UKSP 04

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UK Scheme Publication No 4

DEVELOPERS' GUIDE

Part II

REFERENCE FOR DEVELOPERS

Issue 1.0

July 1996

This document must not be copied or distributed further by the recipient without the prior written approval of the Senior Executive of the UK IT Security Evaluation and Certification Scheme.

Issued by:-

UK IT Security Evaluation & Certification Scheme

Certification Body

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 II of the Developers' Guide) provides a reference for sponsors and developers of the requirements of the ITSEC during each phase of the development life cycle for secure products and systems.

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

Correspondence in connection with 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

ABBREVIATIONS

BS	British Standards
CESG	Communications-Electronics Security Group
CLEF	Commercial Licensed Evaluation Facility
COTS	Commercial-Off-The-Shelf
EN	European Norm
HMG	Her Majesty’s Government
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
Scheme	UK IT Security Evaluation and Certification Scheme
SEF	Security Enforcing Function
SEISP	System Electronic Information Security Policy
SSADM	Structured Systems Analysis and Design Method
SSP	System Security Policy
TCSEC	Trusted Computer System Evaluation Criteria (known as the “Orange Book”)
TOE	Target of Evaluation
UK	United Kingdom
UKSP	UK Scheme Publication

Chapter 1 Introduction

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 for Developers.

1.3 Part I 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 (i.e. this document) 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's documents to readers, with suggested reading plans.

Objective of Part II

1.7 This Part of the Developers' Guide provides guidance on the ITSEC criteria to enable developers and sponsors of IT products and systems to prepare deliverables which will satisfy the criteria.

1.8 This guide does not replace or supersede the ITSEC requirements as specified by the ITSEC/ITSEM.

Scope

1.9 Guidance is provided for the correctness and effectiveness deliverable requirements at all assurance levels.

Layout of the Reference for Developers

1.10 This Part of the Developers' Guide is divided into two sections:

a) Section 1 covers the ITSEC correctness criteria

b) Section 2 covers the ITSEC effectiveness criteria.

1.11 The layout of the ITSEC has been reproduced to a large extent to provide readers with a simple means of locating guidance on any part of the ITSEC criteria, and to avoid lengthy cross referencing between documents.

Correctness Deliverables

1.12 The section on correctness deliverables is divided into separate chapters providing guidance on the criteria for each assurance level. To assist readers in finding the appropriate chapter, the outer top corner of each page contains a large symbol of the relevant assurance level for that page.

1.13 Each chapter begins with an overview of the deliverables which the sponsor and developer must produce for that assurance level. Each chapter then follows the layout used for assurance levels in the ITSEC, i.e. construction, operation, phases and aspects.

1.14 The ITSEC Requirements for Content and Presentation and Requirements for Evidence are replicated verbatim within text boxes, including the use of bold text to signify new or changed criteria from the previous level. The Evaluator Actions are not replicated as they are not relevant to developers or sponsors, although sponsors and developers should be aware that they may have to provide support for these activities.

1.15 New or changed statements within the criteria are repeated below the box and guidance provided where the requirements and implications of the criteria are not obvious.

Effectiveness Deliverables

1.16 The section on effectiveness deliverables covers all the deliverables in one chapter as the criteria are not substantially affected by assurance level. To assist readers in finding the section, the outer top corner of each page contains a large 'ED' symbol.

1.17 The chapter begins with an overview of the effectiveness deliverables which the sponsor and developer must produce irrespective of assurance level. Each chapter then follows the layout used for effectiveness in the ITSEC, i.e. construction, operation, phases and aspects.

1.18 The ITSEC Requirements for Content and Presentation and Requirements for Evidence are repeated verbatim within text boxes, including the use of bold text to signify new or changed criteria from the previous level. The Evaluator Actions are not repeated as they are not relevant to developers or sponsors.

1.19 New or changed statements within the criteria are repeated below the box and guidance provided where the requirements and implications of the criteria are not obvious.

How to use the Guidance

1.20 Note that the ITSEC [Reference 0], ITSEM [Reference 0] and this Guide are not a design guide for secure products or systems. It is up to the sponsor of an evaluation to determine the security objectives of the product or system and to choose security functions to satisfy them, and for the developer to design, implement and test those security functions. The criteria for a particular assurance level form a compulsory standard which must be met by the secure product or system before it can be awarded a certificate.

1.21 The correctness criteria and guidance will be found by looking in Section 1 for the chapter on the appropriate assurance level. To assist readers in finding the appropriate chapter, the outer top corner of each page contains a large symbol of the relevant assurance level for that page.

1.22 The correctness deliverables which the sponsor and developer must produce are listed at the start of each chapter. Each chapter then follows the layout used for correctness in the ITSEC, i.e. construction, operation, phases and aspects.

1.23 Find the text box containing the criteria for the particular correctness deliverable of interest. If the criteria statements are in normal text this signifies that the criteria at this assurance level are unchanged from the previous level. If the criteria statements are in bold text this signifies that the criteria are new or changed from the previous level.

1.24 Individual statements within the criteria are repeated below the box and guidance provided where the requirements and implications require explanation. Guidance will generally be provided for the new or changed criteria. However, reference should be made to the previous levels for guidance which may apply to a range of assurance levels.

1.25 Where the only change to a criteria statement is the degree of specification rigour (i.e. state, describe, explain), a reference will be provided to generic guidance in Part III of the Guide.

1.26 The effectiveness deliverables which the sponsor and developer must produce are listed at the start of the chapter in Section 2. The chapter then follows the layout used for effectiveness in the ITSEC, i.e. by aspects.

1.27 Find the text box containing the criteria for the particular effectiveness deliverable of interest. Statements within the criteria are repeated below the box and guidance provided where the requirements and implications require explanation.

Acknowledgements

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

A Request for Feedback

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

1.30 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.

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

Chapter 2 Evaluation Deliverables

Introduction

2.1 A successful ITSEC evaluation of a product or system relies upon the sponsor and developer preparing information about the product or system which meet the ITSEC requirements for:

a) content and presentation

b) evidence.

2.2 The requirements for content and presentation identify the constituent parts, procedures and standards, and structuring of the deliverables. The requirements for evidence define the proof which must be supplied in order to demonstrate how the criteria in question have been met for the TOE.

2.3 The ITSEC addresses the assurance which may be placed in the security enforcing functionality of the Target of Evaluation (TOE) from two different points of view. It distinguishes assurance in the *correctness* in the implementation of the security enforcing functions and mechanisms from assurance in their *effectiveness*.

2.4 The ITSEC [Reference 0] states that:

Evaluation of effectiveness assesses whether the security enforcing functions and mechanisms that are provided in the TOE will actually satisfy the stated security objectives. (Paragraph 1.14)

Evaluation of correctness assesses whether the security enforcing functions and mechanisms are implemented correctly. (Paragraph 1.16)

2.5 The term 'deliverable' is used to refer to any item (including the TOE itself) that is required to be made available to the evaluation team for evaluation purposes. The purpose of deliverables is to allow evaluators to understand and assess the TOE.

2.6 The ITSEM [Reference 0], paragraph 4.3.5 advises that different types of deliverables satisfy this purpose in different ways, e.g.:

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

b) deliverables may enable the evaluation team to establish additional evidence of effectiveness or correctness, e.g. access to the developed TOE

c) deliverables may improve the overall efficiency of the evaluation team's work, for example through technical support from the developer, and may enable costs to be reduced.

2.7 The general requirements for correctness and effectiveness deliverables are given in Figures 1 and 3 of Annex 0. However, some additional deliverable requirements are implied; in particular, the following deliverables, associated with the development environment in general, are usually required:

a) access to any previous evaluation results (e.g. for re-evaluation of a TOE or where a certified product is a component of the current TOE)

b) access to the development site(s), including development tools and the configuration control system, and facilities for interviewing (some of) the development staff

c) details of development procedures and standards, including security operating procedures

d) access to the TOE in its operational environment (for systems), and details of any security operating procedures for that environment

e) technical and logistical support from the developer.

Correctness Documentation

2.8 The correctness documentation covers a number of the ITSEC requirements as follows:

a) The Development Process consists of four phases:

- Requirements
- Architectural Design
- Detailed Design
- Implementation (which includes Testing and, at E3 and above, Source Code)

b) The Development Environment consists of three aspects:

- Configuration Control
- Programming Languages and Compilers
- Developer's Security

c) The Operational Documentation consists of two aspects:

- User Documentation
- Administration Documentation

d) The Operational Environment consists of two aspects:

- Delivery and Configuration
- Startup and Operation

2.9 The correctness documentation required for a TOE is dependent upon the target assurance level. Seven assurance levels denoted E0 to E6 are defined in the ITSEC. E0 represents no assurance. E1 represents an entry point and E6 represents the highest level of assurance.

2.10 The requirements for the correctness deliverables at each assurance level are detailed in Section 1.

Effectiveness Documentation

2.11 The effectiveness documentation covers a number of the ITSEC requirements as follows:

a) Construction

- Suitability analysis
- Binding analysis
- Strength of mechanisms analysis
- List of known vulnerabilities in construction

b) Operation

- Ease of use analysis
- List of known vulnerabilities in operational use.

2.12 The effectiveness criteria do not change by assurance level. However, some of the correctness documentation is used as input for the preparation of the effectiveness documentation. As the assurance level affects the degree of rigour of the correctness documentation, the effectiveness documentation is influenced by the assurance level. Indeed, although the effectiveness criteria do not change, the degree of rigour required does increase with the assurance level.

2.13 The requirements for the effectiveness deliverables for all assurance levels are detailed in Section 2.

Use of Products as Components of a TOE

2.14 One of a number of alternatives may be adopted for supplying deliverables related to a product which forms a security enforcing or security relevant component. Examples include:

a) the results of any previous evaluation of the product may be supplied

b) the product may be treated in the same way as the rest of the TOE, in which case the appropriate deliverables relating to the product should be supplied.

2.15 The approach adopted for a particular evaluation must be acceptable to the Certification Body, sponsor and evaluation team. If existing evaluation results are to be reused, additional guidance is provided in the Re-evaluation Chapter of Part III of this guide.

Development Environment

2.16 The evaluators will require documentation relating to the configuration control, programming languages and compilers, and developer’s security used or applied during the development of the TOE. The evaluators will also require documentation relating more generally to the procedures, methods, tools and standards used during the development of the TOE, for example:

a) a quality plan, including development procedures

b) details of the development methods and tools used

c) software coding standards.

2.17 The evaluators will require evidence of adherence to procedures and standards, and evidence that methods and tools have been used correctly. Evidence may be provided by:

a) configuration management plan

b) configuration control records

c) minutes of design reviews.

2.18 At assurance levels above E1, the evaluators may also need to make one or more specific visits to examine the development environment and hold discussions with the developer. Topics to be discussed on such visits are identified in Figure 5 of Annex 0.

2.19 The evaluators have no right to access anything that is related solely to financial, contractual or staff issues (other than staff issues within the scope of the developer’s security criteria of the ITSEC). It is in the interests of developers and sponsors to ensure that these issues are not addressed in the deliverables which must be supplied to the evaluators.

Operational Environment

2.20 The evaluators will require documentation relating to the use, administration, delivery, configuration, startup, and operation of the TOE.

2.21 The evaluators will require access to the operational TOE in order to perform penetration testing. This requirement will only be waived in exceptional circumstances, and with the certifier’s approval. In such situations, penetration testing must still be carried out, and will require a representative TOE in a representative environment.

2.22 Where the TOE is a system, the evaluators will require access to the operational site(s) in order to:

a) discuss aspects of the operational procedures with representatives of the users

b) perform penetration testing in the operational environment.

2.23 Where the TOE is a product, the evaluators will require access to a working implementation of that product in order to perform penetration testing. The sponsor can make the TOE available at the development site, or the necessary equipment can be loaned to the evaluators and the penetration tests run at an alternative site where operational conditions can be adequately simulated.

Evaluation Support

2.24 Whether the evaluation is concurrent or consecutive, the sponsor and developer should be aware that evaluation is, by nature, to a certain extent iterative. It is common, and should be expected, that documentation will need to be updated as a result of evaluator findings. The sponsor and developer must make available a technical support contact with the necessary skills and ability to answer the evaluators' queries, as well as with the necessary authority to ensure that the required changes are performed.

2.25 The evaluators may require logistical, consultancy and training support from the sponsor during an evaluation. When the sponsor and the developer are from separate organisations, the sponsor may make arrangements for the developer to supply some or all of this support.

2.26 A named individual in the developer's organisation should act as the point of contact for all developer support. This individual, or nominated alternatives, should be able to:

a) provide support in a timely manner

b) liaise with other development staff, as necessary, where detailed information is required on particular aspects of the TOE.

2.27 The total amount of support required will be evaluation dependant. Factors affecting the amount of support will include the target assurance level, the size and complexity of the system, and whether the developer and/or sponsor has previous experience in the development of evaluated systems and products. Some aspects of the evaluation process will demand more intensive support, such as performing tests on the TOE.

2.28 The type of support required could include:

a) training

b) informal discussions

c) computer access and support

d) office accommodation.

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

a) the hardware and software used in the TOE and its development

b) development methods used

c) development tools used.

2.30 The developer is not normally required to organise formal training courses specifically for the evaluators or certifiers. However, the evaluators 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 secure administration of the TOE.

2.31 Although not compulsory, experience of past evaluations has shown that the provision of training to the evaluators by the developer is highly beneficial for both parties, as the evaluators gain increased understanding of the TOE and its development process, and the developer is able to preempt many issues which would otherwise lead to questions from the evaluators.

2.32 Informal discussions with the sponsor or developer may also be required on any aspect of the TOE. Typically the evaluators may require the sponsor or developer to provide a short description of a particular part of the TOE and then to answer any questions that may arise. However, the rules of the Scheme require the evaluators to retain written evidence of any such discussions.

2.33 The evaluators will require access to one or more suitable computers, principally in order to perform tests on the TOE. 'Computers' in this context include any equipment used by the developer to build the TOE and to test the TOE. Where the TOE is a system, the evaluators will also require, where possible, access to the computer(s) used in the TOE's operation (see paragraphs 0 to 0).

2.34 The evaluators will require dedicated computer access for some of the time when performing tests in addition to those performed by the developer, or when performing penetration testing. The duration of computer access will depend on the nature of a particular TOE. Access to a computer will normally be at the development or operational site. In some cases, however, it may be convenient to provide access in an alternative location, for example, by the supply of a computer to the CLEF.

2.35 When the evaluators are using a computer, support may be required to provide help with basic operations, such as starting up the computer, making backup copies of the TOE and running tests.

2.36 Office accommodation for the evaluators' sole use should be obtained as required for when the evaluators are working at the development or operational site. This accommodation should be capable of supporting the required number of people and may include:

a) basic furniture, including a telephone and access to a photocopier

b) appropriate secure storage facilities for protectively marked information associated with the TOE.

2.37 It is recognised that site rules may prohibit general unescorted access on the development or operational site. However, the evaluators will require privacy during certain periods when working at site, and so arrangements will need to be made to allow the evaluators to be unescorted at agreed locations, e.g. in an office allocated specifically to the evaluators. The evaluators will also require privacy to perform their tests; any escort should therefore be out of range.

Section 1 - Correctness Documentation

Chapter 3 Level E1

Overview of E1 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE

Architecture:

- Informal description of the architecture of the TOE

Detailed Design:

- [no deliverables required, although some may be necessary if a high strength of mechanism is claimed]

Implementation:

- [no deliverables required; however, the following two deliverables may be optionally supplied to reduce the amount of evaluation work performed]
- Test documentation
- Library of test programs and tools used for testing the TOE

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation

Programming Languages and Compilers:

- [no deliverables required]

Developer's Security:

- [no deliverables required]

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall state the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. The security enforcing functions within the security target shall be specified using an informal style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E1.2

The security target shall state the security enforcing functions to be provided by the TOE.

3.1 At least one Security Enforcing Function (SEF) must be identified for a TOE.

3.2 The SEFs must be clearly identified within the security target. It is advisable to uniquely label each SEF to assist with traceability to threats and any security objectives, and through the architecture.

3.3 It is recommended that SEFs be grouped together under the generic headings suggested in Chapter 2 of the ITSEC [Reference 0], namely:

a) Identification and Authentication

b) Access Control

c) Accountability

d) Audit

e) Object Reuse

f) Accuracy

g) Reliability of Service

h) Data Exchange.

3.4 Specific details of SEF specifications should be contained within a single document (usually the TOE's security target), and should not be referenced to other documents. This is particularly important where certified TOEs are being reused. Care must be taken to ensure the uniqueness of identification of the SEFs.

3.5 If a sponsor wishes to claim a predefined functionality class, e.g. such as those in Annex A of the ITSEC, the claim should be stated under the specifications of the SEFs in the following format:

The TOE shall implement all the security enforcing functions of functionality class F-nn as specified in Reference x.

where *nn* is the functionality class descriptor

and *x* is the reference source for the predefined functionality class.

