable of being implemented in a TOE.

4.54 Example types of functionality class include high integrity requirements for data and programs which may be necessary in database TOEs; high requirements for the availability of a complete TOE or special functions of a TOE which may be necessary for TOEs that control manufacturing processes; and high requirements with regard to the safeguarding of data integrity during data exchange. Other example functionality classes exist which are near equivalents to the US TCSEC criteria (see the ITSEC [Reference 0], Annex A for details).

Evaluation Deliverables

4.55 Evaluation Deliverables are those items or resources that must be made available to the evaluators of the TOE for the purpose of evaluation.

4.56 The initial evaluation deliverable is the security target which should also form the basis of the

contract between the **Sponsor** and **CLEF**.

Problem Reports

4.57 During the course of an evaluation, the evaluators may discover various problems relating to the TOE. Some of these problems may concern vulnerabilities or errors, whilst others may concern other aspects of the TOE (e.g. the development environment, operational documentation). Whatever the problem, it is essential that it receives appropriate, prompt attention from the sponsor, the developer, the Certification Body and other parties as necessary.

4.58 The objective of problem reporting is to ensure that the sponsor, the Certification Body and other parties as appropriate are notified as soon as possible, in order that appropriate timely action can be taken.

4.59 Two types of problem report are generated by the evaluators, depending on the severity and nature of the errors discovered, as follows:

a) **Security Fault Notification** (SFN) - more serious problems are defined to be exploitable vulnerabilities in the TOE and are reported on SFNs

b) **Evaluation Observation Report** (EOR) - less serious problems are reported on EORs.

4.60 An **SFN** is used to report any failure of a TOE to comply with its security requirements (including its security objectives) defined in the security target, but only when there is a risk of a security violation (i.e. there is an exploitable vulnerability)

4.61 Due to the seriousness of the problem raised in an SFN, developers or sponsors must respond to this type of problem report and agree to a timetable for the correction of the fault.

4.62 **EOR**s are used to report all security related problems relating to a TOE other than exploitable vulnerabilities. Clearly, this covers a wide range of problems so two categories (Major and Minor) are used to classify the degree of severity. Examples of the use of EORs include:

a) to report problems regarding the development or the operation of the TOE

b) to report problems with the deliverables for evaluation

c) to report problems which may impact on assurance.

4.63 EORs may also be used to draw the attention of the sponsor and Certification Body to any concerns held by the evaluators regarding the TOE or the progress of the evaluation. However, EORs are not used to raise non security issues with the sponsor - this will be done by other means of communication.

Evaluation Technical Report

4.64 For each evaluation, there will be at least one Evaluation Technical Report (ETR). For complex evaluations or evaluations taking place over a long period, multiple ETRs may be produced. In this case, the final ETR will summarise the findings of the evaluation. An ETR is produced by the **CLEF** performing the evaluation and submitted to the **Certification Body**. The ETR details the findings of the evaluation and forms the basis for certification of the **TOE**.

Certification

4.65 Certification is the award of a certificate by the **Certification Body** to certify that the rating of the security of the TOE has been determined by a properly conducted independent evaluation.

4.66 A certifier is appointed by the Certification Body at the start of the evaluation. The certifier oversees the evaluation process ensuring that the evaluators apply the appropriate methods, techniques and tools, and that the evaluators remain impartial throughout the evaluation.

4.67 The certifier reviews the **Evaluation Technical Report** produced by the **CLEF** and prepares a Certificate and Certification Report summarising the conclusions of the evaluation and the assurance level assigned to the TOE.

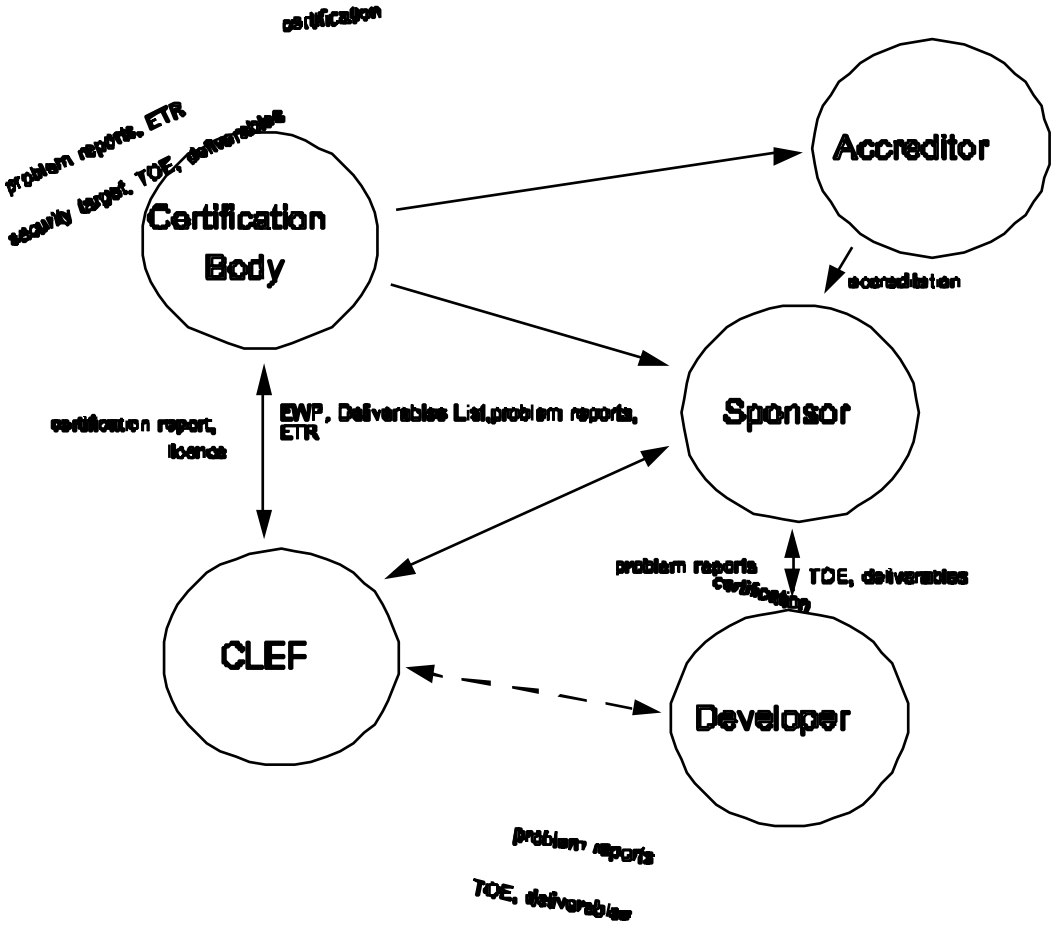

Figure 2 ITSEC Scheme Participants

Chapter 5 The Evaluation Process

Introduction

5.1 The evaluation process outlined here is a framework which describes organisational and procedural aspects which are followed during the conduct of an evaluation. There are many matters surrounding an evaluation which are treated differently in different nations for reasons of, for example, jurisdiction or national security. The rules of the national scheme take precedence in each of the countries. This guide is only concerned with the UK Scheme.

Participants

5.2 The following parties are directly involved in the evaluation process:

a) the sponsor of an evaluation

b) the developers of the IT product or system

c) the Commercial Licensed Evaluation Facility (CLEF)

d) the Certification Body.

5.3 The sponsor of an evaluation will usually be the vendor of a product, or the user or supplier of a system. The sponsor initiates the evaluation of a TOE by a CLEF, defines the security target, bears the cost of the evaluation and receives the certificate and certification report.

5.4 The developer (who may be a system integrator) is the organisation which produces the product or system to be evaluated and provides the requested deliverables for evaluation. The developer should be prepared to cooperate with the sponsor and agree to assist in the evaluation, for example, by providing technical support to the CLEF.

5.5 The CLEF performs the evaluation of the product or system.

5.6 The Certification Body monitors the evaluation process, reviews all evaluation reports to assess the implications of the results for security and to ensure conformance with the ITSEC/ITSEM, and issues the certificate and certification reports.

Other Parties

5.7 Other parties concerned with evaluation and certification are the users and system accreditors. They are mainly concerned with procurement issues and secure operation of systems.

5.8 Users make use of evaluated products and systems to protect their assets. Users are responsible for selection, startup, use and configuration of the products or systems they use.

5.9 System accreditors are responsible for the security of evaluated systems, generally for

government departments. Their responsibilities include the specification of system security policies and system modification rules, calculation of a system's required assurance level and approval of a system's operational use.

Phases of the Evaluation Process

5.10 There are three main phases to the evaluation process - preparation, conduct and conclusion. The process is outlined here for a typical evaluation although, in practice, there are a number of options, in particular when the evaluation is performed in parallel with the development process.

5.11 The Preparation phase includes the initial contact between the sponsor and a CLEF, any feasibility study undertaken, and preparation for the evaluation. The feasibility study is optional, but is particularly recommended for sponsors and developers without prior evaluation experience. The feasibility study will confirm that the sponsor and the developer(s) are well prepared for the conduct of an evaluation, and it will involve, as a minimum, a review of the security target. When a successful evaluation seems to be feasible, a list of required evaluation deliverables, a plan for their delivery, and an evaluation work programme are established. It is sensible to contact the Certification Body to establish a schedule agreed by the sponsor, the developer(s), the CLEF and the Certification Body. The evaluation work programme for a specific TOE is based on the deliverables, their delivery schedule and the ITSEC evaluator actions. The required work is divided into evaluation activities to be performed by the evaluators according to a schedule. A contract is usually agreed between the sponsor and the CLEF during this phase so that the required work is understood.