3.6 A TOE may claim more than one predefined functionality class. A TOE may also have such additional SEFs as the sponsor wishes - subject to maintaining consistency with the claimed functionality class(es) and linking to one or more threats - these SEFs should be grouped under the usual SEF headings of I&A, Access Control, etc.

3.7 A functionality class must be referenced as a whole, and the TOE must claim to meet the class wholly by its own functionality. For example, databases are not awarded functionality classes in their own right, as they usually rely on the underlying operating system for some security functionality.

3.8 It is recommended that the security target simply include a reference to the appropriate functionality class, rather than attempting to include the verbatim particulars. However, if there is a particular need to append information to elements of the class (e.g. for traceability purposes), the reason for the inclusion should be stated in the security target, and the functionality class SEFs should be separately identified from any other SEFs.

3.9 The higher assurance levels require a greater depth of rigour and formality in the specification of SEFs than that provided by the functionality classes. Therefore, notwithstanding the above recommendations, full details of the SEFs must be provided in the security target for the higher assurance levels. In this case, there must be a clear correspondence between the original functionality class statements and the more formal/rigorous claims of the security target.

3.10 Note that in the ITSEC:

a) the predefined classes are examples and may lead to problems establishing traceability

b) classes F-C1, F-C2, F-B1, F-B2 and F-B3 do not guarantee that a TOE will comply with the TCSEC classes.

3.11 Each SEF must:

a) be a high-level specification of that functionality in the TOE which contributes directly to maintaining the security objectives and countering the threats

b) be able to be tested against measurable criteria demonstrating all characteristics of the proposed security enforcing functionality

c) be unambiguous

d) be precise (i.e. all technical terms defined)

e) be internally consistent

f) be externally consistent (i.e. with the other SEFs, assertions and required security mechanisms).

3.12 Where possible, SEF specifications should be kept short to assist with their comprehension and to minimise ambiguity and inconsistency. SEFs should not be split unnecessarily, but should not be so complex as to prevent meaningful traceability.

In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system.

3.13 The SSP can be either a separate document or incorporated with the security target. It is usually the case, however, that two separate documents are supplied.

3.14 It is advisable to uniquely identify the security objectives and threats to assist with their correlation to the SEFs. Grouping the security objectives and threats within the document can aid clarity.

3.15 For large systems, particularly those used by Government, the technical security requirements for the system may be contained in a lower level document, the System Electronic Information Security Policy (SEISP). In this case, the SEFs should be included in the SEISP. A properly constructed SSP and SEISP, taken together, should be capable of meeting the requirements for a security target. It is the responsibility of the sponsor to ensure consistency between the security target and the security policy documents, although this will be checked by the CLEF.

3.16 It is recommended that individual security objectives are uniquely identified to facilitate traceability to the threats and SEFs, and that individual threats are uniquely identified to facilitate traceability to the security objectives and countermeasures (i.e. SEFs and stated environment).

3.17 Security objectives should identify:

a) the assets that are to be protected in the actual environment

b) the way in which the assets are to be protected, such that the objectives can be related back to the fundamental security aspects of confidentiality, integrity and availability.

3.18 There should be at least one threat for each security objective. At least one security objective and one threat must be identified for a system.

3.19 If a SEF relies upon properties of the TOE's operational environment in order for it to function correctly, an assertion of the necessary properties of the TOE's operational environment must be claimed in the policy section of the security target/SSP.

3.20 The physical, procedural and personnel measures must be consistent with the operational environment.

In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment.

3.21 The product rationale can be either a separate document or incorporated with the security target. It is advisable to uniquely identify the assumed threats to assist with the correlation of threats to SEFs, and to group them within the document.

3.22 At least one threat must be identified for a product.

3.23 If a SEF relies upon properties of the TOE's assumed environment in order for it to function correctly, an assertion of the necessary properties of the TOE's assumed environment must be claimed in the rationale section of the security target.

3.24 Although the ITSEC does not explicitly require a product rationale to include security objectives, it is strongly recommended that product security targets include security objectives. These can be included as part of the Intended Method of Use.

3.25 Security objectives should identify:

a) the assets that are to be protected in the intended environment

b) the way in which the assets are to be protected, such that the objectives can be related back to the fundamental security aspects of confidentiality, integrity and availability.

3.26 It is recommended that individual security objectives are uniquely identified to facilitate traceability to the threats and SEFs, and that individual threats are uniquely identified to facilitate traceability to the security objectives and countermeasures (i.e. SEFs and environmental assumptions).

3.27 The intended environment and method of use of a product must be consistent with the assumed threats. Note that it is not important whether the threats are related to the security objectives or vice versa, so long as one is a refinement of the other and provides greater detail.

3.28 The physical, procedural and personnel measures must be consistent with the intended operational environment. If the measures are expected to be produced and provided by purchasers and users of the product, then assertions must be provided within the security target specifying constraints with which the measures must comply.

The security enforcing functions within the security target shall be specified using an informal style as categorised in Chapter 2 (of the ITSEC [Reference 0]).

3.29 Part III of this Guide provides guidance on informal specifications. While informally specified SEFs are written in natural language, which is defined as a notation not requiring special restrictions or conventions, it is important to ensure that SEFs are specified and are therefore clear, consistent and unambiguous.

3.30 It can be helpful for any potentially ambiguous terms to be defined in a glossary within the security target, particularly if different languages are used for parts of the security target. Special care should be taken to clarify the use of definitions and punctuation between British and American English.

Requirements for Evidence

: case of a system the security target shall state how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall state how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. ITSEC E1.3

In the case of a system the security target shall state how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats.

3.31 The means by which the correlation is demonstrated between the proposed functionality (i.e. SEFs), the security objectives, and the identified threats, is not prescribed by the ITSEC. However, the evidence provided in the security target must be sufficient to clearly indicate the correlation.

3.32 Each SEF must be linked to at least one security objective and to one identified threat. Each security objective must be linked to at least one SEF. Each identified threat must be linked to at least one SEF.

3.33 It should be noted that this requirement overlaps with the effectiveness requirements for a suitability analysis, and could be addressed by including the suitability analysis within the security target (either as a reference to a separate document, or as a separate section within the security target itself).

In the case of a product the security target shall state how the functionality is appropriate for that method of use and is adequate to counter the assumed threats.

3.34 The means by which the correlation is demonstrated between the proposed functionality (i.e. SEFs), the method of use, and the assumed threats, is not prescribed by the ITSEC. However, the evidence provided in the security target must be sufficient to clearly indicate the correlation. Suitable correlation methods include textual cross-references and matrices.

3.35 Each SEF must contribute towards satisfying at least one security objective, countering at least one identified threat. Each security objective and each assumed threat must be linked to at least one SEF.

Security Target Requirements

equired contents of a security target can be summarised as follows:

a) Either a System Security Policy
or a Product Rationale
b) A specification of the required security enforcing functions
c) A definition of required security mechanisms (optional)
d) The claimed rating of the minimum strength of mechanisms
e) The target evaluation level. ITSEC 2.4

A security target may optionally prescribe or claim the use of particular security mechanisms. All security mechanisms included in a security target shall be correlated to its security enforcing functions, so that it can be seen which mechanisms implement each function (a mechanism may implement several functions, and a function may be implemented through the combination of several mechanisms). *ITSEC 2.23*

3.36 A security mechanism is the logic or algorithm which implements at least part of a SEF. Within the security target, security mechanisms may be prescribed which stipulate the means by which certain SEFs are to be implemented. In effect, security mechanisms constrain the developer to realise the design using specified techniques.

3.37 Security mechanisms need not be specified within the security target for every, or any, SEF. Their inclusion is a matter for sponsors. However, where they are specified, they must be correlated to the SEFs which they provide.

Every security target shall specify a claimed rating of the minimum strength of security mechanisms of the TOE against direct attack. This shall be one of the ratings basic, medium or high as defined in Chapter 3 (of the ITSEC [Reference 0]). *ITSEC 2.25*

3.38 The security target must include a claimed rating for the minimum strength of the security mechanisms acting in concert, i.e. the claimed strength cannot exceed the strength of individual mechanisms and must be consistent with their combined effect.

3.39 The strength rating provides an indication of the resistance of the TOE to direct attack, as described in the identified threats, and must be commensurate with the target level of assurance.

Every security target shall specify a target evaluation level for evaluation of the TOE. This shall be one of the ratings E1, E2, E3, E4, E5 or E6 as defined in Chapter 4 (of the ITSEC [Reference 0]). *ITSEC 2.26*

3.40 The security target must provide a simple statement of the target level of assurance.

Phase 2 - Architectural Design

Requirements for Content and Presentation

lescription of the architecture shall state the general structure of the TOE. It shall state the external interfaces of the TOE. It shall state any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. ITSEC E1.5

The description of the architecture shall state the general structure of the TOE.

3.41 Paragraph 4.20 of the ITSEC indicates the scope and level of detail necessary to comply with the Architectural Design requirements:

This phase of the development process covers the overall top level definition and design of the TOE. This takes the form of a descriptive high level specification, identifying the basic structure of the TOE, its external interfaces and its separation into major hardware and software components. The specification will distinguish between what the TOE will do (the top level description) and how it will do it (the top level design).

3.42 The architectural design may include diagrams which should be consistent with the textual descriptions.

3.43 The developer should provide relevant standards and procedures, stating the terms, notations and methods used in the design, to assist evaluators with their understanding of the documentation.

3.44 The architectural design for E1 must be informally stated.

Complexity

3.45 Minimal complexity is a property of good design. It also assists the application of effective technical assurance procedures. Paragraph 4.20 of the ITSEC states that:

A good design permits evaluation effort to be concentrated on limited areas of the TOE that contribute to security, and enables the implementation of the security target to be easily followed, as the design is refined into greater and greater detail.

3.46 The degree of complexity of the architectural design is an important consideration for TOE developers. The degree of complexity can affect:

a) the amount of evaluation effort

b) separation of functionality

c) binding of functionality

d) construction vulnerabilities.

It shall state the external interfaces of the TOE.

3.47 All the TOE's interfaces to the external environment identified in the security target must be stated. This includes, but is not limited to:

a) electrical, radio, laser or audio communications

b) removable media

c) visual displays

d) data entry devices (e.g. keyboards, switches, card swipe devices)

e) data entry and transfer protocols.

3.48 For a product intended to be integrated within other TOEs, the developer should consider stating the external interfaces in a form useful for other developers. For example, the information provided may include a specification of all functions that can be invoked from outside the TOE, the purpose of each function, its input parameters and their minimum and maximum and recommended values, its output parameters and possible results and any effects on other parts of the TOE.

It shall state any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware.

3.49 All hardware and firmware, within or external to the TOE, must be identified. A supporting protection mechanism is the hardware or firmware necessary to enable a SEF to be correctly implemented or operated in the operational environment. Where the hardware or firmware provides a supporting protection mechanism to the SEFs, the functionality of the mechanism must be stated in sufficient detail to enable the evaluation team to check that the supporting protection mechanism is appropriate for the SEFs.

Requirements for Evidence

lescription of the architecture shall state how the security enforcing functions of the security target will be provided. ITSEC E1.6

The description of the architecture shall state how the security enforcing functions of the security target will be provided.

3.50 Each SEF identified in the security target must be clearly correlated to, and fully satisfied by, the relevant area of the architectural design. Security enforcing components identified in the architectural design must be wholly correlated to SEFs, i.e. there must be no additional security enforcing functionality in the architectural design.

3.51 Some non security enforcing components may be identified whose failure or misuse could compromise security. These components are called security relevant, as their correct operation is relied upon for the TOE to enforce security. Usually these components are not identified until the detailed design, although it is feasible that they could be specified in the architectural design.

3.52 If an ITSEC certified product is used in a composite TOE, then no architectural design for the certified product is required to be supplied to the evaluators for correctness evaluation, although it may be required to support the effectiveness analyses. Further details on composite TOEs can be found in the Composite TOE Chapter of Part III of the Guide.

Phase 3 - Detailed Design

3.53 There are no detailed design requirements at this assurance level.

Phase 4 - Implementation

3.54 The implementation deliverables are not mandatory at this assurance level; however, the ITSEC identifies some optional requirements. The supply of test documentation to the evaluation team at this assurance level reduces the amount of evaluation work as the evaluation team can sample the developer's tests, thereby reducing costs.

3.55 The ITSEC does not prescribe any particular test strategy by developers.

3.56 When performing tests at E1, the developer should ensure that:

a) the results obtained from the tests are accurately recorded and checked against expected results

b) details of the version and configuration of the TOE are recorded.

3.57 Before the testing process starts, a sponsor should make arrangements with the TOE's developer to give the evaluation team an opportunity to witness the tests.

Requirements for Content and Presentation

locumentation may be provided that shall contain plan, purpose, procedures and results of the tests. A library of test programs may be provided that shall contain test programs and tools to enable tests covered by the test documentation to be repeated. ITSEC E1.11

Test documentation may be provided that shall contain plan, purpose, procedures and results of the tests.

3.58 This is optional at E1. Provision of this information will reduce the amount of evaluation work. Otherwise, the evaluator will perform tests to cover 100% of the security enforcing functionality.

3.59 Where the developer intends to devise tests at E1 for delivery to the evaluation team, a test strategy which provides full test coverage of all SEF functionality will be most beneficial for the evaluation team.

A library of test programs may be provided that shall contain test programs and tools to enable tests covered by the test documentation to be repeated.

3.60 This is optional at E1. Provision of this information will reduce the amount of evaluation work, as the evaluators will be able to repeat a sample of the developer's tests rather than performing a complete set of tests themselves.

Requirements for Evidence

documentation may be provided that shall state the correspondence between tests and the security enforcing functions defined in the security target. ITSEC E1.12

Test documentation may be provided that shall state the correspondence between tests and the security enforcing functions defined in the security target.

3.61 This is optional at E1. Provision of this information will reduce the amount of evaluation work.

3.62 A suitable means of providing this evidence is by constructing a simple table relating SEFs to tests. Note that for this evidence to be acceptable, all SEFs must be tested.

Construction - The Development Environment

Aspect 1 - Configuration Control

3.63 It is an ITSEC requirement that TOEs are uniquely identified. This is to enable:

a) the evaluation team to ensure that the TOE deliverables match the TOE used for penetration testing

b) purchasers and users to check that the TOE matches its ITSEC certificate.

Requirements for Content and Presentation

onfiguration list shall state where the TOE is uniquely identified (version number). ITSEC E1.15

The configuration list shall state where the TOE is uniquely identified (version number).

3.64 The unique identification applies to the version of the TOE submitted for evaluation. Exact copies of the TOE (e.g. copies of a mass-produced product) do not have to be individually identified.

3.65 Although the ITSEC requirement refers to a 'configuration list', at E1 only identification of the overall consolidated TOE needs to be specified.

3.66 The list must indicate where the unique identification is situated, e.g. on an identification plate for hardware, or as a startup screen or checksum for software.

3.67 The configuration list should be provided as early as possible to the evaluation team. If the TOE is subsequently modified during the evaluation, updated details should be issued by the developer.

Requirements for Evidence

onfiguration list shall state how the TOE is uniquely identified. ITSEC E1.16

The configuration list shall state how the TOE is uniquely identified.

3.68 This requirement requires the developer to state how the unique identification is constituted, e.g. the format of the identification scheme.

Aspect 2 - Programming Languages and Compilers

3.69 There are no programming languages and compilers requirements at this assurance level.

Aspect 3 - Developer's Security

3.70 There are no developer's security requirements at this assurance level.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

user documentation shall state the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E1.15

The user documentation shall state the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation.

The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level.

3.71 Note that, dependent on the target audience for the user guide, the developer may provide more detail than required by the ITSEC; for example, at E1 the developer may wish to explain various user aspects for inexperienced users as a condition of a development contract.

3.72 The following guidance should be used when preparing the user documentation:

a) ensure that the SEFs relevant to the end-user are detailed adequately (i.e. stated at E1)

b) ensure that the guidelines provided for the secure use of security enforcing functionality relevant to the end-user are adequate

c) ensure that the documentation is structured and internally consistent

d) ensure that the user documentation is consistent with all the other documentation provided to the evaluation team.

3.73 The user manuals should indicate how the TOE can be used securely, and should not draw unnecessary attention to any potential security weaknesses.

Requirements for Evidence

ıser documentation shall state how an end-user uses the TOE in a secure manner. ITSEC E1.26.

The user documentation shall state how an end-user uses the TOE in a secure manner.

3.74 At E1 and E2, the user guides might state that, for example:

a) The chmod command is used to change the access permissions on a file

b) The syntax of the chmod command is

chmod (*filename, permission-list*) [/+*echo* | /-*echo*]

where:

filename is the name of the file for which the access permissions are to be changed
permission-list is the string describing the new access permissions in the following format (...)
echo is an optional parameter; +echo displays the result of the chmod command, -echo suppresses the display of the result of the chmod command.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

dministration documentation shall state the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall state all security parameters which are under his control. It shall state each type of security-relevant event, relevant to the administrative functions. It shall state details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall state instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E1.28

3.75 Note that in ITSEC terms:

a) an administrator role covers roles such as operators, system administrators, security auditors and information security officers

b) if the TOE can be configured to enable the security features of the TOE to be configured in different ways, the specific configuration parameters are termed 'security parameters'.

The administration documentation shall state the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information.

3.76 The SEFs relevant to an administrator (i.e. those which an administrator can activate, deactivate or modify) must be repeated in the administration documentation. If the TOE requires more than one administrator role, the relevant SEFs for each role should be identified. For each administrator role, the documentation must clearly identify:

a) which SEFs can be controlled by security parameters (e.g. selection of different user actions to be audited)

b) which SEFs provide information to the administrator (e.g. determining user privileges).

3.77 Note that certain SEFs may be included into both categories.

3.78 One method of satisfying these criteria is by presenting one or more tables illustrating the relationships between SEFs, administrator roles, control of SEF security parameters, and SEF provision of information.

If an administrator is required, it shall state all security parameters which are under his control.

3.79 These parameters must not be set in such a manner so as to cause the contravention of the SEFs of the TOE. Security parameters can also enable different possible combinations of security features of the TOE. Only security parameters which affect SEFs need be identified.

It shall state each type of security-relevant event, relevant to the administrative functions.

3.80 Security-relevant events can be interpreted as events using the SEFs of the TOE. They can include events which:

a) are auditable (if audit is part of the security enforcing functionality of the TOE)

b) are in breach of the security objectives

c) affect the configuration of the TOE

d) are user initiated, e.g. file access privilege violation, log-on failure, classification downgrade operation, password change

e) are administrator initiated, eg. system start-up, disable auditing, starting printer queues.

It shall state details, sufficient for use, of procedures relevant to the administration of security.

3.81 Both the administration of the TOE itself and of the surrounding operational environment must be detailed. The procedures must be 'sufficient for use', so for the operational environment they must contain adequate explicit details for systems, and they must contain adequate guidance for administrators of products to enable them to create suitable procedures.

It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact.

3.82 Where different security features can be configured or used in ways which would counter other security features, the guidelines must clearly indicate how the administrator can avoid subverting the security of the TOE. Similarly, the guidelines must clearly indicate effective configurations and administrative use of the TOE.

It shall state instructions on how the system/product shall be installed and how, if appropriate, it shall be configured.

3.83 The correct installation of a TOE is essential to ensure that security is enforced and maintained. Several administrator roles may be required to perform actions at particular stages of the installation. The configuration details must include suitable configurations of the security parameters.

The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level.

3.84 The ITSEC does not prescribe the structure or style of the administration documentation. Several documents may be produced, especially if there are several different administrator roles for the TOE; therefore consistency is especially important. The administration documentation must also be consistent with all the other deliverable documents, e.g. intended method of use, intended operational environment, reliance upon external hardware and software.

Requirements for Evidence

ıdministration documentation shall state how the TOE is administered in a secure manner. ITSEC E1.29

The administration documentation shall state how the TOE is administered in a secure manner.

3.85 The documentation must provide details for the secure administration of the TOE which are clear, comprehensive and effective.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

erent configurations are possible, the impact of the configurations on security shall be stated. The procedures for delivery and system generation shall be stated. ITSEC E1.32

If different configurations are possible, the impact of the configurations on security shall be stated.

3.86 The 'configuration' of the TOE in this context should be taken as meaning the setting of those features which can be given different values. The features may be termed 'configurable options', and are typically exemplified by the privileges and protections for users, devices and files on the TOE.

The procedures for delivery and system generation shall be stated.

3.87 The delivery procedures must cover the transfer of the TOE from the development environment to the operational environment, including any intermediate storage (e.g. product stockists).

3.88 'System generation' in this context applies both to products and systems, and refers to the installation and initial configuration of a TOE from distribution media or components. This can be interpreted as one of:

a) the generation of a dedicated stand alone system or product

b) the generation of a system forming part of a network

c) the generation of a product to form part of a system.

3.89 The system generation procedures must cover:

a) generation of the TOE for distribution

b) configurational system generation procedures for the operational site.

Requirements for Evidence

nformation supplied shall state how the procedures maintain security. ITSEC E1.33

The information supplied shall state how the procedures maintain security.

3.90 The statement of delivery and configuration procedures must show how security is maintained. One means of satisfying these criteria is to identify a number of possible attacks on the TOE during delivery, or a number of things that could go wrong when configuring the TOE, and show how the procedures in use will either prevent these problems or will highlight when these problems have occurred so that some action can be taken to resolve the problems.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be stated. ITSEC 1.35

The procedures for secure startup and operation shall be stated.

3.91 The procedures for ensuring that the TOE can be started and operated securely must be stated. Any relevant SEF requirements must be implemented. The procedures should indicate the relevant role for each activity, e.g. system administrator or user.

Requirements for Evidence

nformation supplied shall state how the procedures maintain security. ITSEC E1.36

The information supplied shall state how the procedures maintain security.

3.92 The statement of startup and operation procedures must show how security is maintained. One means of satisfying these criteria is to identify a number of things that could go wrong when starting up or operating the TOE, and show how the procedures in use will either prevent these problems or will highlight when these problems have occurred so that some action can be taken to resolve the problems.

Chapter 4 Level E2

Overview of E2 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE

Architecture:

- Informal description of the architecture of the TOE

Detailed Design:

- **Informal description of the detailed design**

Implementation:

- **Test documentation**
- **Library of test programs and tools used for testing the TOE**

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation
- **Information on the configuration control system**

Programming Languages and Compilers:

- [no deliverables required]

Developer's Security:

- **Information on the security of the development environment**

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall state the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. The security enforcing functions within the security target shall be specified using an informal style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E2.2

4.1 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

case of a system the security target shall state how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall state how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. ITSEC E2.3

4.2 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Phase 2 - Architectural Design

Requirements for Content and Presentation

escription of the architecture shall state the general structure of the TOE. It shall state the external interfaces of the TOE. It shall state any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. **It shall state the separation of the TOE into security enforcing and other components.** ITSEC E2.5

It shall state the separation of the TOE into security enforcing and other components.

4.3 A fundamental ITSEC requirement (paragraph 4.20 of the ITSEC [Reference 0]) at E2 and higher levels is the clear and effective separation of security enforcing components from the other components in the TOE.

4.4 Security enforcing components are those which directly contribute to satisfying the security objectives of the TOE. Separation through all layers of the design and implementation enables the evaluation to concentrate on the parts of the TOE that contribute to security and, therefore, reduce the amount of evaluation work performed.

4.5 Security enforcing components must be clearly defined and relate either to a single SEF or to a practical grouping of security enforcing functionality, e.g. only access control, and not to a mixture.

4.6 At E2, simple identification is required for the security enforcing components present in the architectural design at the greatest level of granularity. The separation must be consistent with the security target and the description of the architecture.

4.7 If no separation is claimed by a developer, then all the TOE is treated as potentially security enforcing, with a consequent increase in the amount of evaluation work. Lack of separation also reduces the likelihood of being able to reuse the results of the evaluation for future TOE variants or upgrades.

4.8 The degree of complexity of the architectural design can affect the following aspects which are taken into account at E2 and higher levels:

a) traceability

b) the ease with which an architectural design can be refined to produce the corresponding detailed design.

Requirements for Evidence

escription of the architecture shall state how the security enforcing functions of the security target will be provided. **It shall state how the separation into security enforcing and other components is achieved.** ITSEC E2.6

It shall state how the separation into security enforcing and other components is achieved.

4.9 A means by which separation is achieved must be identified, to show how the security enforcing components are kept separate from those components that are security irrelevant.

4.10 Types of separation can include physical, state-based (logical) and temporal mechanisms. Consideration should be given as to whether only one type of separation is sufficient to prevent a security enforcing component from interference by the non security enforcing components.

4.11 Where a TOE contains certified products it is necessary to ensure that the security objectives of each certified product cannot be breached by other parts of the TOE. In such circumstances, the evidence provided must state how separation is achieved between the security enforcing components provided by each certified product and the other parts of the TOE.

Phase 3 - Detailed Design

Requirements for Content and Presentation

etailed design shall state the realisation of all security enforcing and security relevant functions. It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and components. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters. Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels. ITSEC E2.8

4.12 It should be noted that the degree of rigour required is **state** as detailed in Part III of this Guide.

4.13 The developer should provide relevant standards and procedures, stating the terms, notations and methods used in the design, to assist evaluators with their understanding of the documentation.

4.14 When considering whether to use a Computer Aided Software Engineering (CASE) tool to produce the detailed design, the developer is recommended to consider the guidance in Part III of this Guide.

4.15 Where a CASE tool is used, consideration should be given to either providing the evaluation team with a copy of the tool's database and, if necessary, access to the developer's tool. This could reduce the amount of evaluation work required on the detailed design.

The detailed design shall state the realisation of all security enforcing and security relevant functions.

4.16 Each representation must provide a less abstract refinement of the previous level and correctly preserve the intent of the architectural design.

4.17 Some non security enforcing components may be identified whose failure or misuse could compromise security. These components are called security relevant, as their correct operation is relied upon for the TOE to enforce security. Usually at E2 these components are not identified until the detailed design, although it is feasible that they could be specified in the architectural design.

4.18 The detailed design documentation (i.e. application and module specifications) should specify the security mechanisms of the design that implement each of the security enforcing functions defined in the security target.

It shall identify all security mechanisms.

4.19 The product may include one or more common mechanisms which perform a certain function for a number of components throughout the system. The developer should decide which of these mechanisms are relevant to security, i.e. security mechanisms, and clearly identify them within the detailed design. (See Part I of this Guide for a definition of security mechanisms).

4.20 In addition, some of the security mechanisms may be considered critical, i.e. a mechanism whose failure would undermine security. These mechanisms must be considered in the strength of mechanisms analysis which analyses the ability of these mechanisms to withstand direct attack (Refer to the details on Strength of Mechanisms Analysis in Section 2 of this Part of the Guide, and in Part 3 of the Guide).

4.21 Each security enforcing, or security relevant, function must be implemented by at least one security mechanism. Each security mechanism can implement one or more security enforcing or security relevant functions.

4.22 For example, an encryption device may have two security enforcing functions. The first security enforcing function requires user data to be encrypted by a data encrypting key. The second security enforcing function requires that the key which encrypts the user data should itself be encrypted by a key encrypting key. Two separate components may implement these security enforcing functions, but they may use a common encryption mechanism. In this case the mechanism is a critical mechanism.

It shall map security enforcing functions to mechanisms and components.

4.23 One of the fundamental principles of the ITSEC is for traceability information to be provided. Thus, it must be possible to demonstrate how the security enforcing functions (SEFs) specified in the security target are represented in the detailed design.

4.24 The detailed design documentation should correlate the SEFs defined in the security target to the individual components or security mechanisms.

4.25 One approach to the correlation is as follows. Each SEF should have been given a unique identifier in the security target, e.g. SEF 1, SEF 2 etc. In the detailed design a table can be included which identifies each security enforcing function in one column. In an adjacent column, a reference could be included to a section of the detailed design document where there is a specification of a corresponding component or mechanism.

4.26 Additionally, the Certification Body expects a correlation to be provided between the security enforcing components identified in the architectural design and the mechanisms and components in the detailed design. It is likely that the developer will produce this correlation as a matter of course during the design decomposition process.

All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters.

4.27 Not only must the required information be provided, but each interface must be consistent with:

a) the functionality provided by the security enforcing or security relevant component

b) use by other components of the TOE.

4.28 All interfaces should be specified correctly and be capable of fulfilling their purpose. Where appropriate, parameters passed between the components must be identified.

4.29 Interfaces referenced in the specifications of security enforcing and security relevant components must exist in the detailed design.

Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed.

4.30 The term 'mechanisms' in this instance refers to the logic or algorithms which implement the security enforcing or security relevant functions. These mechanisms will generally be the security mechanisms identified for the TOE. The detailed design should include definitions of the mechanisms so that it is possible to see how they interrelate and whether one could conflict with the operation of another (this information will be necessary for the binding analysis).

4.31 The specification of mechanisms may also be used in verifying the strength attributed to the mechanism in the strength of mechanisms analysis.

Specifications need not be provided for components that are neither security enforcing nor security relevant.

4.32 For evaluation purposes it is not required to provide specifications for components of the product which are neither security enforcing nor security relevant. In practice it may not be practical to separate the components in this way and information on all of the components may provide useful background information for the evaluation team.

Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels.

4.33 Depending on the development methods employed and the complexity of the TOE, the detailed design may comprise a number of levels of specification, each level being a further refinement of the last. The levels of specification may be contained within a single design document, or documented separately. Major components of the design may also be documented separately within each level.

4.34 In cases where the detailed design consists of documentation of varying levels of detail, then it should be clear how each level in the design relates. For example, textual program specifications may be supported by diagrammatic representations of data flows or definitions of data entities. In this case each of these supporting representations should be clearly referenced. It is also important for the highest level of representation within the detailed design to correlate to the architectural design.

Requirements for Evidence

etailed design shall state how the security mechanisms provide the security enforcing functions specified in the security target. It shall state why components for which no design information is provided cannot be either security enforcing or security relevant. ITSEC E2.9

The detailed design shall state how the security mechanisms provide the security enforcing functions specified in the security target.

4.35 This aspect is closely related to the detailed design requirement to map security enforcing functions to mechanisms. While the mapping information provides references to those sections of the detailed design where supporting information can be found, this aspect requires a statement of how the mechanisms implement the SEFs defined in the security target.

It shall state why components for which no design information is provided cannot be either security enforcing or security relevant.

4.36 Although at level E2 it is not necessary to provide specifications for components which are not security enforcing nor security relevant, the developer is responsible for providing evidence that the components for which no design information is provided are neither security enforcing nor security relevant.

Phase 4 - Implementation

4.37 When performing tests at E2 and higher levels, the developer should ensure that:

a) each SEF has at least one test, and that all aspects of each SEF's specification are covered by the tests

b) the results obtained from the tests are accurately recorded and checked against expected results

c) all test material is kept under configuration control

d) details of the version and configuration of the TOE are recorded.

4.38 Before the testing process starts, a sponsor should make arrangements with the TOE's developer to give the evaluation team an opportunity to witness the tests.

4.39 The ITSEC does not prescribe any particular test strategy by the developer. However, the structuring of test documentation, where possible, such that the security enforcing and security relevant aspects are easily identifiable, can reduce the amount of work undertaken by the evaluation team. Where large automated test suites are used, the sponsor will need to identify those tests which directly involve SEFs.

> ***Requirements for Content and Presentation***
>
> **est documentation shall contain plan, purpose, procedures and results of the tests. The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated.** ITSEC E2.11

The test documentation shall contain plan, purpose, procedures and results of the tests.

4.40 This is mandatory at E2 and higher assurance levels. The tests must be objective and repeatable.

The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated.

4.41 This is mandatory at E2 and higher assurance levels. Tools are required when they are necessary to enable repetition of tests. The evaluation team must be given access to such tools.

Requirements for Evidence

:est documentation shall state the correspondence between tests and the security enforcing functions defined in the security target. ITSEC E2.12

The test documentation shall state the correspondence between tests and the security enforcing functions defined in the security target.

4.42 This is mandatory at E2 and higher assurance levels. Tests should be provided for each SEF. For E2 to E5 the correspondence must relate to the informal representation of the SEFs.

4.43 When performing tests at E2 and higher levels, the SEFs should be:

a) exercised to an appropriate degree (dependent upon the rigour of the specification)

b) negatively tested for the absence of expected functionality, as well as positively tested for the presence of expected functionality.

Construction - The Development Environment

Aspect 1 - Configuration Control

Requirements for Content and Presentation

levelopment process shall be supported by a configuration control system. The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes are possible. ITSEC E2.15

The development process shall be supported by a configuration control system.

4.44 The ITSEC requirements for content, presentation and evidence for configuration control reiterate parts of standards such as BS EN ISO 9001. The ITSEC places no requirements on the sponsor or developer for accreditation to external quality standards; however, a configuration control system must be used, and must meet the ITSEC requirements.

The configuration list provided shall enumerate all basic components out of which the TOE is built.

4.45 While basic components in detailed design terms are defined as the most detailed level of granularity in the detailed design, in configuration terms the sponsor or developer may have to choose a different set of 'basic components' as configuration items, depending upon the nature and complexity of the TOE. Information should be provided to support any different interpretation used.

4.46 The objective of this ITSEC requirement is that it should be possible to rebuild the TOE. Therefore, not only should all TOE components be identified, but also all the elements necessary for building the TOE, for example, hardware, documentation, test equipment, command files, development tools, etc.

4.47 If an automated configuration control system is used, the developer must inform the evaluation team of the nature of the definitive master record (e.g. hardcopy or computer media).

4.48 When listing previously evaluated components, it is permissible for the configuration list to identify only the unique identification of the overall component.