5.12 The Conduct phase is the main part of the evaluation process. This is when the evaluators perform the ITSEC evaluator actions, including penetration testing based on a list of potential vulnerabilities. All problems identified in this phase are discussed between the relevant parties. Responsibility for the resolution of problems lies with the sponsor, but if no resolution can be agreed, the sponsor may wish to abandon the evaluation or accept potential limitations in the certificate/certification report. The Evaluation Technical Report (ETR) is prepared by the evaluators during this phase and will record the results of the evaluation work and identify any unresolved problems.

5.13 In the Conclusion phase, the CLEF will provide the ETR as the final output of the evaluation process to the sponsor or developer and the Certification Body. The ETR is a basic input to the certification process. Since the ETR contains commercially and possibly nationally sensitive information, it is not a public domain document and is subject to the rules of the Scheme (as enumerated in Scheme publications).

Certification

5.14 During the certification process, the Certification Body reviews the ETR to determine whether the security target is met by the TOE, taking account of any factors outside the scope of the evaluation such as the strength of cryptographic mechanisms. The Certification Body also confirms that the evaluation has been performed in accordance with the rules of the UK Scheme

and as agreed in the Evaluation Work Programme.

5.15 As part of the certification process, the Certification Body is able to assign an assurance level to the TOE. The conclusions of the Certification Body are recorded in the certificate and certification report, which are released to the sponsor and the CLEF. Copies of the certificate are distributed to various interested parties including all the CLEFs and government Project Offices.

Re-evaluation

5.16 Re-evaluation of a TOE will be necessary if, after it has been certified, the TOE is updated, and/or its security target or other associated deliverables are modified and the new TOE is to be marketed as a certified product or used as a certified system.

5.17 Since evaluation results only apply to the release and version of the TOE that was evaluated, the sponsor should conduct an impact analysis if any change is made to the TOE or its operational environment in order to determine the type of change and the consequences for the certificate.

5.18 Depending on the type of change, it may be necessary for the sponsor or developer to notify the Certification Body of the change. If a re-evaluation is required, it will be necessary for the sponsor or developer to supply relevant deliverables to a CLEF.

Certificate Maintenance

5.19 The UK Certification Maintenance Scheme (CMS) is in the process of being introduced. This will require sponsors to either:

a) Make a formal commitment to maintenance of the certificate, or

b) Formally state that there is no commitment to maintain the certificate.

5.20 Future re-evaluation requirements will therefore be performed as part of the CMS, on the same principles as outlined in the Re-evaluation section above, but with an additional objective of reducing re-evaluation costs and timescales.

Chapter 6 Roles and Responsibilities of Developers

Introduction

6.1 This chapter covers the roles and responsibilities of developers in the capacity of both a sponsor and a developer but attempts to clearly identify the specific requirements upon developers, sponsors and vendors. It covers the responsibilities before, during and after evaluation.

Roles

6.2 A developer is responsible for the:

a) specification of the TOE

b) development of the product or system

c) production of the deliverables concerning the product or system, and requested for the evaluation

d) maintenance of the product or system

e) protection of his expertise and proprietary information.

6.3 A sponsor is responsible for the:

a) contracting the CLEF to perform the evaluation

b) definition of the security target

c) definition of the TOE

d) supply of the deliverables requested for the evaluation

e) copyright issues made of the certificate and certification report

f) maintenance of the evaluation rating.

6.4 A vendor is responsible for:

a) product distribution

b) product advertising

c) providing advice (concerning use of the product)

d) product installation.

6.5 UKSP 01 [Reference 0], Annexes D and E provide lists of the main obligations of sponsors and developers. These obligations are split into three periods: before, during and after an evaluation.

Responsibility for Supplying and Managing Evaluation Deliverables

6.6 The term 'deliverable' is used to refer to any item (including the TOE itself) that is required to be made available to the evaluators for evaluation purposes. This includes intangible items, such as support to the evaluators (e.g. training where necessary) and access to computers.

6.7 The ultimate responsibility to provide all the required deliverables for an evaluation lies with the sponsor. However, it is likely that most of the deliverables will be produced by the developer, where the sponsor is not the developer. For example, the developer may produce the design, source code and test documentation. Clear delineation of responsibility should exist between a sponsor and developer to ensure that deliverables are produced in a timely manner and to the necessary quality to satisfy the sponsor's contract with the chosen CLEF. Similar measures should be established where subcontracted developers are involved.

6.8 Responsibility for the running costs and risks (e.g. loss or damage through fire, flood, or theft) in all deliverables should be adopted by the sponsor and developer, unless specifically agreed otherwise. It should be noted that some deliverables, such as new or special-purpose types of hardware may not have an easily identified replacement cost and may well present insurance risks that cannot be transferred to other parties.

6.9 For any contract between a CLEF and a sponsor, the following details may have to be clarified:

a) the medium and format of computer-readable deliverables

b) the schedule for production and supply of the deliverables

c) the number of copies of deliverables to be supplied

d) the number of draft versions of the TOE and its deliverables that may be supplied and evaluated

e) identification of any products required be used in conjunction with the TOE, and arrangements for access to these

f) arrangements for discussing the development environment with the developer(s)

g) access to the operational and development sites

h) the type and duration of development support, including computer access and requirements for office accommodation for evaluators

i) copyright issues.

6.10 The sponsor should ensure that the arrangements with the developer(s) are both:

a) sufficiently definitive to ensure that the evaluators receive the required deliverables in the agreed timescales

b) sufficiently binding to ensure that inadequate deliverables result in a contractual shortfall.

6.11 Before an evaluation the sponsor should, in accordance with national legal regulations:

a) establish all necessary legal rights to the TOE and other deliverables, for the purpose of evaluation and to grant rights to (indemnify) the CLEF and Certification Body in this respect

b) (where appropriate) obtain the written consent of the developer(s) to any specific arrangements to limit access to proprietary information, but taking care not to enforce confidentiality agreements between sponsors, developers and subcontractors that are too restrictive, should the evaluators identify areas requiring corrective action.

6.12 In some cases the evaluators may require access to information provided by subcontractors, or third parties. The sponsor should take such cases into account.

6.13 The sponsor is responsible for supplying the deliverables to the evaluators during the evaluation process, and for providing the security target for the TOE to the developer(s) and the Certification Body.

6.14 The purpose of deliverables is to enable the evaluators to evaluate the TOE. Different types of deliverables satisfy this purpose in different ways, such as:

a) deliverables which provide evidence of effectiveness or correctness (e.g. an informal description of correspondence between source code and detailed design)

b) deliverables which allow the evaluators to establish additional evidence of effectiveness or correctness (e.g. access to the developed TOE)

c) deliverables which improve the overall efficiency of the evaluators' work (e.g. technical support from the developer).

6.15 It is the sponsor's responsibility to supply the evaluators with any required deliverables produced by subcontractors, or associated with third party products (e.g. source code).

6.16 Failure to provide the required deliverables within reasonable timescales, or failure to provide deliverables of adequate quality, may result in contractual problems, or in the TOE failing certification. Until acceptable deliverables are made available, it may not be possible to

complete a successful evaluation.

6.17 The sponsor must ensure that all of the expected deliverables are provided by the due dates agreed at the start of the evaluation. To fulfil this obligation, the sponsor and/or developer should:

a) confirm the correspondence between the Deliverables List and the project plan

b) confirm the correspondence between the Deliverables List and the outputs of the development process

c) confirm the correspondence between the expected level of information and the development methods.

6.18 On occasion, although acceding to the evaluation and the supply of deliverables to the CLEF, a developer may wish to limit the sponsor's access to proprietary information. At the appropriate time, the developer should ensure that the nature and extent of the proprietary information is defined, and should establish basic rules for protecting it.

6.19 As a consequence of the decision to have a product or system evaluated, the sponsor should ensure that the developer agrees to accept his responsibilities in the evaluation process.

6.20 Developers are expected to provide deliverables as evidence that the target assurance level has been achieved. This evidence should be prepared as part of the development process or after development if evaluation was not the original objective.

6.21 During the requirements phase for a system, it is the sponsor's responsibility (though often the developer of a product will also be the sponsor for its evaluation) to provide the security target deliverable(s).

Maintenance of Certificates

6.22 A certificate and certification report only apply to the release and version of the TOE that was evaluated; any changes to a certified TOE will fall under the procedures established under the Scheme for re-evaluation.

6.23 The sponsor may only market a product as a certified product on the basis of a valid certificate and shall ensure that configuration management procedures, appropriate to the assurance level, are in place to prevent unauthorised modifications. The evaluators or sponsor may be required to archive the evaluation material to allow re-evaluation.

6.24 If a TOE or its operational or development environment is subsequently changed, it is the responsibility of the sponsor to classify the type of change and determine the consequences for the certificate. This exercise will, in future, be performed as part of the UK Certificate Maintenance Scheme, which is in the process of being introduced.

6.25 The type of change determines whether the sponsor should notify the Certification Body of the change. It may also be necessary for the sponsor to arrange for a re-evaluation.

6.26 The sponsor and/or developers involved in the maintenance process should consider establishing a dedicated security team to perform an impact analysis of all changes proposed or implemented.

6.27 The maintenance process may be aided by the individual responsibility assignment policy followed during development and may include a review process dedicated to the preparation of the information required for the re-evaluation of the TOE, including:

a) a summary of changes since the previous evaluated release

b) a description of all security relevant changes and an impact analysis of those changes.