4.49 The configuration list should be provided as early as possible to the evaluation team. If the TOE is subsequently modified during the evaluation, updated details should be issued by the developer.

The TOE, its basic components and all documents provided including the manuals shall possess a unique identifier. The use of this unique identifier is obligatory in references.

4.50 The identification must be unique for each item within the TOE, and for different versions of each item. Exact copies of the TOE (e.g. copies of a mass-produced product) do not have to be individually identified.

4.51 When incorporating previously evaluated components, it is permissible use the unique identifiers already assigned to such components.

4.52 The most appropriate format of identifiers may be chosen and, particularly for composite TOEs, different formats may be used within the overall TOE.

The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes are possible.

4.53 The configuration control procedures must indicate the process by which authorised changes can be made.

Requirements for Evidence

nformation on the configuration control system shall state how it is used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures. ITSEC E2.16

The information on the configuration control system shall state how it is used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures.

4.54 The configuration control deliverables must state the configuration control process for the development of the TOE. They must be adequately defined, i.e. documented:

a) clearly

b) unambiguously

c) with a degree of rigour appropriate to the assurance level.

4.55 Where several organisations are developing components of the TOE, it is permissible for more than one configuration control system to be used. However, care must be taken to ensure that data from the various configuration control systems can be incorporated into a configuration control system covering the whole TOE.

4.56 When incorporating previously evaluated or Commercial-Off-The-Shelf (COTS) components, the configuration control measures used during their development do not need to be stated. However, any measures dealing with the integration of the components within the TOE must be stated.

Aspect 2 - Programming Languages and Compilers

4.57 There are no programming languages and compilers requirements at this assurance level.

Aspect 3 - Developer's Security

4.58 The objective of the ITSEC criteria relating to developer's security is to prevent the compromise of the integrity or confidentiality of the TOE by a malicious person, either internal or external to the development team. There is a degree of overlap between this objective and the objective of the ITSEC criteria for configuration control.

4.59 The developer should undertake a risk assessment for the development. The developer's security for the TOE may be influenced by:

a) the threats for the TOE's development

b) the sponsor's requirements for development security

c) other threats and factors affecting the TOE development site.

4.60 The developer may have already been assessed by external bodies for physical and personnel security; for example, for TOEs procured by HMG.

4.61 Developers unfamiliar with the general security issues for development environments should contact the Certification Body for guidance.

Requirements for Content and Presentation

locument on the security of the development environment shall state the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be stated. ITSEC E2.21

The document on the security of the development environment shall state the intended protection for the integrity of the TOE and the confidentiality of the associated documents.

4.62 The most important issue for development security is the integrity of the TOE, i.e. confidence that the developed, evaluated and installed TOEs are all the same. Where the security of the TOE relies on (some part of) its design not being known to an attacker, then the confidentiality of the TOE documentation will become an issue. Similarly, the security of the TOE may rely retaining the confidentiality of the implementation of a particular algorithm in the TOE.

4.63 The documentation must state the intended degree of protection necessary to ensure the integrity of the TOE and the confidentiality of the associated documents.

Physical, procedural, personnel and other security measures used by the developer shall be stated.

4.64 The countermeasures must be sufficient to achieve the intended degree of protection necessary to ensure the integrity of the TOE and the confidentiality of the associated documents.

4.65 The developers should consider, as a minimum, controlling access to, and copying of, (versions of) the TOE, associated documentation (including development practices) and development tools.

4.66 In general, a 'defence in depth' approach will prove cost-effective by enabling simpler countermeasures to be used in combination against the threats.

Requirements for Evidence

nformation on the security of the development environment shall state how the integrity of the TOE and the confidentiality of the associated documentation are maintained. ITSEC E2.22

The information on the security of the development environment shall state how the integrity of the TOE and the confidentiality of the associated documentation are maintained.

4.67 The documentation must state how the chosen countermeasures are to be supported throughout the TOE's development, maintenance and archive. Procedures for review and audit of the countermeasures must be provided.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

ser documentation shall state the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E2.25

4.68 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

ser documentation shall state how an end-user uses the TOE in a secure manner. ITSEC E2.26

4.69 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

ıdministration documentation shall state the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall state all security parameters which are under his control. It shall state each type of security-relevant event, relevant to the administrative functions. It shall state details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall state instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E2.28

4.70 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

dministration documentation shall state how the TOE is administered in a secure manner. ITSEC E2.29

4.71 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

> ***Requirements for Procedures and Standards***
>
> erent configurations are possible, the impact of the configurations on security shall be stated. The procedures for delivery and system generation shall be stated. **A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated.** ITSEC E2.32

A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE.

4.72 Part III of this Guide provides guidance on procedures considered to be acceptable by the UK Certification Body.

While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated.

4.73 The audit data may be either manually or automatically recorded. Care should be taken to ensure that any manually recorded data is correct and complete.

4.74 The extent of the level of detail and accuracy necessary for recording the generation time should be such as to be able to reproduce the specific instantiation of the TOE.

4.75 The system generation audit for a system must cover both the following types, whereas the system generation audit for a product must cover only the first:

a) generation of the TOE for distribution

b) configurational system generation procedures for the operational site.

Requirements for Evidence

formation supplied shall state how the procedures maintain security. ITSEC E2.33

4.76 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be stated. **If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be stated. If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment.** ITSEC E2.35

If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be stated.

4.77 Any possible override of SEFs, whether intentional or not, must be stated.

If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment.

4.78 The tests are intended to give operators and users of the TOE confidence in the correct operation of any security enforcing hardware components. The test must be able to be performed while the TOE is still in its operational environment, i.e. they must not require the TOE to be removed from its working location. However, the diagnostic tests may require the TOE to be temporarily inoperative while the tests are executed.

4.79 The scope of the tests must cover all security enforcing aspects of the hardware.

4.80 Note that the inclusion within the TOE of, or the use of, diagnostic tests may create additional threats to the TOE and consequent potential vulnerabilities. The threats should be addressed by the sponsor and incorporated with any appropriate SEFs or relevant security operating procedures in the security target. This aspect should be considered prior to the start of the evaluation to minimise the likelihood of any impact on the evaluation.

Requirements for Evidence

ıformation supplied shall state how the procedures maintain security. **The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during startup and operation.** ITSEC E2.36

The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components.

4.81 The results may be either manually recorded or automatically generated. Care should be taken to ensure the accuracy and completeness of manually recorded results.

The sponsor shall provide examples of any audit trail output created during startup and operation.

4.82 If an audit trail output is produced by the TOE, it must be supplied by the developer or sponsor, whether or not it is stipulated by any of the TOE's SEFs. For the purposes of this criterion, an audit trail can be considered as the TOE's record of start-up or operation, even if it is not intended as a true audit trail.

4.83 Procedures must exist for the proper handling and storage of any audit trail output.

Chapter 5 Level E3

Overview of E3 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE

Architecture:

- Informal description of the architecture of the TOE

Detailed Design:

- Informal description of the detailed design

Implementation:

- Test documentation
- Library of test programs and tools used for testing the TOE
- **Source code or hardware drawings for all security enforcing and security relevant components**
- **Informal description of correspondence between source code or hardware drawings and the detailed design**

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system
- **Information on the acceptance procedure**

Programming Languages and Compilers:

- **Description of all implementation languages used**

Developer's Security:

- Information on the security of the development environment

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall **describe** the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. The security enforcing functions within the security target shall be specified using an informal style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E3.2

5.1 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

5.2 Descriptions must be provided as to how the SEFs are to be provided for the particular TOE. Where a functionality class is claimed, this description must be traceable to the statements in the functionality class.

Requirements for Evidence

case of a system the security target shall **describe** how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall **describe** how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. ITSEC E3.3

5.3 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Phase 2 - Architectural Design

Requirements for Content and Presentation

escription of the architecture shall **describe** the general structure of the TOE. It shall **describe** the external interfaces of the TOE. It shall **describe** any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. It shall **describe** the separation of the TOE into security enforcing and other components. ITSEC E3.5

5.4 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

lescription of the architecture shall **describe** how the security enforcing functions of the security target will be provided. It shall **describe** how the separation into security enforcing and other components is achieved. ITSEC E3.6

5.5 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Phase 3 - Detailed Design

Requirements for Content and Presentation

letailed design shall specify all basic components. It shall **describe** the realisation of all security enforcing and security relevant functions. It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and components. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters. Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels. ITSEC E3.8

5.6 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

The detailed design shall specify all basic components.

5.7 All components that are identifiable at the lowest hierarchical level of detailed design specification must be specified, e.g. all functions, procedures and subroutines identified in the detailed design must be defined. The detailed design specification must correspond with the degree of rigour required and be consistent with higher hierarchical levels of the design.

5.8 This information may be used to contribute to the binding analysis where insufficient detail of relevance to the binding analysis is included in the mechanism specifications.

It shall ***describe*** *the realisation of all security enforcing and security relevant functions.*

5.9 The level of rigour has increased over that required for E2. Therefore, the detailed design documentation that specifies the program modules/procedures, which implement each of the security enforcing and security relevant functions, must be described (e.g. the inputs and outputs to each module should be identified and the major operations each module performs should be identified and described).

Requirements for Evidence

etailed design shall **describe** how the security mechanisms provide the security enforcing functions specified in the security target. It shall **describe** why components for which no design information is provided cannot be either security enforcing or security relevant. ITSEC E3.9

The detailed design shall ***describe*** *how the security mechanisms provide the security enforcing functions specified in the security target.*

5.10 The level of rigour has increased over that required for E2. Therefore, the design documentation must describe how the mechanisms implement the security enforcing functions defined in the security target.

It shall ***describe*** *why components for which no design information is provided cannot be either security enforcing or security relevant.*

5.11 The level of rigour has increased over that required for E2. Therefore, the justification for components being neither security enforcing nor security relevant must be described.

Phase 4 - Implementation

Requirements for Content and Presentation

escription of correspondence shall describe the correspondence between source code or hardware drawings and basic components of the detailed design. The test documentation shall contain plan, purpose, procedures and results of the tests. The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated. ITSEC E3.11

5.12 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

The description of correspondence shall describe the correspondence between source code or hardware drawings and basic components of the detailed design.

5.13 An informal correlation between the source code or hardware drawings and the basic components is required. The degree of detail must be sufficient for the entirety of the source code or hardware relating to each basic component to be clearly identified. Correspondence could be provided by using the source code module names in the detailed design documentation; in this case, no additional correspondence information would be needed.

5.14 Although only a one-way correspondence is mandated, the developer may find it helpful to produce a two-way correspondence.

Requirements for Evidence

ɘst documentation shall **describe** the correspondence between tests and the security enforcing functions defined in the security target. **It shall describe the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design. It shall describe the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings. Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced.** ITSEC E3.12

5.15 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

It shall describe the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design.

5.16 An informal correlation between the tests and the security enforcing and security relevant functions is required. The application of suitable unique identification codes to the tests and the security enforcing and security relevant functions may assist this activity.

5.17 If the sponsor and developer do not describe how the security enforcing and security relevant components are separated from the security irrelevant components, then the evaluators will be required to treat the entire TOE as if it were relevant to security and potentially security enforcing. In this case, tests must be provided to cover the whole of the functionality described in the detailed design and source code.

5.18 Although only a one-way correspondence is mandated (i.e. links between the tests and the security enforcing and security relevant functions), the developer may find it helpful to produce a two-way correspondence (i.e. links between the tests and the security enforcing and security relevant functions and vice versa).

It shall describe the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings.

5.19 An informal correlation between the tests and the security mechanisms is required. The application of suitable unique identification codes to the tests and the security mechanisms may assist this activity.

5.20 Although only a one-way correspondence is mandated, the developer may find it helpful to produce a two-way correspondence.

5.21 Note that, at E3, one method of achieving adequate coverage of source code is if the sponsor/developer can demonstrate that every statement of security enforcing and security relevant source code has been tested.

Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced.

5.22 When an error is revealed by a test, the process followed to eliminate the error and perform retesting must adhere to the developer’s quality procedures including change and configuration control. Satisfactory evidence must be produced to the evaluation team, and could include some form of report detailing the nature of the error, its impact, the rework required, any authorisations required and subsequent retesting results.

5.23 Depending on the nature of the test the developer may:

a) suspend the test until the error has been fixed

b) insert a temporary patch to enable testing to proceed

c) continue the testing with a known fault.

5.24 Before making a change to a software or hardware component of a TOE, the developer should first perform a detailed analysis of the change in order to fully understand the implications and the possible impact on other components of the TOE. It is often the case, that in correcting a known error, a change cannot be made to a single hardware or software part of a TOE in isolation.

5.25 The implications of a change to a hardware or software component are that:

a) tests which have already been completed successfully may need to be rerun (regression testing)

b) test specifications may need to be amended.

5.26 The developers should provide evidence that the extent of retesting after fault correction is adequate. This could be by recording the dependencies between software and/or hardware components of the TOE implementation. Where such evidence is not made available, complete retesting of the TOE will be required.

5.27 The practice of applying software, hardware or test specification 'patches' (temporary changes to enable testing to proceed after a fault is encountered) should be carried out in a controlled manner.

5.28 Where patches are applied to software, hardware or test specifications, the developer should ensure that:

a) the patch applied is described in the test documentation

b) if a patch is required to successfully complete a test then the test outcome is recorded as a 'fail' and the appropriate quality procedures are invoked

c) there is adequate separation between any parts of the software and the locally patched software

d) All tests performed using a patch to the TOE (software or hardware) or performed using modified test input are formally repeated when the corrected software, hardware or test scripts are re-issued.

5.29 Temporary software or hardware patches are not considered acceptable during acceptance tests.

5.30 Before undertaking retests, where these are performed during the course of the evaluation, the developer should offer the evaluation team an opportunity to witness the retests. This will provide an added measure of confidence, and may reduce the effort required during the visits to the development site, either as part of the development environment assessment or as part of the penetration testing.

Construction - The Development Environment

Aspect 1 - Configuration Control

Requirements for Content and Presentation

evelopment process shall be supported by a configuration control system **and an acceptance procedure.** The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals **and the source code or hardware drawings** shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes are possible. ITSEC E3.15

The development process shall be supported by a configuration control system ***and an acceptance procedure.***

5.31 An acceptance procedure must be used to ensure that the TOE's constituent parts are of adequate quality prior to their incorporation within the TOE. The procedure should cover:

a) each stage of building the TOE, e.g. module, integration, system

b) software, firmware and hardware

c) the acceptance of previously evaluated or COTS components.

The TOE, its basic components and all documents provided including the manuals ***and the source code or hardware drawings*** *shall possess a unique identifier.*

5.32 This requirement extends the scope of the items requiring unique identifiers. Where possible, the identifiers should be included within the original derivation of the source code (e.g. in the header or comment field) or in the automated form of drawings prior to producing hardcopy output.

Requirements for Evidence

nformation on the configuration control system shall **describe** how it is used in practice and applied in the manufacturing process in accordance with the developer’s quality management procedures. ITSEC E3.16

5.33 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

programming languages used for implementation shall be well-defined, e.g. as in an ISO standard. Any implementation dependent options of the programming language shall be documented. ITSEC E3.18

Any programming languages used for implementation shall be well-defined, e.g. as in an ISO standard.

5.34 This requirement applies to basic components implemented in software and firmware only.

5.35 The developer may wish to consider well-defined languages according to whether the languages have:

a) a reference to a recognised standards document defining the language

b) a formal syntax.

Any implementation dependent options of the programming language shall be documented.

5.36 Any differences from standard languages must be documented.

5.37 The options may either be documented by the developer or contained in a reference source which is made available to the evaluation team.

5.38 At E3, the options actually used in the development are not required to be documented, although, if this information exists, it may reduce the evaluation team's work.

Requirements for Evidence

lefinition of the programming languages shall define unambiguously the meaning of all statements used in the source code. ITSEC E3.19

The definition of the programming languages shall define unambiguously the meaning of all statements used in the source code.

5.39 The nature of programming languages hinders the detection of ambiguities in a language description. Ambiguities can exist in both the syntax and semantics of even formally defined languages. The developer should carefully select languages to minimise this problem. In difficult cases the developer may approach the Certification Body for guidance. The following checklist may assist the developer:

a) very widely used, relatively simple languages are likely to be well-defined

b) complex languages with complex run time systems are difficult to define completely

c) in the language definition, phrases such as "the effect of this construct is undefined" and terms such as "implementation dependent" or "erroneous" may indicate ill-defined areas

d) aliasing (allowing the same area of memory to be referenced in different ways) is a common source of ambiguity problems

e) exception handling (i.e. what happens after departures from expected states) is poorly defined.

Aspect 3 - Developer's Security

Requirements for Content and Presentation

locument on the security of the development environment shall **describe** the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be **described.** ITSEC E3.21

5.40 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

nformation on the security of the development environment shall **describe** how the integrity of the TOE and the confidentiality of the associated documentation are maintained. ITSEC E3.22

5.41 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

ser documentation shall **describe** the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E3.25

5.42 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

ser documentation shall **describe** how an end-user uses the TOE in a secure manner. ITSEC E3.26

5.43 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

5.44 At E3 and E4, the user guides might describe what happens when using the chmod command, for example:

a) The chmod command must be used to change the access permissions on a file

b) The syntax of the chmod command is

chmod (*filename*, *permission-list*) [/+*echo* | /-*echo*]

where:

filename is the name of the file for which the access permissions are to be changed
permission-list is the string describing the new access permissions in the following format (...)
echo is an optional parameter allowing the user to choose whether to view the result of the chmod command. The default setting is /+echo (echo on), which causes the filename and new access permissions to be displayed. Setting -echo (echo off) causes the display of the result of the chmod command to be suppressed and replaced by a simple 'OK' response.

c) The possible responses to the chmod command are as follows:

- a filename and a list of permissions in the following format: (...). This indicates that the chmod command did not detect an error, and that the echo option was selected.
- the 'OK' response. This indicates that the chmod command did not detect an error, and that the echo option was not selected.
- an error message. The text of the error message may indicate a syntax error, or that the user does not have sufficient privilege to change the access permissions for the file. (... or any other error ...)

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

dministration documentation shall **describe** the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall **describe** all security parameters which are under his control. It shall **describe** each type of security-relevant event, relevant to the administrative functions. It shall **describe** details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall **describe** instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E3.28

5.45 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

lministration documentation shall **describe** how the TOE is administered in a secure manner. ITSEC E3.29

5.46 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

ferent configurations are possible, the impact of the configurations on security shall be **described.** The procedures for delivery and system generation shall be **described.** A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated. ITSEC E3.32

5.47 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

ıformation supplied shall **describe** how the procedures maintain security. ITSEC E3.33

5.48 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be **described.** If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be **described.** If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment. ITSEC E3.35

5.49 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Requirements for Evidence

nformation supplied shall **describe** how the procedures maintain security. The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during startup and operation. ITSEC E3.36

5.50 It should be noted that the degree of rigour required is **describe** as detailed in Part III of this Guide.

Chapter 6 Level E4

Overview of E4 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE
- **Definition of, or reference to, an underlying formally specified model of security**
- **Informal interpretation of the underlying model in terms of the security target**

Architecture:

- **Semiformal** description of the architecture of the TOE

Detailed Design:

- **Semiformal** description of the detailed design

Implementation:

- Test documentation
- Library of test programs and tools used for testing the TOE
- Source code or hardware drawings for all security enforcing and security relevant components
- Informal description of correspondence between source code or hardware drawings and the detailed design

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- **Audit information on modification of all parts of the TOE subject to configuration control**
- Information on the acceptance procedure

Programming Languages and Compilers:

- Description of all implementation languages used
- **Description of all compilers used**

Developer's Security:

- Information on the security of the development environment

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall describe the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. **A formal model of security policy shall be provided or referenced to define the underlying security policy to be enforced by the TOE. An informal interpretation of this model in terms of the security target shall be provided.** The security enforcing functions within the security target shall be specified using **both** an informal and **semiformal** style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E4.2

A formal model of security policy shall be provided or referenced to define the underlying security policy to be enforced by the TOE.

6.1 Refer to Part III of this Guide for guidance on formal security policy models.

An informal interpretation of this model in terms of the security target shall be provided.

6.2 Part III of this Guide provides guidance on formal security policy models, and the informal interpretation of such. It is important to ensure that the informal interpretation does not provide any information that is not included in the formal specification; the informal interpretation should provide supporting information only.

The security enforcing functions within the security target shall be specified using ***both*** *an informal and* ***semiformal*** *style as categorised in Chapter 2 (of the ITSEC [Reference 0]).*

6.3 Information on suitable types of semiformal specification can be found in Part III of this Guide.

6.4 Descriptions in both informal text and semiformal notation must be provided as to how the SEFs are to be provided for the particular TOE. The informal text should be consistent with the semiformal specification for each SEF. The informal text should not add any extra functionality which is not defined in the semiformal specification, but it should provide a description in natural language.

6.5 Where a functionality class is claimed, both the informal description and the semiformal description must be traceable to the statements in the functionality class. Note that where an ITSEC example functionality class is claimed, it must be rewritten in semi-formal notation.

Requirements for Evidence

case of a system the security target shall describe how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall describe how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. **The informal interpretation of the formal security policy model shall describe how the security target satisfies the underlying security policy.** ITSEC E4.3

The informal interpretation of the formal security policy model shall describe how the security target satisfies the underlying security policy.

6.6 The definition of an underlying formally specified model of security (or a reference to a suitable published model) must be provided which models the essential security characteristics embodied in an overall security requirement.

6.7 Guidance on formal security policy models is given in Part III of this Guide.

6.8 Sponsors and developers 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.

Phase 2 - Architectural Design

Requirements for Content and Presentation

niformal notation shall be used in the architectural design to produce a semiformal description. It shall describe the general structure of the TOE. It shall describe the external interfaces of the TOE. It shall describe any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. It shall describe the separation of the TOE into security enforcing and other components. ITSEC E4.5

A semiformal notation shall be used in the architectural design to produce a semiformal

description.

6.9 Part III of this Guide provides guidance on semiformal specification of the SEFs. While informally specified SEFs are written in natural language, which is defined as a notation not requiring special restrictions or conventions, it is important to ensure that SEFs are specified and are therefore clear, consistent and unambiguous.

6.10 The language used for expressing the architectural design must be capable of expressing features relevant to security. For instance, both data models and data flow diagrams qualify as semiformal notations. However, a single notation, such as a data model or data flow diagrams, may not be capable of expressing every facet of a TOE's architecture. In this case, use can be made of several notations which, in combination, will provide a complete picture of the architecture.

6.11 Semiformal notations should be capable of illustrating the general structure of the TOE, its decomposition into major components, and how these components interact to provide the SEFs in the security target. It must be possible to show the separation of the TOE into security enforcing and other components.

6.12 Care should be taken when following structured design methods, such as SSADM, which provide logical separation rather than physical separation of security functionality. Additional design documentation may be necessary to demonstrate sufficient separation.

6.13 An informal description, in addition to the semiformal description, is not required by the ITSEC. If an informal description is included to support the semiformal one, its purpose should be to explain the semiformal one and make the semiformal one easier to understand, and not to augment it. The following rule should be followed:

Where a semiformal description includes a semiformal part and informal prose, the informal prose should not enumerate security relevant facts which are not covered by the semiformal part.

Requirements for Evidence

escription of the architecture shall describe how the security enforcing functions of the security target will be provided. It shall describe how the separation into security enforcing and other components is achieved. **It shall describe how the chosen structure provides for largely independent security enforcing components.** ITSEC E4.6

It shall describe how the chosen structure provides for largely independent security enforcing

components.

6.14 A description must be provided showing how the structure of the architectural design enables the majority of security enforcing components to be independent from the other security enforcing components.

6.15 Formal or semi-formal modelling, or animation of an architectural design can provide an objective means of demonstrating the separation of security enforcing components. Animation is the exercising of an executable description of the design. Where such modelling or animation is undertaken and is used to justify the separation, the evaluators should be given access to the model or animation and the results obtained.

Phase 3 - Detailed Design

Requirements for Content and Presentation

niformal notation shall be used to develop a semiformal detailed design. The detailed design shall specify all basic components. **It shall describe, through all levels of the design hierarchy, the realisation of all security enforcing and security relevant functions. It shall describe the separation of the TOE into security enforcing, security relevant and other components. It shall be structured into well-defined, largely independent basic components that facilitate testing and minimise the potential for violations of security.** It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and components. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters. Specifications/definitions for mechanisms shall be provided, These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels. ITSEC E4.8

A semiformal notation shall be used to develop a semiformal detailed design.

6.16 The developer must ensure that the notations used, and the manner of their use, are appropriate. The semiformal notation used must conform to the ITSEC definition of semiformal. Acceptable semiformal styles include graphical representation (e.g. data flow diagrams, process structure diagrams) or a restricted use of natural language. Part III of this Guide gives a more detailed discussion of the requirements for semiformal notations.

6.17 All the detailed design must be expressed using semiformal notation. If more than one notation is used, the developer should ensure that the design maintains completeness, consistency and traceability. An equivalent informal expression of the design is not required for evaluation purposes, but can be useful to assist the evaluators' understanding of the detailed design. In some cases, the accompanying informal text may be essential to understanding the semiformal or formal parts of the specification.

6.18 The evaluation team may require access to any automated tools and associated databases used to create the design.

It shall describe, through all levels of the design hierarchy, the realisation of all security enforcing and security relevant functions.

6.19 Intermediate levels of specification may exist, depending on the development method employed and the complexity of the TOE. The realisation of all security enforcing and security relevant functions must be detailed, both within each level of the design hierarchy, and across each level.

6.20 Each representation must provide a less abstract refinement of the previous level and correctly preserve the intent of the architectural design.

It shall describe the separation of the TOE into security enforcing, security relevant and other components.

6.21 The techniques and manner in which the separation is achieved must be documented.

It shall be structured into well-defined, largely independent basic components that facilitate testing and minimise the potential for violations of security.

6.22 A basic component is the most detailed level of granularity in the detailed design. It would usually correspond to a process, entry point, compilation unit, function or procedure. The only minimum requirement for granularity of a detailed design is that it be sufficiently detailed to enable coding to take place without any further refinement.

6.23 The use of automated tools to enforce a semiformal design notation is likely to assist with meeting this requirement.

Requirements for Evidence

letailed design shall describe how the security mechanisms provide the security enforcing functions specified in the security target. It shall describe why components for which no design information is provided cannot be either security enforcing or security relevant. ITSEC E4.9

6.24 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Phase 4 - Implementation

Requirements for Content and Presentation

lescription of correspondence shall describe the correspondence between source code or hardware drawings and basic components of the detailed design. The test documentation shall contain plan, purpose, procedures and results of the tests **and a justification why the extent of test coverage is sufficient.** The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated. ITSEC E4.11

The test documentation shall contain plan, purpose, procedures and results of the tests ***and a justification why the extent of test coverage is sufficient.***

6.25 The ITSEC paragraph 4.22 states:

... it will be necessary at higher evaluation levels to supplement testing by analysis.

6.26 Note that, at E4 and higher assurance levels, one method of achieving adequate coverage of source code is if the sponsor/developer can demonstrate that every statement and branch of all source code belonging to a security enforcing or security relevant basic component has been tested.

6.27 If automated test coverage analysers are used as part of the test procedures, then the results of the analysis must be included in the test documentation as evidence that the specified tests provide the degree of coverage stated by the developer.

Requirements for Evidence

ɘst documentation shall describe the correspondence between tests and the security enforcing functions defined in the security target. It shall describe the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design. It shall describe the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings. Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced. ITSEC E4.12

6.28 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Construction - The Development Environment

Aspect 1 - Configuration Control

Requirements for Content and Presentation

evelopment process shall be supported by a **tool based** configuration control system and an acceptance procedure. The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals and the source code or hardware drawings shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes **by authorised persons** are possible. **The configuration control tools shall be able to control and audit changes between different versions of objects subject to configuration control.** ITSEC E4.15

*The development process shall be supported by a **tool based** configuration control system and an acceptance procedure.*

6.29 An automated configuration control system is required for E4 and higher assurance levels. Several tools may be necessary depending upon the nature of the TOE and the number of development organisations involved.

6.30 Note that the acceptance procedure does not require a tool based system.

*The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes **by authorised persons** are possible.*

6.31 The procedures must not only indicate the process by which authorised changes can be made, but also who (e.g. the roles) has the necessary authorisation.

The configuration control tools shall be able to control and audit changes between different versions of objects subject to configuration control.

6.32 The tool(s) must be able to satisfy these ITSEC criteria.

Requirements for Evidence

nformation on the configuration control system shall describe how it is used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures. ITSEC E4.16

6.33 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

rogramming languages used for implementation shall be well-defined, e.g. as in an ISO standard. Any implementation dependent options of the programming language shall be documented. **For all compilers used, the implementation options selected shall be documented.** ITSEC E4.18

For all compilers used, the implementation options selected shall be documented.

6.34 This requirement applies to both software and firmware compilers.

Requirements for Evidence

The definition of the programming languages shall define unambiguously the meaning of all statements used in the source code. ITSEC E4.19

6.35 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 3 - Developer's Security

Requirements for Content and Presentation

ocument on the security of the development environment shall describe the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be described. ITSEC E4.21

6.36 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

nformation on the security of the development environment shall describe how the integrity of the TOE and the confidentiality of the associated documentation are maintained. ITSEC E4.22

6.37 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

ser documentation shall describe the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E4.25

6.38 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

ser documentation shall describe how an end-user uses the TOE in a secure manner. ITSEC E4.26

6.39 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

dministration documentation shall describe the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall describe all security parameters which are under his control. It shall describe each type of security-relevant event, relevant to the administrative functions. It shall describe details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall describe instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E4.28

6.40 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

dministration documentation shall describe how the TOE is administered in a secure manner. ITSEC E4.29

6.41 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

ferent configurations are possible, the impact of the configurations on security shall be described. The procedures for delivery and system generation shall be described. A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated. ITSEC E4.32

6.42 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

nformation supplied shall describe how the procedures maintain security. ITSEC E4.33

6.43 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be described. If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be described. **Procedures shall exist which can restore the TOE to a secure state after a failure, or a hardware or software error.** If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment. ITSEC E4.35

Procedures shall exist which can restore the TOE to a secure state after a failure, or a hardware or software error.

6.44 Procedures for restoring a TOE to a secure state after a failure, or a hardware or software error must be produced. A secure state should be defined by the security target, but can be summarised as maintaining any confidentiality, integrity and availability requirements placed on the TOE.

Requirements for Evidence

ıformation supplied shall describe how the procedures maintain security. The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during startup and operation. ITSEC E4.36

6.45 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Chapter 7 Level E5

Overview of E5 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE
- Definition of, or reference to, an underlying formally specified model of security
- Informal interpretation of the underlying model in terms of the security target

Architecture:

- Semiformal description of the architecture of the TOE

Detailed Design:

- Semiformal description of the detailed design

Implementation:

- Test documentation
- Library of test programs and tools used for testing the TOE
- Source code or hardware drawings for all security enforcing and security relevant components
- Informal description of correspondence between source code or hardware drawings and the detailed design

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- Audit information on modification of all objects of the TOE subject to configuration control
- Information on the acceptance procedure
- **Information on the integration procedure**

Programming Languages and Compilers:

- Description of all implementation languages used
- Description of all compilers used
- **Source code of all runtime libraries used**

Developer’s Security:

- Information on the security of the development environment

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall **explain** the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. A formal model of security policy shall be provided or referenced to define the underlying security policy to be enforced by the TOE. An informal interpretation of this model in terms of the security target shall be provided. The security enforcing functions within the security target shall be specified using both an informal and semiformal style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E5.2

7.1 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

The security target shall ***explain*** *the security enforcing functions to be provided by the TOE.*

7.2 Explanations in informal text must be provided as to how the SEFs are to be provided for the particular TOE.

Requirements for Evidence

case of a system the security target shall **explain** how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall **explain** how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. The informal interpretation of the formal security policy model shall **explain** how the security target satisfies the underlying security policy. ITSEC E5.3

7.3 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Content and Presentation

iformal notation shall be used in the architectural design to produce a semiformal description. It shall **explain** the general structure of the TOE. It shall **explain** the external interfaces of the TOE. It shall **explain** any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. It shall **explain** the separation of the TOE into security enforcing and other components. **It shall explain the interrelationships between the security enforcing components.** ITSEC E5.5

7.4 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

*It shall **explain** the separation of the TOE into security enforcing and other components.*

7.5 Formal or semi-formal modelling, or animation of an architectural design can provide an objective means of demonstrating and justifying the consistency and completeness of design, and the separation of security enforcing and other components. Where such modelling or animation is undertaken and is used to justify the separation, the evaluators should be given access to the model or animation and the results obtained.

It shall explain the interrelationships between the security enforcing components.

7.6 An explanation must provide a description and rationale for any interrelationships between security enforcing components.

7.7 Formal or semi-formal modelling, or animation of an architectural design can provide an objective means of demonstrating and justifying the separation of security enforcing components. Where such modelling or animation is undertaken and is used to justify the separation, the evaluators should be given access to the model or animation and the results obtained.

Requirements for Evidence

escription of the architecture shall **explain** how the security enforcing functions of the security target will be provided. It shall **explain** how the separation into security enforcing and other components is achieved. It shall **explain** how the chosen structure provides for largely independent security enforcing components. **It shall explain why the interrelationships between the security enforcing components are necessary.** ITSEC E5.6

7.8 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

It shall explain why the interrelationships between the security enforcing components are necessary.