6.28 Sponsors and developers are encouraged to consider re-evaluation and certificate maintenance during TOE development and preparation for the initial evaluation. Once the CMS is in place, sponsors will be required to either:

a) Make a formal commitment to maintenance of the certificate, or

b) Formally state that there is no commitment to maintain the certificate.

Selling Certified Products

6.29 Sponsors, developers or vendors who sell certified products have the following duties:

a) to provide the security target, where appropriate

b) to provide the certificate/certification report when requested by potential users

c) not to make misleading claims about the product (e.g. claiming a product is certified when it is not, or exaggerating the benefits of the product)

d) to report known problems in certified products to potential users

e) if a vulnerability is found in a certified product, to inform existing users and the Certification Body of it

f) when a certified product changes, not to claim the new product as certified until the certificate and certification report have been upgraded.

6.30 The security target, as the guiding document for the evaluation, forms a valuable source of information for vendors and purchasers.

Installing and Configuring Products

6.31 Installation and configuration are generally performed by developers, vendors or (for simple products) users.

6.32 Those installing and configuring products should:

a) follow the product's instructions accurately

b) select configuration options in accordance with the product's configuration documentation, and record what was done so that the product configuration will be known thereafter

c) follow the appropriate procedure for checking the authenticity of the product, and address any discrepancies found.

6.33 At this stage the 'operational environment' documentation will be of most use to the user.

Providing Advice

6.34 Users who are considering purchasing certified products will often request advice from developers, vendors or CLEFs.

6.35 Those providing advice have the following duties:

a) to provide impartial advice, i.e. the advice given should be in the user's best interests; any interest the advisor has in a particular product should be explained to the user.

b) not to provide advice outside the advisor's field of competence.

Publications and Publicity

6.36 It is a requirement of the Scheme that CLEFs, sponsors, developers, or their agents obtain Certification Body agreement to a suitable form of words for all press releases and similar statements that refer to evaluation or certification. No statements can be made in press releases or other promotional material which would in any way misrepresent the conclusions of the evaluation or certification or might otherwise bring the Scheme into disrepute.

6.37 The issue of a certificate does not imply Certification Body or CLEF endorsement of a TOE, and only applies to the version of the TOE that was evaluated. For a product, the certificate may also identify a platform which must be used in order to retain the product's certified status. Sponsors are required to market products as certified products only on the basis of valid certificates.

6.38 Certificates and Certification Reports are the property of the Certification Body. Their reproduction and distribution by the sponsor is authorised provided that the report is copied in its entirety.

6.39 A series of UK Scheme Publications (UKSPs), including the document *Description of the Scheme* (UKSP 01), is available from the Certification Body.

UK Certified Product List

6.40 The *UK Certified Product List* (UKSP 06) [Reference 0] provides information on products that have been evaluated and certified under the Scheme. It is updated periodically and sponsors are invited to propose entries for agreement by the Certification Body. At the request of sponsors, details of products in evaluation can also be included.

6.41 Inclusion of any product, regardless of status, in UKSP 06 is ultimately at the discretion of the Head of the Certification Body.

Chapter 7 Preparation for Evaluation

Objectives

7.1 The primary objectives of preparing for an evaluation are to confirm the appropriate level of assurance for the evaluation and to obtain agreement from the Certification Body that the TOE would be certifiable, in principle, under the Scheme.

Independent Advice

7.2 Sponsors and developers new to the security evaluation process may find it beneficial to obtain independent consultancy advice regarding the required evaluation deliverables. If this type of advice is obtained from a CLEF, it must not be such as to affect the selected CLEF's independence in the evaluation. Guidance on this subject is available from the Certification Body and Part II of this Guide provides details on the contents of the evaluation deliverables.

Correctness Documentation

7.3 The set of design and development documentation for the TOE is referred to as correctness documentation. The purpose of correctness documentation within the evaluation is to show that the requirements have been correctly and completely implemented. It is likely that correctness documentation will be produced as part of the normal TOE development process. Consequently, apart from guidance on its applicability to the ITSEC, sponsors and developers do not generally require assistance to produce correctness documentation.

Effectiveness Documentation

7.4 Unless a sponsor has previous evaluation experience, it is likely that advice and guidance will be required regarding the effectiveness documentation. Effectiveness documentation is not part of the normal development process (except where evaluation is an objective), and concerns the ability of the TOE components to work together to provide complete protection against the identified threats.

7.5 Advice may be sought on the content of the effectiveness documentation, as well as on the timing of its production. Ideally, the various effectiveness analyses should be produced as part of the development process. This will enable the developer to produce correctness documents which take account of effectiveness issues. Each effectiveness document should be produced as soon as the correctness documentation from which it derives is ready.

Preparation

7.6 The sponsor must select a CLEF to initiate the evaluation of a TOE. Once the sponsor has selected a CLEF, he must then supply this CLEF with the security target for the TOE under evaluation.

7.7 If the sponsor wishes to put the evaluation of the TOE out to competitive tender before

selecting a CLEF, it is strongly recommended that the security target (possibly in draft form) for the TOE under evaluation is included with the tender documentation. This will allow the competing CLEFs to assess the work involved in the evaluation of the TOE. From the initial security target, a CLEF assesses the likelihood of a successful evaluation, requesting relevant information from the sponsor. If a CLEF is satisfied, it will agree a contract with the sponsor to perform the evaluation. Optionally, the CLEF may review the security target and advise the sponsor about changes necessary to ensure a firm basis for the evaluation.

7.8 The selected CLEF will formally advise the Certification Body of the sponsor's intention to submit the TOE for evaluation. After the Certification Body has, in principle, accepted the evaluation into the Scheme, a certifier is appointed.

7.9 In order to gain full acceptance into the Scheme, the Certification Body will need more information about the intended evaluation and the TOE itself. The CLEF prepares an Evaluation Work Programme (EWP) which details the work that the CLEF will undertake during the evaluation. The CLEF also prepares a Deliverables List which identifies the deliverables required for the evaluation.

7.10 The EWP is submitted to the Certification Body together with the Security Target, so that the Certification Body can determine whether the proposed evaluation work is adequate for the target assurance level. The Certification Body may require the CLEF to alter its scope of work or the amount of planned effort to ensure that, for example:

a) the requirements of the ITSEC, ITSEM and the Scheme are being correctly applied and/or any anticipated deviations have been agreed

b) the planned effort is commensurate with the evaluation requirements.

7.11 The Deliverables List is submitted to both the Certification Body and the sponsor, and provides a description of the deliverables required from the sponsor and their delivery dates. The Deliverables List will allow the sponsor to plan resources and timescales for the production of the required deliverables if this has not already been done.

7.12 During the start-up process, a formal Task Startup Meeting is held between the certifier, the CLEF, the sponsor and optionally the developer, to discuss any issues arising from the formal acceptance of the evaluation into the Scheme, and to ensure that the sponsor and developer have a clear understanding of the evaluation and certification process and what they are required to do.

7.13 If the development of the TOE is spread over a considerable period, e.g. several years, then the overall evaluation may be broken down into a series of 'jobs'. Each job may have its own EWP and Deliverables List.

Re-Evaluation and Reuse Deliverables

7.14 Re-evaluation of a TOE may be necessary when the TOE or its associated evaluation deliverables change. Examples of changes include increasing a TOE's target assurance level or adding security enforcing functions to a TOE's security target. The sponsor performs an impact analysis and determines the appropriate course of action in order that the previous evaluation results can be reaffirmed according to the guidance contained in the ITSEM [Reference 0], Part 6, Annex 6.D.

7.15 Reuse of evaluation results can enable the evaluation effort to be reduced for an evaluation of a TOE containing one or more previously evaluated TOEs. The results of the original evaluation may or may not be valid in the context of the evaluation of the new TOE. The complexity and variety of potential TOE compositions limits the guidance that can be given in this document. The following general guidance can be given:

a) If the assurance level of a previously certified component is greater than, or equal to, the target assurance level of the TOE, then the previous correctness results for that component, confirmed by its certificate/certification report, can be used directly in the evaluation of the new TOE.

b) When a certified product or system is used as a component of a new TOE, the context of its use will have changed. Hence, whilst the correctness of the certified component with respect to its original security target is still valid, its effectiveness with respect to its new security target in the context of its new use needs to be reaffirmed.

c) The sponsor will be expected to provide the deliverables for the new TOE for the target assurance level together with the certificates/certification reports for any certified components.

d) It may be necessary to supply the correctness deliverables for the TOE's components in order to support the effectiveness analysis for the new TOE.

e) The new TOE deliverables for effectiveness will need to cover the effectiveness of the pre-evaluated component(s) as they are used in their new context. For instance, the security target for the new TOE will have to be demonstrated to make suitable use of the pre-evaluated component(s). Similarly, the binding between *all* the new TOE components must be addressed by the sponsor.

7.16 The following examples are intended to provide a brief overview of the cases where a re-evaluation may be required.

a) A TOE may be modified to produce a new version. The original certificate is only applicable to the version that was evaluated and so a re-evaluation would usually be required for the later version to be certificated. The extent of any re-evaluation would be dependent upon the extent of the changes made to the TOE.

b) It is possible that, after certification of a TOE, an exploitable vulnerability is discovered. This may lead to the withdrawal of the original certificate until a re-evaluation has been conducted to confirm that the vulnerability has been neutralised.

c) Some certificates may only be valid for a period of time, e.g. because of a continually changing threat.

7.17 The Certification Report may state that certain proposed changes may be implemented without invalidating the Certificate, provided that the Certification Body is informed and that suitable reference material is made available for inspection. This may, on occasion, reduce re-certification to a trivial, largely administrative exercise.

7.18 Further guidance on re-evaluation and reuse is available from the Certification Body.

Certificate Maintenance Scheme

7.19 The UK Scheme is being enhanced to introduce a Certificate Maintenance Scheme (CMS). This will allow for the re-evaluation of TOEs, the purpose being to minimise the work involved in re-evaluation and subsequent cost to sponsors. The CMS is in the process of being introduced, and further information is available from the Certification Body.

Chapter 8 Evaluation Timescales

Introduction

8.1 There are several factors that contribute to the length of time and degree of effort required to perform an evaluation and, therefore, to the sponsor's cost. The major factors are the target assurance level and the size and complexity of the TOE, since these factors require the sponsor to produce more evidence to the selected CLEF which, in turn, must perform more work to check that sufficient evidence has been provided to satisfy the ITSEC requirements.

8.2 Other factors affecting evaluation timescales include:

a) the number of Security Enforcing Functions (or testable security features) claimed in the security target

b) whether it is a concurrent or consecutive evaluation

c) whether it is a re-evaluation or whether results from other evaluations can be reused (e.g. by using previously evaluated and certified products)

d) whether it is to be a continuous evaluation (e.g. a large system may have a long development timescale where the required inputs to the evaluation are to be delivered at widely spaced intervals)

e) the number of problem reports produced and the general quality of the TOE and its documentation.

8.3 Prior to an evaluation, the sponsor is responsible for the preparation of the security target and for planning the development of the corresponding TOE. The sponsor must take account of the cost of the evaluation itself and the additional requirements which evaluation imposes on the sponsor and developer.

Concurrent Evaluations

8.4 With a concurrent evaluation, the deliverables are provided as the development progresses. The sponsor should provide specific deliverables at the times agreed at the start of the evaluation and documented in the agreed Deliverables List. Any problems identified during a concurrent evaluation would normally mean that only one level of representation is affected, minimising the number of deliverables that need to be modified. Concurrent evaluation provides the opportunity for the sponsor or developer to react rapidly to problems discovered by the evaluation team, before those problems are replicated in lower level representations.

Consecutive Evaluations

8.5 With a consecutive evaluation, all the deliverables are normally available at the start of the evaluation. Any problems identified during the evaluation could mean that a number of documents (and possibly the TOE itself) are affected and, hence, several deliverables may need to be modified.

Re-evaluation

8.6 A re-evaluation may involve a full assessment of the TOE which has been previously evaluated. Therefore, this could be expected to take up to the same time as the original evaluation. Factors that can affect re-evaluation timescales include:

a) whether any of the original evaluation work is still valid, so that previous evaluation results may be reused (e.g. where a new version of a product is issued and the changes can be deemed to be compartmentalised, thereby minimising the areas of security enforcing and security relevant functionality affected)

b) significantly different functionality (e.g. if a product has been upgraded significantly and the sponsor wishes the later version to be certified, a full evaluation would almost certainly be required)

c) a higher target assurance level than the original is required (this would involve more work than the original evaluation and, therefore, must be expected to take significant additional time).

Long-Term Evaluations

8.7 Evaluations of long-term development projects (e.g. several years) are usually split into more manageable groups of activities called 'evaluation jobs'. See Part III of this Guide for further details.

Typical Product Timescales

8.8 The following timescale ranges give a very general indication of the time taken for the evaluation process for products, i.e. from the start of evaluation to delivery of ETR to the Certification Body (this is elapsed time, not effort requirements).

a) E1: up to 6 months

b) E2: 6 - 18 months

c) E3: 8 - 24 months.

8.9 The time taken for an evaluation can vary considerably depending on a variety of factors including: assurance level, type of TOE, number of SEFs, amount of documentation, adequacy

of deliverables, resolution of problems. The times indicated above are based on an average product, with an average number of SEFs, average to good documentation, and speedy resolution of problems. They are also based on a full evaluation; these times can be considerably reduced for a re-evaluation, where evaluation results are reused, the amount of reduction depending on the amount of reuse.

8.10 The Certification Body does not guarantee the duration of the certification process. However, the aim is to produce the Certification Report within eight weeks of receiving the Evaluation Technical Report from the CLEF. Where possible, the Certification Body will attempt to meet certification deadlines imposed on the sponsor.

Chapter 9 Project Management Issues

Introduction

9.1 The decision to submit a TOE for evaluation, or to bid for a contract to develop a TOE for a sponsor, is important and can have significant consequences for the management of the project.

9.2 This chapter discusses the management of development projects in relation to evaluation and provides guidance to assist project managers. It covers:

a) planning issues

b) preparation of deliverables

c) likely training requirements

d) issues to be considered by the sponsor when analysing the project risk associated with the evaluation

e) handling problem reports from the evaluation team

f) how the Certification Body uses Scheme Information Notices to provide guidance or interpretation on the Scheme

g) evaluation meetings.

Planning

General

9.3 Evaluations depend on the timely supply of deliverables to the evaluation team. A sponsor planning the acquisition of a TOE, or a developer planning the development of a TOE should make due allowance for the factors listed below. Failure to provide timely, complete, consistent and correct deliverables is likely to result in an evaluation being temporarily suspended or incurring extra costs from the CLEF.

9.4 The following issues should be considered when planning an evaluation:

a) establishing all necessary legal rights to the TOE, its components and other deliverables including those produced by the CLEF (see below)

b) the copyright of evaluation outputs, e.g. ETR, problem reports (Note that attention should be paid to the copyright of any material produced by third parties)

c) arranging commercial confidentiality with subcontractors, etc.

d) access to previous evaluation results for the evaluation team and certifier (e.g. for re-evaluation of a TOE or where an evaluated product is a component of the TOE)

e) establishing a technical point of contact

f) preparation of correctness deliverables

g) preparation of effectiveness deliverables

h) time for problem resolution

i) technical and logistical support to the evaluation team and certifier

j) access to the development site by the evaluation team, including access to the development tools, and facilities for interviewing (some of) the development staff

k) access to the TOE in its operational environment

l) penetration test requirements

m) attendance at meetings (refer to the relevant section in this chapter)

n) time allowance for the evaluation team to prepare the Evaluation Technical Report at the conclusion of the evaluation, and for the Certificate and Certification Report to be prepared by the certifier.

Concurrent vs. Consecutive Evaluations

9.5 An evaluation might be performed after development of the TOE has been completed, which is called a *consecutive evaluation*, or in parallel with the development of the TOE, which is called a *concurrent evaluation*.

9.6 The main difference between concurrent and consecutive evaluations is the availability of the various representations of the TOE provided as deliverables. In a consecutive evaluation all deliverables required by the ITSEC, from the security target to the operational TOE, are normally available right from the start of the evaluation. In a concurrent evaluation the deliverables will be provided by the sponsor/developer as the development progresses. Concurrent evaluations provide the opportunity for the sponsor/developer to react rapidly to problems discovered.

9.7 The difference between the two types of evaluation does not have any technical impact, but affects the organisation of an evaluation, i.e. the evaluation work programme. In the concurrent evaluation both the order and the timescale of the evaluation activities are oriented towards the delivery of the deliverables. Penetration and other testing cannot be performed before the operational TOE is available. The potential consequences of delays and iterations need to be considered.

Preparation of Deliverables

9.8 Part II of this Guide discusses the deliverables necessary for evaluation.

9.9 Prior to the start of the evaluation, the evaluation team will prepare a Deliverables List after discussion with the sponsor, and developer (if necessary). The Deliverables List will identify the deliverables required and the timetable for their supply.

Concurrent Evaluations

9.10 Concurrent evaluations offer the ideal opportunity for the deliverables to be prepared in phase with the development life cycle of the TOE.

9.11 The majority of the ITSEC deliverables result from conventional development outputs and do not require significant alteration or delay in their production.

9.12 In addition to the standard documentation outputs which a developer may produce, the ITSEC also requires the production of a set of deliverables known as effectiveness documents. It is recommended that production of these documents is started as early in the development life cycle as is consistent with their required content. The early delivery of effectiveness documents to the evaluation team will not only expedite the evaluation, but will also enable the developer to take prompt action on any problems with the TOE's effectiveness discovered by the evaluation team.

Consecutive Evaluations

9.13 Consecutive evaluations differ from concurrent evaluations as the TOE and any development documentation already exists.

9.14 If the existing documentation provides all the necessary information to met the ITSEC correctness criteria, then it can be immediately delivered to the evaluation team.

9.15 If the existing documentation requires additional information to meet the ITSEC correctness criteria, e.g. traceability data, then either the documentation may be updated or additional documentation may be provided. If the latter approach is selected, care must be taken to ensure that the additional documentation is consistent with the existing documentation, and that it is clear and unambiguous.

9.16 The majority of the ITSEC deliverables result from conventional development outputs and do not require significant alteration or delay in their production.

9.17 With consecutive evaluations, the effectiveness documentation will usually not exist and will have to be prepared retrospectively. The party responsible for its preparation should contact the Certification Body for advice.

Training

9.18 Project Managers should consider the provision of training for two groups involved in evaluations:

a) their staff (either as sponsors or developers)

b) the evaluation team and certifier.