7.9 It is possible to cover this criterion within the content and presentation requirement: *It shall explain the interrelationships between the security enforcing components*, however, the explanation must cover the necessity for the interrelationships, showing that the components could not operate correctly without those interfaces, with evidence that can be used to contribute to the binding analysis to show that no vulnerabilities are introduced through these interrelationships.

Requirements for Content and Presentation

iformal notation shall be used to develop a semiformal detailed design. The detailed design shall specify all basic components. It shall **explain**, through all levels of the design hierarchy, the realisation of all security enforcing and security relevant functions. It shall **explain** the separation of the TOE into security enforcing, security relevant and other components. It shall be structured into well-defined, largely independent basic components that facilitate testing and minimise the potential for violations of security. **It shall incorporate significant use of layering, abstraction and data hiding.** It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and **functional units. Unnecessary functionality shall be excluded from security enforcing and security relevant components**. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters **and effects. The purpose of all variables used by more than one functional unit shall be explained**. Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels. ITSEC E5.8

7.10 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

It shall incorporate significant use of layering, abstraction and data hiding.

7.11 The objective of these techniques, as described in the glossary included in Part I of this Guide, is to isolate those aspects which are of primary importance at each layer of a system, providing a set of subsystems which each know about the layers below them but not about the layers above. These techniques are intended to aid understanding and maintenance of the design, to minimise the impact of change, and to improve portability. Guidance on the application of these techniques can be found in various software engineering texts.

It shall map security enforcing functions to mechanisms and ***functional units****.*

7.12 Functional units are procedures or functions in the source code. This requirement requires the SEFs to be correlated to a greater degree of detail within the design than at lower assurance levels.

Unnecessary functionality shall be excluded from security enforcing and security relevant components.

7.13 At this level of assurance, further confidence in the correctness of the design is gained by the exclusion of unnecessary functionality from the components addressing the security of the TOE. This requirement is solely on the developer; however, the further requirement referred to by paragraph 0 requires the developer to justify the reason for retaining the remaining functionality.

All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters ***and effects****.*

7.14 This additional condition requires the effects of security enforcing and security relevant components to be stated to the same degree of detail expressed in the detailed design.

The purpose of all variables used by more than one functional unit shall be explained.

7.15 The use of 'common' or 'global' variables (e.g. queues, lists, pools) by more than one functional unit must be justified and consistent with the definitions of the common variables. Common variables must only be defined once.

Requirements for Evidence

letailed design shall **explain** how the security mechanisms provide the security enforcing functions specified in the security target. **It shall explain why the remaining functionality cannot be excluded from the security enforcing and security relevant components.** It shall **explain** why components for which no design information is provided cannot be either security enforcing or security relevant. ITSEC E5.9

7.16 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

It shall explain why the remaining functionality cannot be excluded from the security enforcing and security relevant components.

7.17 The reason for retaining the remaining functionality must be justified.

Requirements for Content and Presentation

source code and hardware drawings shall be completely structured into small, comprehensible, separate sections. The description of correspondence shall **explain** the correspondence between source code or hardware drawings and **functional units** of the detailed design. The test documentation shall contain plan, purpose, procedures and results of the tests and a justification why the extent of test coverage is sufficient. The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated. ITSEC E5.11

7.18 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

The source code and hardware drawings shall be completely structured into small, comprehensible, separate sections.

7.19 In this context a section should be considered to be a compilation unit (e.g. a logically distinct, single unit of source code to be input to a compiler) or a hardware drawing (e.g. a drawing on a single sheet of paper in a human-readable form). Note that further documentation will be necessary if the structure of the detailed design in terms of basic components and functional units does not show how the functional units are packaged into separate sections.

7.20 The following guidelines should be followed:

a) the contents of each section should be clearly identified and described (e.g. by means of a text header at the start of a compilation unit)

b) interfaces between sections should be clearly defined

c) each section should contain only one type of functionality (i.e. security enforcing or security relevant functionality should not be mixed with functionality that is irrelevant to security).

*The description of correspondence shall **explain** the correspondence between source code or hardware drawings and **functional units** of the detailed design.*

7.21 This requirement is extended at this assurance level to include functional units (procedures or functions in the source code).

Requirements for Evidence

ɜst documentation shall **explain** the correspondence between tests and the security enforcing functions defined in the security target. It shall **explain** the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design. It shall **explain** the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings. Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced. ITSEC E5.12

7.22 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Construction - The Development Environment

Aspect 1 - Configuration Control

Requirements for Content and Presentation

evelopment process shall be supported by a tool based configuration control system and an acceptance procedure. **The configuration control tools shall ensure that the person responsible for acceptance of an object into configuration control was not one of its designers or developers.** The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals and the source code or hardware drawings shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes by authorised persons are possible. **All objects created during the development process which pass through the acceptance procedure shall be subject to configuration control. All security enforcing and security relevant objects under configuration control shall be identified as such.** The configuration control tools shall be able to control and audit changes between different versions of objects subject to configuration control. **All modifications of these objects shall be audited with originator, date and time. The configuration control tools shall be able to support the creation and handling of variable relationships between objects under configuration control. In the event of a change to any of these objects, the tools shall be able to identify all other objects under configuration control affected by this change together with an indication of whether they are security enforcing or security relevant objects.** ITSEC E5.15

The configuration control tools shall ensure that the person responsible for acceptance of an object into configuration control was not one of its designers or developers.

7.23 This requirement implicitly requires the tools to enforce identification and authentication and access control.

All objects created during the development process which pass through the acceptance procedure shall be subject to configuration control.

7.24 The quality procedures for the development must ensure that this requirement is addressed and an appropriate link is established between the acceptance and configuration control procedures.

All security enforcing and security relevant objects under configuration control shall be identified as such.

All modifications of these objects shall be audited with originator, date and time.

The configuration control tools shall be able to support the creation and handling of variable relationships between objects under configuration control.

In the event of a change to any of these objects, the tools shall be able to identify all other objects under configuration control affected by this change together with an indication of whether they are security enforcing or security relevant objects.

7.25 The tools chosen for configuration control must satisfy these criteria. It may be possible to meet the requirement by a set of tools used in combination to provide an effective configuration control system, the various tools and their uses being adequately documented.

Requirements for Evidence

ıformation on the configuration control system **and the integration procedure** shall **explain** how **they are** used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures. **The information on the configuration control system shall explain how the tools ensure that the person responsible for acceptance of an object was not one of its designers or developers. Example audit trail output from the configuration control system shall be provided.** ITSEC E5.16

7.26 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this

Guide.

The information on the configuration control system ***and the integration procedure*** *shall* ***explain*** *how* ***they are*** *used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures.*

7.27 This requirement is expanded to include the integration procedure. Integration covers the process of combining software elements, hardware elements or firmware elements, or combinations of these elements, into larger assemblies.

The information on the configuration control system shall explain how the tools ensure that the person responsible for acceptance of an object was not one of its designers or developers.

7.28 The evidence must both describe and justify how the tools enforce adequate identification and authentication and access control to provide the separation of roles. Supporting operating procedures defining the administration of the separation of roles may need to be provided.

Example audit trail output from the configuration control system shall be provided.

7.29 The audit trail output must be representative of normal working configuration control practices, demonstrate the separation of roles, and the acceptance of new or modified objects.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

programming languages used for implementation shall be well-defined, e.g. as in an ISO standard. Any implementation dependent options of the programming language shall be documented. For all compilers used, the implementation options selected shall be documented. **The source code of any runtime libraries shall be provided.** ITSEC E5.18

The source code of any runtime libraries shall be provided.

7.30 This requirement applies to software and firmware run time supporting libraries used to develop the TOE. Note should be taken of this requirement prior to selecting compilers and associated libraries for developing the TOE.

7.31 If the source code is commercially confidential, the owners of the code may wish to enter into a confidentiality agreement with the evaluation team and supply the code directly to the team.

Requirements for Evidence

lefinition of the programming languages shall define unambiguously the meaning of all statements used in the source code. ITSEC E5.19

7.32 The requirements for evidence at this assurance level are unchanged since level E3. Refer to level E3 for guidance.

Aspect 3 - Developer's Security

Requirements for Content and Presentation

ocument on the security of the development environment shall **explain** the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be **explained.** ITSEC E5.21

7.33 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Evidence

ıformation on the security of the development environment shall **explain** how the integrity of the TOE and the confidentiality of the associated documentation are maintained. ITSEC E5.22

7.34 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

ser documentation shall **explain** the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E5.25

7.35 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Evidence

ıser documentation shall **explain** how an end-user uses the TOE in a secure manner. ITSEC E5.26

7.36 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

7.37 At E5 and E6, the user guides might, in addition to the description provided at E3 or E4, explain that (refer to the example in paragraph 0):

a) The user may need to change the access permissions for a file which he owns, because:

- there may be changes in personnel or in the requirements for other users to see the file
- the requirements for access permissions on a newly created file may differ from those already allocated by default.

b) The manner of specification of the filename parameter is consistent with the manner of specification of filenames in other commands.

c) The manner of specification of the access permissions is consistent with the listing provided by the *ls* command.

d) The results of the *chmod* command can optionally be echoed to the screen in the same format as that provided by the *ls* command. The option of a screen echo is provided in order to draw the user's attention to the effects of using the *chmod* command, so that the user can detect any unintended or insecure consequences of using the *chmod* command. For this reason, the echo option is selected by default, unless explicitly switched off. The *ls* command may also be used to check the access permissions for a file.

e) Use of the chmod command is an auditable event, in order to provide individual accountability for security relevant actions (such as changing file access permissions).

f) It is recommended that the echo option is not switched off, in order to ensure that unexpected results of the *chmod* command are immediately detectable by the user.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

dministration documentation shall **explain** the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall **explain** all security parameters which are under his control. It shall **explain** each type of security-relevant event, relevant to the administrative functions. It shall **explain** details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall **explain** instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E5.28

7.38 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Evidence

dministration documentation shall **explain** how the TOE is administered in a secure manner. ITSEC E5.29

7.39 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

ferent configurations are possible, the impact of the configurations on security shall be **explained.** The procedures for delivery and system generation shall be **explained.** A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated. ITSEC E5.32

7.40 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Evidence

formation supplied shall **explain** how the procedures maintain security. ITSEC E5.33

7.41 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be **explained.** If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be **explained.** Procedures shall exist which can restore the TOE to a secure state after a failure, or a hardware or software error. If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment. ITSEC E5.35

7.42 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Requirements for Evidence

ıformation supplied shall **explain** how the procedures maintain security. The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during startup and operation. ITSEC E5.36

7.43 It should be noted that the degree of rigour required is **explain** as detailed in Part III of this Guide.

Chapter 8 Level E6

Overview of E6 Evaluation Correctness Deliverables

Requirements:

- The security target for the TOE
- Definition of, or reference to, an underlying formally specified model of security
- Informal interpretation of the underlying model in terms of the security target

Architecture:

- **Formal** description of the architecture of the TOE

Detailed Design:

- Semiformal description of the detailed design

Implementation:

- Test documentation
- Library of test programs and tools used for testing the TOE**, including tools which can be used to detect inconsistencies between source code and executable code if there are any security enforcing or security relevant source code components (e.g. a disassembler and/or a debugger)**
- Source code or hardware drawings for all security enforcing and security relevant components
- Informal description of correspondence between source code or hardware drawings and the detailed design **and the formal specification of security enforcing functions**

Configuration Control:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- Audit information on modification of all objects of the TOE subject to configuration control
- Information on the acceptance procedure
- Information on the integration procedure

Programming Languages and Compilers:

- Description of all implementation languages used
- Description of all compilers used
- Source code of all runtime libraries used

Developer's Security:

- Information on the security of the development environment

Operation:

- User documentation
- Administration documentation
- Delivery and configuration documentation
- Startup and operation documentation

Construction - The Development Process

Phase 1 - Requirements

Requirements for Content and Presentation

ecurity target shall explain the security enforcing functions to be provided by the TOE. In the case of a system, in addition the security target shall include a System Security Policy (SSP) identifying the security objectives and the threats to the system. In the case of a product, in addition the security target shall include a rationale, identifying the method of use for the product, the intended environment and the assumed threats within that environment. A formal model of security policy shall be provided or referenced to define the underlying security policy to be enforced by the TOE. An informal interpretation of this model in terms of the security target shall be provided. The security enforcing functions within the security target shall be specified using both an informal and **formal** style as categorised in Chapter 2 (of the ITSEC [Reference 0]). ITSEC E6.2

The security enforcing functions within the security target shall be specified using both an informal and ***formal*** *style as categorised in Chapter 2 (of the ITSEC [Reference 0]).*

8.1 Part III of this Guide provides information on suitable formal specifications and notations.

8.2 A formal notation must be used to specify the SEFs for the TOE. The informal text explanation of the SEFs must be consistent with the formal specification for each SEF. The informal text should not add any extra functionality which is not defined in the formal specification, but it should provide an explanation in natural language.

8.3 Note that it may be possible to use the formal specification of the SEFs together with the definition of the notations used, including all axioms, as the formal Security Policy Model; this would reduce evaluation effort in checking consistency between definitions.

8.4 Where a functionality class is claimed, both the informal description and the formal description must be traceable to the statements in the functionality class.

Requirements for Evidence

case of a system the security target shall explain how the proposed functionality fulfils the security objectives and is adequate to counter the identified threats. In the case of a product the security target shall explain how the functionality is appropriate for that method of use and is adequate to counter the assumed threats. The informal interpretation of the formal security policy model shall explain how the security target satisfies the underlying security policy. ITSEC E6.3

8.5 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Phase 2 - Architectural Design

Requirements for Content and Presentation

mal notation shall be used in the architectural design to produce a **formal** description. It shall explain the general structure of the TOE. It shall explain the external interfaces of the TOE. It shall explain any hardware and firmware required by the TOE with a statement of the functionality of supporting protection mechanisms implemented in that hardware or firmware. It shall explain the separation of the TOE into security enforcing and other components. It shall explain the interrelationships between the security enforcing components. ITSEC E6.5

*A **formal** notation shall be used in the architectural design to produce a **formal** description.*

8.6 Part III of this Guide provides information on suitable formal specifications and notations.

8.7 The language used for expressing the architectural design must be capable of expressing features relevant to security. A single notation may not be capable of expressing every facet of a TOE's architecture. In this case, the developer could make use of several notations which, in combination, will provide a complete picture of the architecture.

8.8 Formal notations should be capable of illustrating the general structure of the TOE, its decomposition into major components, and how these components interact to provide the SEFs in the security target. It should be possible to show the separation of the TOE into security enforcing and other components.

8.9 Note that structured design methods would not be considered a formal notation, but could be used to supplement the formal notation as part of the architectural design.

8.10 An informal description, in addition to the formal description, is not required by the ITSEC for the overall architectural description. It is likely that the exactness of a formal description will preclude the need for an informal description. If an informal description is included to support the formal one, its purpose should be to explain it and make it easier to understand, and not to augment it. The following rule should be followed:

Where a formal description includes a formal part and informal prose, the informal prose should not enumerate security relevant facts which are not covered by the formal part.

8.11 While an informal description is not needed, note that the Z notation requires there to be an accompanying English text in addition to the formal description.

Requirements for Evidence

escription of the architecture shall explain how the security enforcing functions of the security target will be provided. It shall explain how the separation into security enforcing and other components is achieved. It shall explain how the chosen structure provides for largely independent security enforcing components. It shall explain why the interrelationships between the security enforcing components are necessary. **It shall explain, using a combination of formal and informal techniques, how it is consistent with the formal security policy model of the underlying security policy.** ITSEC E6.6

It shall explain, using a combination of formal and informal techniques, how it is consistent with the formal security policy model of the underlying security policy.

8.12 The ITSEC requires consistency between the architectural design and the formal model of the underlying security policy model to be provided using a combination of formal and informal techniques.

8.13 Evidence must be provided by means of formal proof that the formal description of the security enforcing components in the architectural design satisfies the relevant SEF properties in the formal security policy model.

8.14 The informal text should not add any extra evidence which is not defined in the formal proof, but it should provide a description of the formal proof in natural language.

8.15 If the formal description and the formal security policy model are in different formal languages, the developer should provide a translation, or equivalent, between the two languages.