Sponsors and Developers

9.19 The ITSEC does not prescribe any specific training of staff or evidence of their skill and experience.

9.20 However, staff involved with the preparation of security targets and the development of secure TOEs may find training useful in the following areas:

a) application of any relevant quality procedures

b) application of any relevant security procedures

c) formally specified models of security

d) design methods, especially those involving semiformal and formal notations

e) use of automated tools, e.g. configuration control, animation, analysis and test tools.

9.21 The sponsor and developer should note that development of underlying formally specified models of security is impractical unless they have received substantial training or lengthy practical experience in the use of the chosen formal notation, and have adequate tool support.

Evaluation Team and Certifier

9.22 The developer and sponsor are not normally required to organise formal training courses specifically for the evaluation team and certifier. However, the evaluation team and certifier may wish to attend any training courses provided for other staff, for example where:

a) development staff are being trained, e.g. on a particular development method

b) user training is being provided, e.g. on the security administration of the TOE.

9.23 Informal training, preferably from someone in the development team, may be required in a number of proprietary areas where documentation is not available at that time, such as:

a) the hardware and operating system(s) used in the TOE and its development

b) development methods used

c) development tools used.

9.24 Informal discussions with the sponsor or developer may be required on any aspect of the TOE. Typically the evaluation team may require the sponsor or developer to provide a short description of a particular part of the TOE and then to answer any questions from the team.

9.25 It is recommended that the sponsor makes arrangements for responsibility for training requirements prior to the start of the evaluation. This might include support from specialist sub-contract developers.

9.26 On occasion, the evaluation team may request that a TOE is made available for training at the CLEF's premises. Note that some TOEs, such as new or special purpose types of hardware, may not have an easily identified replacement cost and may well present insurance risks that cannot be transferred to the CLEF.

Sponsor's Evaluation Project Risk Analysis

Introduction

9.27 This section provides generic information for sponsors performing a risk analysis on the evaluation aspects of the production of a TOE. Sponsors are recommended to perform a risk analysis to maximise the chances of a successful evaluation. The section presents the risks that can lead to problems during an evaluation, and expands each one where appropriate to give a clear and concise definition of the problem.

9.28 Having identified and described the risks in each sector, the section then describes the countermeasures that could be employed to ensure such risks do not have an adverse effect, both before and during an evaluation.

9.29 The risks associated with the sponsor, the CLEF, and the Certification Body are addressed in this section. There are risks that are associated with each of these bodies which could cause an evaluation to either fail or be delayed to such an extent that timescales and hence contractual obligations are not met.

9.30 The risks associated with the developer are not specifically addressed as the sponsor is responsible for ensuring that the developer meets the ITSEC criteria.

9.31 Each of the risks associated with the relevant party are identified below, together with approaches which could be used to minimise the probability of their occurrence or their impact on the success of the evaluation.

Risks - The Sponsor

9.32 The risks in an evaluation, over which a sponsor has control, centre around the deliverables

supplied to the CLEF. The primary risks associated with the deliverables are as follows:

a) non availability

b) late supply

c) inconsistencies

d) inadequacies.

9.33 Each of these primary risks is expanded below, with their implications for the evaluation.

9.34 The non availability of deliverables will result in the basic requirements for the evaluation not being met, leading to failure of the evaluation.

9.35 The late supply of deliverables can result in the required level and depth of work not being carried out within the original contract's timescales and costs. This can lead to either extra time (and cost to the sponsor) being required to complete the work, or, if this is not forthcoming, the failure of the evaluation.

9.36 Significant problems can be caused by the late supply of documentation relating to a third party certified product which is being used as a component of the TOE under evaluation. The documentation likely to be needed in such a case includes the product's security target, effectiveness documentation, ETR and Certification Report.

9.37 Inconsistencies in the deliverables, such as conflicting statements within the design documentation, can lead to delays and, hence, possible time and cost implications for the evaluation. In the worst case, failure of the evaluation could occur. The final risk, that of inadequate deliverables, can be expanded into the specific areas of design, implementation and development environment. Each of these areas is discussed below.

9.38 The deliverables may reflect an inadequacy in the design of a product or system where:

a) The design is insecure - it does not meet all of the threats identified.

b) There is some fault in the design itself, such as an error in the design of a security feature that renders the system or product insecure.

c) There are inconsistencies between the representations of the design, for instance the high level and low level design of a feature may not agree.

d) The design documentation has inadequate traceability between representations, making it difficult or impossible to trace the existence of a feature from the highest level document (i.e. the security target) through to the implementation.

e) The design does not have the required level of modularity, resulting in (at the higher

assurance levels) the required level of separation between the security enforcing and the other functionality not being achieved.

9.39 The deliverables may reflect an inadequacy in the implementation of a product or system where:

a) the actual implementation of a security feature is weak, resulting in a security enforcing feature being unacceptably easy to bypass or overcome.

b) an implementation contains faults, such as bugs, which result in the security of the product or system being compromised.

9.40 The deliverables may reflect an inadequacy in the development and operation of a product or system if:

a) The development environment of the product or system (and of any other products used) does not have the controls in place to meet the requirements for the particular level. This will have implications on the integrity of the product or system, and can apply to the delivery of the product or system.

b) In the case of a system, there is no definition of the controls that must be imposed on the use of the operational system to ensure that the system is used in a secure fashion.

9.41 Inadequacies of the types described above could result in failure of the evaluation. They will invariably lead to delays to the completion of the evaluation.

9.42 Where a third party product is used in the TOE under evaluation, last minute changes to the product's security target may mean that the TOE's security requirements are no longer met by that product. This may necessitate rework by the TOE developer and by the evaluators.

Risk Reduction - The Sponsor

9.43 As can be seen, there are a number of risks that can result either in delays to the completion of the evaluation, or in failure of the evaluation.

9.44 To counter the risk of non availability of deliverables, the sponsor should request the CLEF to identify the deliverables that the sponsor is required to supply before the evaluation commences. The Deliverables List from the CLEF will provide a definitive list of required deliverables along with a schedule for the delivery of all items. It is supplied to, and agreed by, the sponsor before the start of the formal evaluation.

9.45 To ensure that deliverables are supplied in a timely manner, the sponsor should liaise closely with the CLEF to produce a timetable for the evaluation that is acceptable to both parties. Any constraints (i.e. limited time on the sponsor's TOE to carry out penetration tests, or licensing constraints on the time that the CLEF is allowed to hold source code) should be jointly identified with the CLEF, and the evaluation planned with such limitations in mind.

9.46 In addition, the sponsor and CLEF should hold regular progress meetings to ensure that any problems with the supply of deliverables are identified as early as possible, to enable remedial action to be taken. These can be included within the framework of the Evaluation Progress Meetings.

9.47 Where a third party product is used in the TOE under evaluation, the TOE sponsor may wish to hold regular progress meetings with the sponsor/developer of the product to ensure that the system timescales will be met, and discuss the impact of any changes to the product and its security target. It may be possible for the TOE sponsor to include in his contract with the product supplier requirements and deadlines for certification of the third party product.

9.48 If a sponsor is unsure of the precise requirements for the evaluation deliverables, he may wish to employ additional consultancy support to help produce them. Alternatively, the sponsor may seek advice on the required content and presentation of the deliverables so as to minimise the effort he must expend to comply with the ITSEC requirements. In this way, inadequacies in the deliverables can be identified before the start of the formal evaluation, and can be rectified by the sponsor. If inadequacies come to light during the formal evaluation, they will result in problem reports, which are treated as described above. The Certification Body, through CESG, holds a list of registered companies which are approved to act in the capacity of ITSEC consultancy support.

Risks - The CLEF

9.49 The potential risks involved in having the evaluation carried out by the CLEF centre around the provision of staff to carry out the evaluation. These risks can be summarised as follows:

a) the inability of the CLEF to have the staff required to start an evaluation on the date required by the sponsor

b) the loss of the CLEF's Project Manager during the evaluation

c) the loss of a member of the evaluation team.

9.50 These risks could impact on the timescales of the evaluation.

Risk Reduction - The CLEF

9.51 In order to ensure there is no delay in starting an evaluation when the sponsor requires it, sponsors should ascertain the availability of evaluators within the chosen CLEF.

9.52 In order to ensure there is minimal impact on an evaluation if the Project Manager of the evaluation should be unable to continue that role, sponsors should ascertain the measures which the chosen CLEF would follow under those circumstances.

9.53 If an evaluator becomes unavailable, then it should be possible to provide a replacement without

undue disruption to the evaluation learning curve as all evaluations in each CLEF are carried out to UKAS approved standards governing accountability and repeatability, and all actions carried out by an evaluator are fully documented.

Risks - The Certification Body

9.54 The final area of risk which needs to be addressed revolves around the Certification Body. The Certification Body ensures that the CLEF works within the constraints of the UK IT Security Evaluation Scheme, and as such it must approve all of the outputs from the CLEF.

9.55 The main areas of risk can be summarised as:

a) delays in the approval of the Evaluation Work Programme, leading to slippage of the start date of the formal evaluation

b) delays in the release of the final Certification Report, delaying the certification of the product or system

c) misinterpretation of a problem report or the Evaluation Technical Report, again giving rise to delays in the certification of the system or product

d) the loss of the Certifier.

9.56 These risks could impact the timescales of the evaluation. The misinterpretation of reports could lead to the product or system incorrectly failing to achieve certification.

Risk Reduction - The Certification Body

9.57 In order to prevent delays during the Certification Body's review of CLEF reports, time should be set aside for the review in the initial plans. Also, the Certification Body, aware of the requirements on them, adopts a sound commercial attitude towards the quickest possible turnaround consistent with the Scheme's requirements.

9.58 If a Certifier becomes unavailable, then his deputy for the evaluation task will take over the duties, thereby minimising the disruption to the evaluation of the TOE.

Conclusions

9.59 Good project management principles should be adopted to minimise unforeseen delays and increase the probability that the evaluation results in successful certification.

9.60 The route to successful evaluation relies on good communication being maintained between the sponsor, the developer, the CLEF and the Certification Body. This will result in the sponsor achieving an understanding of the requirements placed on him for the evaluation, the CLEF receiving good quality deliverables in a timely manner, and the Certification Body responding to problems quickly.

9.61 If the above methods are used, then the chances of successful evaluation are greatly increased.

Problem Reports

Objective

9.62 During the course of an evaluation, the evaluation team may discover various problems relating to the TOE. Some of these problems may concern vulnerabilities or errors, whilst others may concern other aspects of the TOE (e.g. the development environment, operational documentation). Whatever the problem, it is essential that it receives appropriate, prompt attention from the sponsor, the developer, the Certification Body and other parties as necessary.

9.63 The objective of problem reporting is to ensure that the sponsor, the Certification Body and other parties as appropriate are notified as soon as possible, in order that appropriate timely action can be taken.

9.64 The Scheme provides a system for notifying the sponsor and developer of problems by issuing formal problem reports to the affected parties. Two types of problem reports are generated by the evaluators, depending on the severity and nature of the errors discovered, as follows:

a) Security Fault Notification (SFN) - any failure of a TOE to comply with its security requirements (including its security objectives) when there is a real risk of a security violation (i.e. there is a potential vulnerability), is reported in an SFN

b) Evaluation Observation Report (EOR) - any other security issue (pertinent to the scope of the security target, and the evaluation criteria and method) is reported in an EOR.

Security Fault Notification

9.65 An SFN is used to report any failure of a TOE to comply with its security requirements (including its security objectives) defined in the security target, but only when there is a risk of a security violation (i.e. there is an exploitable vulnerability). An SFN will be reported as soon as a potential vulnerability is identified.

9.66 It is very important that the sponsor and developer take due regard of problem reports. The ITSEC [Reference 0] paragraph 3.9 states that:

"a TOE will … fail evaluation on effectiveness grounds if an exploitable vulnerability … has not been eliminated before the end of the evaluation".

9.67 Due to the seriousness of an SFN a sponsor or developer must respond to the report and agree to a timetable for the correction of the fault. All SFNs must be cleared to the satisfaction of the Certifier prior to a certificate being awarded.

Evaluation Observation Report

9.68 EORs are used to report all security related problems relating to a TOE other than exploitable vulnerabilities. Clearly, this use covers a wide range of problems. Examples of the use of EORs include:

a) to report problems regarding the development or the operation of the TOE

b) to report problems with the content, presentation and evidence of deliverables for evaluation

c) to report problems which may impact on assurance.

9.69 EORs may also be used to draw the attention of the sponsor and Certification Body to any concerns held by the evaluators regarding the TOE or the progress of the evaluation. However, EORs are not used to raise non security issues with the sponsor; this is done by other means of communication.

9.70 EORs include an assessment of the impact on security posed by the problem (major or minor). EORs should be cleared to the satisfaction of the Certifier prior to a certificate being awarded. Where there are outstanding EORs, and the aggregate of problems identified is considered significant, the Certifier may determine not to award a certificate. However, if the totality of the problems is not considered significant, the Certifier may award a certificate, but with a number of caveats which could affect how the TOE is to be operated.

Problem Report Status Register (PRSR)

9.71 The Problem Report Status Register ensures that problem reports are progressed efficiently and effectively. The PRSR is maintained by the evaluation team during the evaluation, and is considered at Evaluation Progress Meetings.

Issue Procedure

9.72 Evaluators may generate SFNs or EORs at any time during an evaluation. One problem report can be used to cover:

a) a single problem

b) more than one related problem.

9.73 Where more than one related problem is documented in an EOR then each problem is separately numbered. There should not be more than five related problems documented in an EOR. The PRSR will reflect the status of each EOR as a whole.

9.74 Problem reports usually carry a protective marking and must be handled accordingly. The Task Startup Meeting (TSM) is the usual forum where specific guidance for the evaluation is

provided on protective markings, so that the sponsor and developer understand the requirement at the start of an evaluation.

Discussion of Problem Reports

9.75 A technical meeting will usually be held between the CLEF and sponsor to discuss problem reports, and at which the Certification Body may also be represented. Subject to the agreement of the sponsor, representatives from the developer and the accreditation authority (for systems) may also be invited to attend. The purpose of such a meeting is to discuss the technical details of the problem reports and to determine future actions. Where agreement cannot be reached, further meetings may be required involving the Certification Body. Where appropriate, problems may be resolved via correspondence. However, final decisions on problem report resolutions must be endorsed by the Certification Body (usually at Evaluation Progress Meetings).

Scheme Information Notice (SIN)

9.76 The objective of a SIN is to provide timely guidance or interpretation on any aspect of the Scheme and its associated documentation, including the ITSEC and ITSEM.

9.77 SINs may be issued to a limited audience, depending on their content and any protective marking. SINs may also be issued at draft status and circulated for comment prior to their final release.

9.78 SINs are regularly reviewed and incorporated into Scheme publications, at which point they are withdrawn.

9.79 All recipients of this Guide will automatically receive copies of relevant formal SINs as they are released.

Evaluation Meetings

Overview

9.80 During an evaluation a number of meetings will occur that involve the sponsor and/or developer. These meetings will allow progress, problems and plans to be discussed. The types of meetings at which the sponsor and developer may attend include:

a) Task Startup Meeting - mandatory

b) Evaluation Progress Meetings

c) Evaluation Control Meetings

d) Task Closedown Meeting.

Task Startup Meeting

9.81 The objective of the Task Startup Meeting (TSM) is to enable the attendees to discuss issues arising from the formal acceptance of the evaluation into the Scheme.

9.82 A representative of the sponsor or developer should present an overview of the TOE, including:

a) the target hardware and software

b) the operational role (e.g. if the target is a system)

c) the current state of development (and, for a concurrent evaluation, the anticipated development timescales)

d) the required target assurance level

e) the security functionality and scope of the evaluation.

9.83 The CLEF representative should summarise:

a) the anticipated evaluation timescales and whether it is necessary to complete the evaluation by a particular time

b) any constraints on the evaluation, e.g. limited access to the developer or to deliverables

c) any specific evaluation staff experience that is required.

9.84 An example TSM agenda is shown in Figure 3.

9.85 The main items on this agenda of concern to the sponsor and developer are:

a) Evaluation Technical Support - although it may be too early to determine the level of technical support required, the developer should bear in mind that they may need to provide the evaluators with both consultancy support and training

b) Sponsor Issues - this subject concerns press releases, proposed entry in UKSP 06 (the Evaluated Products List), re-evaluation requirements, problem report handling, copyright of ETRs and evaluation documents and reuse of the ETR

c) Contacts - any constraints on contact between the evaluators and the developer and/or sponsor should be determined

d) Evaluation Meetings - the requirement to hold (and frequency of) Evaluation Progress Meetings (EPMs) and Evaluation Control Meetings (ECMs) should be determined with the first one (if required) to be scheduled where actions arising from the TSM can be followed up

e) Cryptos - any issues associated with the use of cryptographic hardware or software by the TOE, which will require liaison with CESG.

Evaluation Progress Meetings

9.86 Evaluation Progress Meetings (EPMs) are formal meetings between the sponsor, the evaluators, the Certification Body and (possibly) the developer and accreditor (for systems) in which progress and timescales are reviewed for both the project and the evaluation, problems are identified and discussed, and actions are placed as appropriate. They may be held periodically during the course of an evaluation.

9.87 The requirement for progress reporting should be agreed between the CLEF and the sponsor during task startup. For small evaluations, a CLEF may adopt a more informal means of progress reporting (e.g. by submitting written progress reports to the Certification Body and the sponsor).

9.88 EPMs should be organised by the CLEF in conjunction with the sponsor. The CLEF is responsible for producing and distributing the agenda in consultation with the sponsor, together with the Problem Report Status Register (PRSR).

9.89 The following EPM roles are usually assigned:

a) Chairman: a representative of the CLEF or sponsor

b) Secretary: a representative of the CLEF.

9.90 EPMs are called as required by each evaluation. The requirement for, and frequency of, EPMs may form part of the contractual agreement between the sponsor and the CLEF, or may be called on an ad hoc basis.

9.91 Depending on the approach taken in the particular project, the sponsor and the CLEF may agree that the substance of the EPM should be covered in alternative forums. For example, it may be possible to cover certain issues in the sponsor's or developer's own project progress meetings.

9.92 An example EPM agenda is shown in Figure 4.

Evaluation Control Meetings

9.93 Evaluation Control Meetings (ECMs) are primarily a forum for the CLEF and the Certification Body to discuss detailed technical work relating to a particular evaluation. Exceptionally, a sponsor or developer will be invited to attend.

9.94 The agenda is at the discretion of the party calling the meeting and so no example agenda is presented here.

Task Closedown Meeting

9.95 The primary objective of the Task Closedown Meeting (TCM) is to enable the organisations involved with an evaluation to assess the overall conduct of the evaluation.