Phase 3 - Detailed Design

Requirements for Content and Presentation

iformal notation shall be used to develop a semiformal detailed design. The detailed design shall specify all basic components. It shall explain, through all levels of the design hierarchy, the realisation of all security enforcing and security relevant functions. It shall explain the separation of the TOE into security enforcing, security relevant and other components. It shall be structured into well-defined, largely independent basic components that facilitate testing and minimise the potential for violations of security. It shall incorporate significant use of layering, abstraction and data hiding. It shall identify all security mechanisms. It shall map security enforcing functions to mechanisms and functional units. Unnecessary functionality shall be excluded from security enforcing and security relevant components. All interfaces of security enforcing and security relevant components shall be documented stating their purpose and parameters and effects. The purpose of all variables used by more than one functional unit shall be explained. Specifications/definitions for mechanisms shall be provided. These specifications shall be suitable for the analysis of interrelationships between the mechanisms employed. Specifications need not be provided for components that are neither security enforcing nor security relevant. Where more than one level of specification is provided, there shall be a clear and hierarchical relationship between levels. ITSEC E6.8

8.16 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

The detailed design shall explain how the security mechanisms provide the security enforcing functions specified in the security target. It shall explain why the remaining functionality cannot be excluded from the security enforcing and security relevant components. It shall explain why components for which no design information is provided cannot be either security enforcing or security relevant. ITSEC E6.9

8.17 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Content and Presentation

ource code and hardware drawings shall be completely structured into small, comprehensible, separate sections. The description of correspondence shall explain the correspondence between source code or hardware drawings and functional units of the detailed design. **It shall explain the correspondence between the security mechanisms as represented in the source code or hardware drawings and the formal specification of security enforcing functions in the security target.** The test documentation shall contain plan, purpose, procedures and results of the tests and a justification why the extent of test coverage is sufficient. The library of test programs shall contain test programs and tools to enable all tests covered by the test documentation to be repeated. ITSEC E6.11

It shall explain the correspondence between the security mechanisms as represented in the source code or hardware drawings and the formal specification of security enforcing functions in the security target.

8.18 An informal correlation is required. As the degree of rigour is 'explain', the correlation must not only provide a simple mapping, but must also provide justification of how the formal SEFs are realised in the security mechanisms.

8.19 Although only a one-way correspondence is mandated, it can be helpful to produce a two-way correspondence.

8.20 Note that it may be possible to satisfy the requirements for correspondence by means of the explained traceability from the security target through the architectural and detailed design documents to the source code.

Requirements for Evidence

:st documentation shall explain the correspondence between tests and the **formal specification of** security enforcing functions defined in the security target. It shall explain the correspondence between tests and the security enforcing and security relevant functions defined in the detailed design. It shall explain the correspondence between tests and the security mechanisms as represented in the source code or hardware drawings. Evidence of retests after the discovery and correction of errors relevant to security is obligatory to demonstrate that the errors have been eliminated and no new errors have been introduced.
ITSEC E6.12

The test documentation shall explain the correspondence between tests and the ***formal specification of*** *security enforcing functions defined in the security target.*

8.21 For E6 the correspondence must relate to the formal representation of the SEFs.

Construction - The Development Environment

Aspect 1 - Configuration Control

Requirements for Content and Presentation

evelopment process shall be supported by a tool based configuration control system and an acceptance procedure. The configuration control tools shall ensure that the person responsible for acceptance of an object into configuration control was not one of its designers or developers. The configuration list provided shall enumerate all basic components out of which the TOE is built. The TOE, its basic components and all documents provided including the manuals and the source code or hardware drawings shall possess a unique identifier. The use of this unique identifier is obligatory in references. The configuration control system shall ensure that the TOE under evaluation matches the documentation provided and that only authorised changes by authorised persons are possible. **All tools used in the development process shall be subject to configuration control.** All objects created during the development process which pass through the acceptance procedure shall be subject to configuration control. All security enforcing and security relevant objects under configuration control shall be identified as such. The configuration control tools shall be able to control and audit changes between different versions of objects subject to configuration control. All modifications of these objects shall be audited with originator, date and time. The configuration control tools shall be able to support the creation and handling of variable relationships between objects under configuration control. In the event of a change to any of these objects, the tools shall be able to identify all other objects under configuration control affected by this change together with an indication of whether they are security enforcing or security relevant objects. ITSEC E6.15

All tools used in the development process shall be subject to configuration control.

8.22 All tools used in the development process must be subject to automated configuration control. Modern IT development can encompass a wide range of tools which can include:

a) compilers/assemblers

b) Computer Aided Design (CAD) tools

c) Programmable Read Only Memory (PROM) blowers

d) 4GLs

e) test tools (analysers, simulators, test harness builders, etc.)

f) configuration tools.

Requirements for Evidence

ıformation on the configuration control system and the integration procedure shall explain how they are used in practice and applied in the manufacturing process in accordance with the developer's quality management procedures. The information on the configuration control system shall explain how the tools ensure that the person responsible for acceptance of an object was not one of its designers or developers. Example audit trail output from the configuration control system shall be provided. ITSEC E6.16

8.23 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

ırogramming languages used for implementation shall be well-defined, e.g. as in an ISO standard. Any implementation dependent options of the programming language shall be documented. For all compilers used, the implementation options selected shall be documented. The source code of any runtime libraries shall be provided. ITSEC E6.18

8.24 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

lefinition of the programming languages shall define unambiguously the meaning of all statements used in the source code. ITSEC E6.19

8.25 The requirements for evidence at this assurance level are unchanged since level E3. Refer to level E3 for guidance.

Aspect 3 - Developer's Security

Requirements for Content and Presentation

ocument on the security of the development environment shall explain the intended protection for the integrity of the TOE and the confidentiality of the associated documents. Physical, procedural, personnel and other security measures used by the developer shall be explained. ITSEC E6.21

8.26 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

nformation on the security of the development environment shall explain how the integrity of the TOE and the confidentiality of the associated documentation are maintained. ITSEC E6.22

8.27 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Operation - The Operational Documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

ser documentation shall explain the security enforcing functions relevant to the end-user. It shall also give guidelines covering their secure operation. The user documentation e.g. Reference Manuals, User Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E6.25

8.28 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

ıser documentation shall explain how an end-user uses the TOE in a secure manner. ITSEC E6.26

8.29 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

dministration documentation shall explain the security enforcing functions relevant to an administrator. It shall distinguish two types of functions: those which allow an administrator to control security parameters, and those which only allow him to obtain information. If an administrator is required, it shall explain all security parameters which are under his control. It shall explain each type of security-relevant event, relevant to the administrative functions. It shall explain details, sufficient for use, of procedures relevant to the administration of security. It shall give guidelines on the consistent and effective use of the security features of the TOE and how those features interact. It shall explain instructions on how the system/product shall be installed and how, if appropriate, it shall be configured. The administration documentation, e.g. Reference Manuals, Administrator Guides, shall be structured, internally consistent, and consistent with all other documents supplied for this level. ITSEC E6.28

8.30 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

dministration documentation shall explain how the TOE is administered in a secure manner. ITSEC E6.29

8.31 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Operation - The Operational Environment

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

erent configurations are possible, **they shall be defined in terms of the formal architectural design, and** the impact of the configurations on security shall be explained. The procedures for delivery and system generation shall be explained. A procedure approved by the national certification body for this evaluation level shall be followed, which guarantees the authenticity of the delivered TOE. While generating the TOE, any generation options and/or changes shall be audited in such a way that it is subsequently possible to reconstruct exactly how and when the TOE was generated. ITSEC E6.32

If different configurations are possible, ***they shall be defined in terms of the formal architectural design, and*** *the impact of the configurations on security shall be explained.*

8.32 If any different configurations (i.e. configuration parameters) are possible they must be formally defined and demonstrate consistency with the formal architectural design. One way to provide this would be to include the configurations within the formal architectural design and provide a cross-reference from the delivery documentation. The specification of the configuration options must accurately reflect the potential configurations of the TOE.

8.33 It is likely that this formal ITSEC requirement will not be included in the delivery documentation delivered to users, but provided separately to the evaluation team.

Requirements for Evidence

ıformation supplied shall explain how the procedures maintain security. ITSEC E6.33

8.34 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Aspect 2 - Startup and Operation

Requirements for Procedures and Standards

rocedures for secure startup and operation shall be explained. If any security enforcing functions can be deactivated or modified during startup, normal operation or maintenance, this shall be explained. Procedures shall exist which can restore the TOE to a secure state after a failure, or a hardware or software error. If the TOE contains hardware which contains security enforcing hardware components, then administrator, end-user, or self initiated diagnostic tests shall exist that can be performed on the TOE in its operational environment. ITSEC E6.35

8.35 The requirements for content and presentation at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Requirements for Evidence

nformation supplied shall explain how the procedures maintain security. The sponsor shall provide example results from all diagnostic test procedures for security enforcing hardware components. The sponsor shall provide examples of any audit trail output created during startup and operation. ITSEC E6.36

8.36 The requirements for evidence at this assurance level are unchanged from the previous level. Refer to the previous level for guidance.

Section 2 - Effectiveness Documentation

Chapter 9 Assurance - Effectiveness

Overview

9.1 The effectiveness criteria do not change by assurance level. However, Figure 4 of the ITSEC specifies that certain correctness documents are used as input for the preparation of the effectiveness documentation and, as the assurance level affects the degree of rigour of the correctness documents, hence the effectiveness documentation is influenced by the assurance level.

9.2 For assurance levels E1 to E6 the developer must provide the following deliverables:

a) Construction

- Suitability analysis
- Binding analysis
- Strength of mechanisms analysis
- Construction vulnerability analysis

b) Operation

- Ease of use analysis
- Operation vulnerability analysis.

9.3 The ITSEC mandates the information that is required but not how it is organised. It is not necessary to produce six separate effectiveness analyses; one analysis may be sufficient as long as sufficient traceability and cross-reference information is included to show clearly how the six effectiveness aspects are satisfied.

9.4 Some issues are difficult to relate to a single effectiveness aspect. For such issues, the assignment of the issue to an effectiveness aspect is less important than the completeness with which the issue is addressed.

9.5 Further information on the preparation and content of effectiveness documentation can be found in Part III of this Guide.

Effectiveness Criteria - Construction

Aspect 1 - Suitability of Functionality

Requirements for Content and Presentation

suitability analysis shall link security enforcing functions and mechanisms to the threats, enumerated in the security target, that they are designed to counter. ITSEC 3.14

The suitability analysis shall link security enforcing functions and mechanisms to the threats, enumerated in the security target, that they are designed to counter.

9.6 A simple correlation must be provided between the SEFs and any prescribed mechanisms, and the threats. This can be a reference to the correlation provided by the sponsor in the security target. Suitable correlation methods include textual cross-references and matrices.

Requirements for Evidence

uitability analysis shall show how the threats are countered by the security enforcing functions and mechanisms. It shall show that there are no threats that are not adequately countered by one or more of the stated security enforcing functions. The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. ITSEC 3.15

The suitability analysis shall show how the threats are countered by the security enforcing functions and mechanisms.

9.7 The behaviour of each SEF (and mechanism, if any are specified in the security target) must be specified in sufficient detail in the security target to allow the evaluation team to verify that it does indeed counter the threat. This requires each link between a SEF or mechanism and threat to be applicable and appropriate, and to be stated, described or explained as appropriate.

It shall show that there are no threats that are not adequately countered by one or more of the stated security enforcing functions.

9.8 The correlation between SEFs and threats must be complete, i.e. each threat must be addressed by one or more SEFs (and mechanisms, if any are specified in the security target).

The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.9 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis,* identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability (i.e. effectiveness) analysis. The extent of the information increases according to the assurance level. The figure is repeated in this Guide as Figure 7. Guidance on the application of this figure to the suitability analysis is given in Part III of this Guide.

Aspect 2 - Binding of Functionality

Requirements for Content and Presentation

inding analysis shall provide an analysis of all potential interrelationships between security enforcing functions and mechanisms. ITSEC 3.18

The binding analysis shall provide an analysis of all potential interrelationships between security enforcing functions and mechanisms.

9.10 The binding analysis must demonstrate that the SEFs work together in a way that is mutually supportive and that in working together they meet the security objectives.

9.11 The binding analysis should be performed during the development of the TOE, when the components and mechanisms which implement the security enforcing functions provided by the product will be specified. For E1 and E2 this involves consideration of the information provided in the architectural design. For higher levels, or where a high strength of mechanism is claimed, the detailed design information must also be considered. At E4 and above, the binding analysis should also consider additional information provided in the source code, while it may be necessary to consider implications from the object code for E6.

Requirements for Evidence

ɔinding analysis shall show that it is not possible to cause any security enforcing function or mechanism to conflict with or contradict the intent of other security enforcing functions or mechanisms. The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. ITSEC 3.19

The binding analysis shall show that it is not possible to cause any security enforcing function or mechanism to conflict with or contradict the intent of other security enforcing functions or mechanisms.

9.12 It is possible for SEFs to be implemented correctly when each is viewed as a stand alone piece of functionality but, when integrated, result in the compromise of one or more of the security objectives. The binding analysis must show that it is not possible to cause any SEF to conflict with, or contradict, the intent of any other SEF so as to compromise any security objective.

The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.13 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis,* identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability (i.e. effectiveness) analysis. The extent of the information increases according to the assurance level. The figure is repeated in this document as Figure 7.

9.14 The following table gives some idea of how the Figure 4 documentation could be used in the binding analysis:

Level	Documentation	Information of use to binding analysis
E1-6	security target	definition of security objectives, security functionality, SEFs and mechanisms
E1-6	architectural design	TOE structure and interfaces, dependencies on hardware/firmware/software protection mechanisms, design of SEFs and mechanisms, separation of components, and interactions between components
E3-6	detailed design	internal structure, design of SEFs and mechanisms and components, interactions between components and use of variables, functionality included in security enforcing and

		security relevant components
E4-6	source code and hardware drawings	implementation details
E6	object code	run time information
E1-6	operation documentation	configuration and use of security features, diagnostics and error handling

9.15 When the evaluators have checked all the aspects described above, they will perform a final check to ensure that the intention of the ITSEC has been met, investigating *the ability of the security enforcing functions and mechanisms of the TOE to work together in a way that is mutually supportive and provides and integrated and effective whole.* This summarises the purpose of the binding analysis, and sponsors and developers would do well to ensure that the supplied documentation does cover this aspect.

Aspect 3 - Strength of Mechanisms

Requirements for Content and Presentation

trength of mechanisms analysis shall list all security enforcing mechanisms that have been identified as critical within the TOE. It shall include or reference analyses of the underlying algorithms, principles and properties of those mechanisms. ITSEC 3.22

The strength of mechanisms analysis shall list all security enforcing mechanisms that have been identified as critical within the TOE.

9.16 The ITSEM [Reference 0], Annex 6.C gives guidance on strength of mechanisms. The annex introduces the concept of a Type A mechanism, i.e. a mechanism which can be defeated by the use of resources, collusion or expertise.

9.17 Critical mechanisms are those Type A security enforcing mechanisms within the TOE whose failure through direct attack would prevent the TOE from meeting one or more of its security objectives.

9.18 The ITSEM, Annex 6.C also discusses Type B mechanisms. These are mechanisms which, if correctly implemented, cannot be defeated by direct attack. A direct attack is defined as:

a violation of a mechanism's security objective by means of inputs to the mechanisms which are within its specification.

9.19 As Type B mechanisms have no weaknesses, they are not susceptible to direct attack. A strength claim for a Type B mechanism is therefore not appropriate. If all the mechanisms in the TOE are of Type B, the security target should state that a strength claim is not appropriate, with justification provided in the strength of mechanisms analysis.

It shall include or reference analyses of the underlying algorithms, principles and properties of those mechanisms.

9.20 The underlying algorithms, principles and properties of all critical mechanisms must be made available to the evaluation team.

9.21 If all the mechanisms in the TOE are non-critical (being either Type B or non-exploitable Type A), the strength of mechanisms analysis should justify this claim.

Requirements for Evidence

strength of mechanisms analysis shall show that all critical mechanisms satisfy the claimed minimum strength of mechanisms rating, as defined in paragraphs 3.6 to 3.8 [of the ITSEC]: in the case of cryptographic mechanisms, this shall take the form of a statement of confirmation from the appropriate national body. Other analyses shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. ITSEC 3.23

The strength of mechanisms analysis shall show that all critical mechanisms satisfy the claimed minimum strength of mechanisms rating, as defined in paragraphs 3.6 to 3.8 [of the ITSEC]: in the case of cryptographic mechanisms, this shall take the form of a statement of confirmation from the appropriate national body.

9.22 The three ratings defined in the ITSEC are: basic, medium and high. Each critical mechanism (i.e. Type A security enforcing mechanism) must be assessed by the sponsor or developer and given a rating for its *minimum* strength.

9.23 In the UK, the Communications-Electronics Security Group (CESG) is the appropriate national authority for cryptographic mechanisms. Contact with CESG may be established via the Certification Body at the address at the front of this document.

9.24 Cryptographic strength of mechanism ratings will be carried out where appropriate by CESG, who will only confirm that the cryptographic mechanism has a strength which is appropriate to the assurance level claimed for the TOE as a whole. This confirmation will be sufficient for the evaluation team.

Other analyses [for non-cryptographic mechanisms] shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.25 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis,* identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability (i.e. effectiveness) analysis. The extent of the information increases according to the assurance level. The figure is repeated in this document as Figure 7.