9.96 Representatives of the sponsor and/or developer organisations are welcome to attend the TCM.

9.97 An example TCM agenda is shown in Figure 5.

9.98 The main items of concern on this agenda to the sponsor and developer are:

a) Evaluation Issues - there may be implications for re-evaluating the TOE or part of the TOE; there may be concerns over the liaison between the sponsor, developer and other parties involved in the evaluation; there may be views on the operation of the Scheme

b) Sponsor Issues - this is an opportunity to provide feedback from the sponsor to the CLEF and the Certification Body on the conduct of the evaluation, and the Scheme in general

c) Disposal of Material - the attendees should agree which items of evaluation material are to be archived.

Chairman's Introduction
TOE Overview
2.1 Operational Role / Method of Use
2.2 Security Architecture (Hardware, Firmware, Software)
2.3 Development Status and Timescales
2.4 Target Assurance Level and Specific Security Functionality
Evaluation Requirements
3.1 Independence and Impartiality
3.2 Consultancy
3.3 Relevant SINs
3.4 Suitability for Evaluation
3.5 Scope of Evaluation
3.6 Constraints and Limitations
3.7 Specific Evaluation Staff Experience
3.8 Evaluation Timescales
Certification Issues
4.1 Status of Security Target and EWP
4.2 Evaluation Re-use
4.3 Evaluated Products
4.4 Certification Timescales
4.5 Accreditation Timescales / Requirement for Interim Certification
Evaluation End Products
5.1 ETR and ESR Timescales
5.2 EMR/DMR Requirements
Confidentiality
6.1 Confidentiality Agreements
6.2 Secret Matters / Proprietary Information
6.3 Minimum Clearance Required
6.4 Clearance Required for Meetings
6.5 Clearance Required for Development and Operational Site Visits
6.6 Clearance Required for Penetration Tests
6.7 Protective Markings of Evaluation / Certification Documents
Evaluation Technical Support
7.1 Consultancy from Developer
7.2 Tools from Certification Body
7.3 Vulnerabilities from Certification Body
7.4 Training from Developer

Figure 3 Task Startup Meeting - Example Agenda (Part 1 of 2)

Sponsor Issues
8.1 Press Releases
8.2 UKSP 06 Product in Evaluation Entry
8.3 Re-evaluation Requirements
8.4 Problem Report Handling and PRSR
8.5 Copyright of Evaluation Documents (inc ETR, ESR)
8.6 Request for Previous ETRs and CRs
8.7 Rights to Reuse of Final ETRs
8.8 Distribution of UKSPs and SINs
Planning
9.1 Assignment of Evaluators
9.2 Evaluation Plan
Contacts
10.1 Certification Body
10.2 Non-Certification Body
10.2 Liaison Rules
Evaluation Meetings
11.1 Evaluation Progress Meetings
11.1.1 Frequency and Venue
11.1.2 Distribution of Agenda with Evaluation Plan, Status and PRSR
11.2 Evaluation Control Meetings
Any Other Business
Action Summary
Date of First EPM

Figure 3 Task Startup Meeting - Example Agenda (Part 2 of 2)

Chairman's Introduction
Minutes of Previous Meeting
Matters Arising
Project Progress and Timescales
Evaluation Progress and Timescales (Evaluation Progress Statement and Evaluation Plan)
Deliverables Issues
Status of Problem Reports (PRSR)
Certification Issues
Any Other Business
Summary of Actions
Date, Time and Venue of Next Meeting

Figure 4 Evaluation Progress Meeting - Example Agenda

1 Chairman's Introduction
Summary of the Evaluation
Certification Body Feedback
Evaluation Issues
Sponsor Issues
Scheme Issues
Disposal of Material
Any Other Business

Figure 5 Task Closedown Meeting - Example Agenda

Chapter 10 Contractual Issues

10.1 While this chapter identifies many of the contractual issues involved in the evaluation and certification process, the guidance is not fully comprehensive and does not obviate the need for participants in the process to obtain appropriate legal advice and support where necessary.

Initiating Evaluations

10.2 Sponsors are advised to take the contractual issues identified in this chapter into account when selecting and placing work with CLEFs. Sponsors are encouraged to contact the Certification Body for assistance prior to issuing tenders or awarding contracts.

10.3 Sponsors are free to choose different CLEFs for different evaluations or re-evaluations. The UKAS requirements stipulated by the Scheme ensure that each CLEF records their work in sufficient detail to enable evaluations to be reproducible.

Deliverables

10.4 Where a TOE is being re-evaluated or where an evaluated TOE is a component of the new TOE, the evaluators will require access to previous evaluation results. The sponsor is responsible for arranging this access. Where necessary, commercial confidentiality agreements can be agreed between the CLEF and the organisations developing the TOE, and/or its component parts.

10.5 The evaluators will require access to the development site, including access to the development tools, and facilities for interviewing (some of) the development staff when they check the development environment.

10.6 The evaluators will also require access to the TOE in its operational environment during their penetration testing activities. The sponsor is responsible for ensuring that this can occur, as necessary.

10.7 The provision of intangible deliverables such as technical and logistical support from the sponsor and/or developer(s) to the evaluators will often be necessary for the successful conduct of an evaluation.

10.8 Some design information may be confidential to the developer and, as such, may not be made available to the sponsor, whose responsibility it is to ensure the supply of deliverables. Before progressing towards evaluation, the sponsor should ensure that he understands and accepts his obligations under the Scheme and, in particular, that he shall ensure the timely supply of the deliverables for the evaluation. The sponsor must therefore make contractual arrangements with the developer, where they do not both belong to the same organisation, to ensure the supply of evaluation deliverables.

10.9 Producers of deliverables should be aware that meeting the supply dates identified in the agreed Deliverables List is essential if the CLEF is to perform the evaluation to the agreed schedule.

Access

10.10 On occasions, the developer may wish to limit the sponsor's access to proprietary information used in the production of the TOE. It is the responsibility of the sponsor to obtain the written consent of the developer to allow the CLEF and Certification Body access to any proprietary information and to relinquish his own rights to any results of the evaluation that would compromise such information.

10.11 Where necessary, arrangements should be made for access by the evaluators to any subcontractors or external consultants employed on the development.

10.12 Evaluation work, particularly during concurrent evaluations, may require technical support from the developer. The provision of this support is a contractual issue between the sponsor and developer. The level of support should be adequate for the target assurance level. The format of the support can include informal discussions, formal meetings, and informal correspondence.

10.13 Confidentiality agreements between sponsors, developers and subcontractors to limit access to proprietary information should not be so restrictive as to cause problems among the parties, should the evaluation process identify areas that require corrective action.

Release of Information

10.14 Sponsors may wish to include provision for future access and supply of deliverables in their contracts with developers in order to facilitate future re-evaluations.

10.15 The Evaluation Work Programme and Deliverables List usually remain the property of the CLEF which performed the evaluation.

10.16 The ownership and copyright of Evaluation Technical Reports (ETRs) must be agreed between the sponsor and the CLEF during the pre-contract negotiations, but usually remains with the sponsor. Where a CLEF claims intellectual property rights over methods and techniques developed at its own expense, the CLEF may produce a separate document (as property, copyright and title of the CLEF) including the evaluation outputs specific to these methods and tools.

10.17 Where a TOE forms part of another evaluation, the ETR must not be unreasonably withheld from the CLEF performing the new evaluation.

10.18 It should be noted that the Certification Body will use evaluation results in the production of the Certification Report, which will be Crown copyright.

Penetration Testing

10.19 The CLEF may require the owner of the system used for penetration tests to sign a disclaimer to the effect that the evaluators will not be held liable if any damage occurs during the tests. The damage covers aspects such as data, programs, source files and configuration parameters.

10.20 In general, the implementation of an adequate backup strategy will enable suitable recovery measures to be taken.

Resolution of Problems

10.21 During the course of an evaluation, the evaluation team may discover various problems relating to the TOE and the supplied deliverables. As soon as a problem has been confirmed to exist, it will be reported to the sponsor of the evaluation, using a special Scheme form. Problems and their status will be discussed during Evaluation Progress Meetings. It is important that any problem receives prompt action from the sponsor in order to ensure a successful evaluation result. The sponsor should ensure that there is adequate contractual cover for the resolution of problems and the re-evaluation of the updated documentation.

10.22 It is often the case that problems are discovered during penetration testing, i.e. towards the end of the evaluation. This may involve a considerable amount of rework requiring re-evaluation effort at the end of the main body of evaluation activity. It is important to be clear whether the initial evaluation contract with the CLEF covers this rework, or whether a contract extension will need to be negotiated to handle major changes.

Insurance

10.23 Sponsors and developers should consider whether insurance is necessary for any deliverables including TOEs made available, or provided, to the CLEF for training or penetration testing. Note that some deliverables, such as new or special purpose types of hardware, may not have an easily identified replacement cost and may well present insurance risks that cannot be transferred to evaluators.

Assurance Level

10.24 Neither the CLEF nor the Certification Body can guarantee that a TOE will achieve a specific assurance level. Impartiality is an important part of the third-party evaluation and certification process and maintains the value of the Scheme.

Award of Certificate

10.25 CLEFs are prohibited from entering into any arrangements which rely upon the award of a Certificate resulting from an evaluation by that CLEF.

10.26 The Certification Body does not guarantee the duration of the certification process, although a period of up to eight weeks from receipt of the Evaluation Technical Report from the CLEF is the aim. Where possible, the Certification Body will attempt to meet certification deadlines imposed on the sponsor.

CLEF & Evaluator Impartiality

10.27 Under the rules of the Scheme, the TOE evaluators cannot provide detailed advice to sponsors or developers about design changes required to correct identified weaknesses or problems with that TOE.

10.28 However, a sponsor or developer may commission the CLEF to produce a Development Methods Review (DMR) to provide feedback to assist in performing future developments which will be subject to evaluation. A DMR can be negotiated at any stage during an evaluation and can be performed under a separate contractual agreement with the CLEF. If the DMR is produced at the request of the sponsor, then commercially sensitive information belonging to the developer will be sanitised before its release. This feedback is available informally during progress meetings.

Concurrent & Consecutive Evaluations

10.29 The main contractual issues for a concurrent evaluation are:

a) the need for access and commercial confidentiality agreements to be agreed between the sponsor, developers and CLEF to prevent delays

b) agreement between the sponsor, developers and CLEF regarding the schedule for supply of deliverables, including any penalty clauses.

10.30 As consecutive evaluations are retrospective, sponsors need to ensure that any necessary access to development staff, development site, development tools and support is made available to the evaluation team.

10.31 Regardless of the type of evaluation, the sponsor must arrange access to the operational site for penetration test purposes.

Confidentiality

10.32 During their work, CLEFs will be given access to their clients' commercially sensitive information, and may gain access to nationally sensitive information. While general requirements for confidentiality are a matter for the Scheme, sponsors, developers and CLEFs may agree additional requirements as long as these are consistent with the Scheme and, if applicable, national protective measures.

10.33 If part of the TOE's source code is commercially confidential, the owners of the code may wish to enter into a confidentiality agreement with the CLEF and supply the code directly to the CLEF, rather than through the sponsor or developer (if the owners are subcontracted to the developer).

10.34 At the conclusion of an evaluation, sponsors and developers should advise the CLEF as to which deliverables may be destroyed and which should be returned to the issuer. UKAS rules require the CLEF to archive its internal evaluation material for a period of at least six years. The sponsor should be aware of the requirement to retain TOE deliverables in case of future re-

evaluation needs.

Marketing & Selling Certified Products

10.35 Attention is drawn to the conditions outlined in sections Roles and Responsibilities of Developers, Selling of Certified Products and Publications and Publicity in Chapter 0.

Integrating Certified TOEs

10.36 When a TOE contains a certified TOE, sponsors and developers must ensure they have access to the following items for the certified TOE:

a) the Certificate and Certification Report

b) the security target.

10.37 Copies of the above items should also be issued to the CLEF evaluating the new TOE. The sponsor must also ensure that arrangements are made for the certified TOE's ETR to be delivered to the CLEF evaluating the TOE.

Appeals Procedure

10.38 Disputes concerning the operation of the Scheme may be referred to the Certification Body by any party involved in an evaluation, i.e. sponsor, developer or CLEF. If this course of action is considered to be ineffective, or if the Certification Body itself is involved in the dispute, the party may appeal to the Management Board for resolution.

Annex AGlossary

A.1 This section provides a glossary for all parts of the Developer's Guide.

Abstraction:

The process of exclusion of unnecessary detail from a specification (or model), to avoid the specification being oriented towards a particular solution or implementation.

Accreditation:

There are two definitions according to circumstances as follows:

a) the procedure for accepting an IT system for use within a particular environment (system accreditation)

b) the procedure for recognising both technical competence and the impartiality of a test laboratory to carry out its associated tasks (laboratory accreditation).

Animation:

This is defined as the translation of a specification or design definition into a form which can be executed, in order to gain early insight into the behaviour of the product or system which is to be developed from the specification or design. This can be achieved by building a prototype or using a software tool such as an executable specification language.

Availability:

The prevention of the unauthorised withholding of information or resources.

Basic Component:

A component that is identifiable at the lowest hierarchical level of specification produced during Detailed Design.

Certificate / Certification Report:

The public document issued by the Certification Body as a formal statement confirming the results of the evaluation and that the evaluation criteria, methods and procedures were correctly applied; the document includes appropriate details about the evaluation based on the ETR.

Certification:

The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were correctly applied.

Certification Body:

An independent and impartial national organisation that performs certification.

CLEF:

A Commercial Licensed Evaluation Facility (CLEF) is an organisation accredited in accordance with some agreed rules and licensed by the Certification Body to perform security evaluations.

Component:

An identifiable and self-contained portion of a Target of Evaluation.

Confidentiality:

The prevention of the unauthorised disclosure of information.

Correctness:

A property of a representation of a Target of Evaluation such that it accurately reflects the stated security target for that system or product.

Countermeasure:

A technical or non-technical security measure which contributes to meeting the security objective(s) of a Target of Evaluation.

Critical Mechanism:

A security enforcing mechanism within a Target of Evaluation whose failure through direct attack would create a vulnerability.

Covert Channel:

A covert channel is the use of a mechanism not intended for communication to transfer information in a way which violates security. [ITSEC 6.21]

Data Hiding:

The technique of encapsulating software design decisions in modules in such a way that the module's interfaces reveal as little as possible about the module's inner workings; thus, each module is a 'black box' to the other modules in the TOE. The discipline of data hiding forbids the use of information about a module that is not in the module's interface specification.

Deliverable:

An item or resource produced or used during development of a TOE that is required to be made available to the evaluators for the purpose of evaluation.

Deliverables List:

A document produced by a CLEF containing the definition of the documents comprising the security target, all representations of the TOE and developer support required to meet the work specified in the EWP. The Deliverables List may be included as part of the EWP.

Developer:

The organisation that manufactures a Target of Evaluation.

Effectiveness:

A property of a Target of Evaluation representing how well it provides security in the context of its actual or proposed operational use.

EOR:

An acronym for Evaluation Observation Report.

Evaluation:

The assessment of an IT system or product against defined evaluation criteria.

Evaluation Observation Report:

Evaluation Observation Reports are used to report all security related problems relating to a TOE other than exploitable vulnerabilities.

Evaluation Technical Report (ETR):

A report produced by a CLEF and submitted to the Certification Body detailing the findings of an evaluation and forming the basis of the certification of a TOE. There may be more than one ETR per TOE (one per evaluation job), but the final ETR will summarise the findings of the whole evaluation.

Evaluation Work Programme (EWP):

A document produced by a CLEF and submitted to the Certification Body detailing a description of how the work required for evaluation is organised; i.e. it is a description of the work packages involved in the evaluation and the relationships between them.

Functional Unit:

Functional units are procedures or functions in the source code.

Impartiality:

Freedom from bias towards achieving any particular result.

Integrity:

The prevention of the unauthorised modification of information.

Layering:

The process of designing a TOE in increasingly less abstract levels.

Mechanism:

See Security Mechanism.

Objectivity:

The property of a test whereby the result is obtained with the minimum of subjective judgement or opinion.

Product:

A package of IT software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Product Rationale:

A description of the security capabilities of a product, giving the necessary information for a prospective purchaser to decide whether it will help to satisfy his system security objectives.

Repeatability:

The repeated evaluation of the same Target of Evaluation to the same security target by the same CLEF yields the same overall verdict as the first evaluation (e.g. E1 or E5).

Reproducibility:

The evaluation of the same Target of Evaluation to the same security target by a different CLEF yields the same overall verdict as the first CLEF (e.g. E1 or E5).

Security:

The combination of confidentiality, integrity and availability.

Security Enforcing:

That which contributes directly to satisfying the security objectives of the Target of Evaluation.

Security Fault Notification:

A Security Fault Notification is used to report any failure of a TOE to comply with its security requirements (including its security objectives) defined in the security target, but only when there is a risk of a security violation (i.e. there is an exploitable vulnerability).

Security Irrelevant:

That which is neither security enforcing nor security relevant, and in no way contributes to either the enforcement or interference of security in a Target of Evaluation.

Security Mechanism:

The logic or algorithm that implements a particular security enforcing or security relevant function in hardware or software. Note that some security mechanisms may not be critical.

Security Objective:

The contribution to security which a Target of Evaluation is intended to achieve.

Security Relevant:

That which is not security enforcing, but must function correctly for Target of Evaluation to enforce security.

Security Target:

A specification of the security required of a Target of Evaluation (TOE), used as a baseline for evaluation. The security target will specify the security enforcing functions of the TOE. It will also specify the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Security Threat:

An action or event that might prejudice security.

Separation of Functionality:

This refers to the separation of security enforcing, security relevant and security irrelevant functions that comprise a TOE.

SFN:

An acronym for Security Fault Notification.

Sponsor:

The person or organisation that requests an evaluation.

Supporting Protection Mechanism:

The hardware or firmware necessary to enable a SEF to be correctly implemented or operated in the operational environment.

System:

A specific IT installation, with a particular purpose and operational environment.

System Security Policy:

The set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specified system.

Target Assurance Level:

There are seven assurance (or evaluation) levels defined in the ITSEC ranging from level E0 to level E6, where level E0 represents inadequate or no assurance and E6 the highest assurance. The target assurance level of a TOE is the set of (confidence) criteria identified in the security target against which the TOE is to be evaluated. The ratings/levels E1, E2, E3, E4, E5 and E6 are defined in the ITSEC [Reference 0], Chapter 4, paragraphs 4.5 to 4.10.

Target Evaluation Level:

See Target Assurance Level.

Target of Evaluation (TOE):

An IT system or product which is subjected to security evaluation.

Threat:

See Security Threat.

Traceability:

The complete mapping of each security enforcing function from one level of representation to the next level of representation for the TOE. This mainly involves tracing the security enforcing functions and mechanisms through the various levels of design.

Vulnerability:

A weakness in the construction or operation of a TOE that would prevent the TOE from meeting one or more of its security objectives.

INDEX