9.26 The following table gives some idea of how the Figure 4 documentation could be used in the strength of mechanisms analysis:

Level	**Documentation**	**Information of use to strength of mechanisms analysis**
E1-6	security target	definition of threats, security objectives, environment, method of use, security functionality, and mechanisms
E1-6	architectural design	TOE structure, design of mechanisms, and interactions between mechanisms
E3-6	detailed design	internal structure and whether any mechanisms can be misused, design of mechanisms, and interactions between mechanisms
E4-6	source code and hardware drawings	details of the implementation of mechanisms
E6	object code	run time information
E1-6	operation documentation	configuration and use of security features

9.27 If an E1 security target makes a strength of mechanisms claim, or if a critical mechanism is relied upon to maintain the security of the TOE, then the sponsor and developer must provide evidence to support the strength of mechanism assessment. Such evidence may require more documentation than the standard E1 correctness documentation set to be provided to the evaluation team; for instance, a description of the detailed design may be necessary. In this instance, the Certification Body should be contacted for more specific advice.

Aspect 4 - Construction Vulnerability Assessment

Requirements for Content and Presentation

ist of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in the construction of the TOE known to him. It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect. ITSEC 3.26

The list of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in the construction of the TOE known to him.

9.28 Construction vulnerabilities can arise as a consequence of some property of the TOE introduced during its construction. The ITSEM gives the following guidance on areas which should be considered in the construction vulnerability assessment:

a) changing the order in which components are invoked

b) executing an additional component

c) using interrupts or scheduling functions to disrupt sequencing

d) reading,writing or modifying internal data, either directly or indirectly

e) executing data not intended to be executed, or making such data executable

f) using a component in an unexpected context, or for an unexpected purpose

g) generating unexpected input for a component

h) activating error recovery

i) using implementation detail introduced in lower representations

j) disrupting concurrence

k) using interference between components which are not visible at a higher level of abstraction

l) invalidating assumptions and properties on which lower level components rely

m) using the delay between time of check and time of use.

9.29 The Certification Body maintains a database of public domain vulnerabilities. The sponsor or developer must request any relevant information from the database for their TOE by completing a Vulnerability Information Request Form which is available from the Certification Body at the address at the front of this document. The vulnerability information received must be incorporated in a vulnerability analysis. The issue of requesting information from the database will be covered during the Task Startup Meeting at the outset of the evaluation.

It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect.

9.30 Countermeasures to constructional vulnerabilities can include other SEFs, or procedural measures outside the TOE.

Requirements for Evidence

analysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:

the vulnerability is adequately covered by other, uncompromised, security mechanisms, or

it can be shown that the vulnerability is irrelevant to the security target, will not exist in practice, or can be countered adequately by documented technical, personnel, procedural or physical security measures outside the TOE. These external security measures shall have been defined within (or shall have been added to) the appropriate documentation.

nalysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. ITSEC 3.27

The analysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:

- ***the vulnerability is adequately covered by other, uncompromised, security mechanisms, or***

- ***it can be shown that the vulnerability is irrelevant to the security target, will not exist in practice, or can be countered adequately by documented technical, personnel, procedural or physical security measures outside the TOE. These external security measures shall have been defined within (or shall have been added to) the appropriate documentation.***

9.31 Construction vulnerabilities are vulnerabilities which arise as a consequence of some property of the TOE introduced during its construction (whereas operational vulnerabilities concern only non technical countermeasures).

9.32 The list of vulnerabilities in construction supplied by the sponsor or developer must identify all relevant vulnerabilities known to them, whether or not they are perceived as exploitable, or countered by a proposed, or already provided, measure. Details of any measures proposed or provided to counter the effects of a known construction vulnerability must be provided. For example, these vulnerabilities may be countered through other (mutually supportive) SEFs, or operational environment countermeasures.

9.33 The analysis must support its arguments by providing specific, detailed references to relevant areas within other deliverables.

9.34 The following list gives some examples of ways in which construction vulnerabilities may be exploited, and can be used as the basis for determining the potential impact on the TOE:

a) change the predefined sequence of invocation of components

b) execute an additional component

c) use interrupts or scheduling functions to disrupt sequencing

d) read, write or modify internal data directly or indirectly

e) execute data not intended to be executed or make it executable

f) use a component in an unexpected context, or for an unexpected purpose

g) generate unexpected input for a component

h) activate error recovery

i) use implementation detail introduced in lower representations

j) disrupt concurrence

k) use interference between components which are not visible at a higher level of abstraction

l) invalidate assumptions and properties on which lower-level components rely

m) use the delay between time of check and time of use.

The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.35 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis*, identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability analysis. The extent of the information increases according to the assurance level. The figure is repeated in this document as Figure 7.

9.36 The following table gives some idea of how the Figure 4 documentation could be used in the construction vulnerability analysis:

Level	Documentation	Information of use to construction vulnerability analysis
E1-6	security target	definition of security objectives, security functionality, SEFs and mechanisms
E1-6	architectural design	TOE structure and interfaces, interactions between components, supporting hardware/firmware/software, and design of SEFs and mechanisms
E3-6	detailed design	internal structure and interactions between components, and design of SEFs and mechanisms and components
E4-6	source code and hardware drawings	implementation details
E6	object code	run time information
E1-6	operation documentation	intended use of security features

Effectiveness Criteria - Operation

Aspect 1 - Ease of Use

Requirements for Content and Presentation

ase of use analysis shall identify possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation. ITSEC 3.31

The ease of use analysis shall identify possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.

9.37 This aspect of the ease of use analysis is likely to provide valuable information for inclusion within the user and administration documentation.

9.38 The ease of use analysis must:

a) identify all possible modes of operation of the TOE following a failure (e.g. the termination of a detached process due to a run time error)

b) identify all possible modes of operation of the TOE following an operational error (e.g. accidentally disabling auditing functions)

c) identify the consequences of a failure or operational error and the implications for maintaining secure operation

d) show that any operation which deactivates or disables a SEF is clearly documented and easily detectable

e) show that if it is possible to configure the TOE in a way that is insecure, this fact will be easily detectable and is well documented.

Requirements for Evidence

ease of use analysis shall show that any human or other error in operation that deactivates or disables security enforcing functions or mechanisms will be easily detectable. It shall show that if it is possible to configure or cause the TOE to be used in a way which is insecure (i.e. the security enforcing functions and mechanisms of the TOE do not satisfy the security target), when an end-user or administrator of the TOE would reasonably believe it to be secure, then this fact will also be detectable. The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. ITSEC 3.32

The ease of use analysis shall show that any human or other error in operation that deactivates or disables security enforcing functions or mechanisms will be easily detectable.

9.39 The objective of the ease of use analysis is to assess whether the TOE can be configured or used in a way which is insecure but which an administrator or end-user might reasonably believe to be secure.

It shall show that if it is possible to configure or cause the TOE to be used in a way which is

insecure (i.e. the security enforcing functions and mechanisms of the TOE do not satisfy the security target), when an end-user or administrator of the TOE would reasonably believe it to be secure, then this fact will also be detectable.

9.40 The TOE must be able to be configured and used in a secure manner, purely by using the user and administration documentation provided to end-users and administrators.

9.41 The 'configuration' of a TOE is the selection of one of the sets of possible combinations of features of that TOE. These features may be termed 'configurable options', and are typically exemplified by the privileges and protections for users, devices and files on the TOE.

9.42 While the ease of use analysis is confined to the operational environment, experience suggests that it should be addressed at all stages during development. The temptation to postpone the consideration of configuration until a TOE becomes operational should be avoided, as it can result in a well-developed TOE being rendered completely insecure by poor configuration.

The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.43 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis*, identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability (i.e. effectiveness) analysis. The extent of the information increases according to the assurance level. The figure is repeated in this document as Figure 7.

9.44 The following table gives some idea of how the Figure 4 documentation could be used in the ease of use analysis:

Level	Documentation	Information of use to ease of use analysis
E1-6	security target	definition of threats, security objectives, security functionality, SEFs and mechanisms
E1-6	architectural design	TOE structure and interfaces, supporting hardware/firmware/software, design of SEFs and mechanisms, and interactions between functions
E3-6	detailed design	internal structure and whether any mechanisms can be misused without realising, design of SEFs and mechanisms and components, and interactions between components
E4-6	source code and hardware drawings	implementation details
E6	object code	run time information
E1-6	operation	installation of TOE, configuration and use of security

	documentation	features including secure startup, handling of security events such as warnings and alarms, diagnostics and error handling

Aspect 2 - Operational Vulnerability Assessment

Requirements for Content and Presentation

ist of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in operation of the TOE known to him. It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect. ITSEC 3.35

The list of known vulnerabilities provided by the sponsor shall identify all vulnerabilities in operation of the TOE known to him.

9.45 Operational vulnerabilities are vulnerabilities which permit an attacker to take advantage of weaknesses in non technical countermeasures to violate the security objectives of the TOE. Examples can include weaknesses in the operating procedures or administrator's guides, such as lack of specific advice to administrators to ensure that no user accounts are without passwords.

It shall identify each known vulnerability, provide an analysis of its potential impact, and identify the measures proposed or provided to counter its effect.

9.46 Countermeasures to operational vulnerabilities can include other (mutually supportive) SEFs, or non technical procedural measures outside the TOE.

Requirements for Evidence

ınalysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:

the vulnerability is adequately covered by other, uncompromised, external security measures, or

It can be shown that the vulnerability is irrelevant to the security target or will not be exploitable in practice.

nalysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question. Any required external security measures shall have been defined within (or shall have been added to) the appropriate documentation. ITSEC 3.36

The analysis of the potential impact of each known vulnerability shall show that the vulnerability in question cannot be exploited in the intended environment for the TOE, because either:

- ***the vulnerability is adequately covered by other, uncompromised, external security measures, or***

- ***it can be shown that the vulnerability is irrelevant to the security target or will not be exploitable in practice.***

9.47 Operational vulnerabilities are vulnerabilities which permit an attacker to take advantage of weaknesses in non technical countermeasures to violate the security objectives of the TOE (whereas construction vulnerabilities are vulnerabilities which arise as a consequence of some property of the TOE introduced during its construction). For example, operational vulnerabilities could be weaknesses in operating procedures or administrator's guides.

9.48 The list of known vulnerabilities in operation supplied by the sponsor or developer must identify all relevant vulnerabilities known to them, whether or not they are perceived as exploitable, or countered by a proposed, or already provided, measure. Details of any measures proposed or provided to counter the effects of a known operational vulnerability must be provided. For example, these vulnerabilities may be countered through other (mutually supportive) SEFs, or non technical countermeasures.

9.49 The analysis must support its arguments by providing specific, detailed references to relevant areas within other deliverables.

9.50 Any possible interaction between operational and constructional vulnerabilities must be considered, as well as interactions between operational vulnerabilities.

The analysis shall be performed using, at minimum, all the information given in figure 4 [of the ITSEC] for the evaluation level in question.

9.51 Figure 4 of the ITSEC, *Information used in a Vulnerability Analysis*, identifies the minimum information that producers of effectiveness documentation must obtain from the correctness deliverables to perform a vulnerability (i.e. effectiveness) analysis. The extent of the information increases according to the assurance level. The figure is repeated in this document as Figure 7.

9.52 The following table gives some idea of how the Figure 4 documentation could be used in the operational vulnerability analysis:

Level	Documentation	Information of use to operational vulnerability analysis
E1-6	security target	definition of threats, security objectives, intended environment, method of use, SEFs and mechanisms
E1-6	architectural design	TOE interfaces, interactions between functions, supporting hardware/firmware/software, and design of SEFs and mechanisms
E3-6	detailed design	internal structure and interactions between components, design of SEFs and mechanisms and components
E4-6	source code and hardware drawings	implementation details
E6	object code	run time information
E1-6	operation documentation	installation of TOE, configuration and use of security features including secure startup, handling of security events such as warnings and alarms, diagnostics and error handling

Any required external security measures shall have been defined within (or shall have been added to) the appropriate documentation.

9.53 Any procedural measures outside the TOE, e.g. Security Operating Procedures, must be made available to the evaluation team.

Annex ADeliverables Checklists

Correctness Evaluation Deliverables (Part 1)						
Deliverable	Assurance Level					
	E1	E2	E3	E4	E5	E6
Requirements:						
1 The security target for the TOE	_	_	_	_	_	_
2 Definition of or reference to an underlying formally specified model of security				_	_	_
3 Informal interpretation of the underlying model in terms of the security target				_	_	_
Architecture:						
1 Informal description of the architecture of the TOE	_	_	_			
2 Semiformal description of the architecture of the TOE				_	_	
3 Formal description of the architecture of the TOE						_
Detailed Design:						
1 Informal description of the detailed design		_	_			
2 Semiformal description of the detailed design				_	_	_
Implementation:						
1 Test documentation	(_)	_	_	_	_	_
2 Library of test programs and tools used for testing the TOE	(_)	_	_	_	_	
3 Library of test programs and tools used for testing the TOE, including tools which can be used to detect inconsistencies between source code and executable code if there are any security enforcing or security relevant source code components (e.g. a disassembler and/or a debugger)						_
4 Source code or hardware drawings for all security enforcing and security relevant components			_	_	_	_
5 Informal description of correspondence between source code or hardware drawings and the detailed design			_	_	_	
6 Informal description of correspondence between source code or hardware drawings and the detailed design and the formal specification of security enforcing functions						_

Note: (_) - optional deliverables, _ - mandatory deliverables

Figure 1 Correctness Evaluation Deliverables (Part 1 of 2)

Correctness Evaluation Deliverables (Part 2)						
Deliverable	Assurance Level					
	E1	E2	E3	E4	E5	E6
Configuration Control:						
1 Configuration list identifying the version of the TOE for evaluation	_	_	_	_	_	_
2 Information on the configuration control system		_	_			
3 Information on the configuration control system and its tools				_	_	_
4 Audit information on modification of all parts of the TOE subject to configuration control				_		
5 Audit information on modification of all objects of the TOE subject to configuration control					_	_
6 Information on the acceptance procedure			_	_	_	_
7 Information on the integration procedure					_	_
Programming Languages and Compilers:						
1 Description of all implementation languages used			_	_	_	_
2 Description of all compilers used				_	_	_
3 Source code of all runtime libraries used					_	_
Developer's Security:						
1 Information on the security of the development environment		_	_	_	_	_
Operation:						
1 User documentation	_	_	_	_	_	_
2 Administration documentation	_	_	_	_	_	_
3 Delivery and configuration documentation	_	_	_	_	_	_
4 Startup and operation documentation	_	_	_	_	_	_

Note: _ - mandatory deliverables

Figure 1 Correctness Evaluation Deliverables (Part 2 of 2)

Effectiveness Evaluation Deliverables	
Deliverable	**All Assurance Levels**
Suitability Analysis: an investigation showing that the security enforcing functions and mechanisms of the TOE will in fact counter the threats to the security of the TOE identified in the security target	–
Binding Analysis: an investigation showing that the security enforcing functions and mechanisms of the TOE bind together in a way that is mutually supportive and that provides an integrated and effective whole	–
Strength of Mechanisms Analysis: an investigation showing the ability of the TOE as a whole to withstand direct attacks based on deficiencies in its underlying algorithms, principles or properties; this assessment will require consideration of the level of resources that would be needed for an attacker to execute a successful attack	–
Construction Vulnerability Analysis: a list of potential vulnerabilities in the construction of the TOE (identified by the developer) plus an argument for why they are not exploitable	–
Ease of Use Analysis: an investigation showing that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure	–
Operational Vulnerability Analysis: a list of potential vulnerabilities in the operation of the TOE (identified by the developer) plus an argument for why they are not exploitable	–

Figure 3 Effectiveness Evaluation Deliverables

Development Environment Discussion Topics		
Subject	**Scope**	**Topics**
Development Configuration Control	The procedures (manual and automated) for the control and traceability of project material, including design, implementation and user documentation	Computer organisation - directory structures - software library and access control Change control Release Procedures Configuration Management of TOE components
Programming Languages and Compilers	The programming languages used for implementation	Definition of languages Implementation options Compilers
Development Security	Security of the development environment, i.e. protection of the TOE and confidentiality of associated documents	Physical measures Procedural measures Personnel measures IT measures
Development Methods	The different phases of the development and the approach adopted	Project history and current status Representations produced Design process Coding phase Test strategy
Development Tools	The tools (proprietary and purpose-built) used during development	Development computers, system management Compilers/linkers/debuggers System generation procedures Test harnesses
Development Procedures	The controls applied during development	Project management procedures Quality assurance procedures Technical assurance procedures
Development Standards	The standards used during the development	Design standards Coding standards Documentation standards

Figure 5 Development Environment Discussion Topics

Information Used In A Vulnerability Analysis						
INFORMATION	Level of Rigour					
	State		Describe		Explain	
	E1	E2	E3	E4	E5	E6
SECURITY TARGET (threats, objectives, functions, mechanisms, evaluation level, strength of mechanisms)	–	–	–	–	–	–
FORMAL MODEL OF SECURITY POLICY				–	–	–
FUNCTIONS (informal)	–	–	–	–	–	–
FUNCTIONS (semiformal)				–	–	
FUNCTIONS (formal)						–
ARCHITECTURAL DESIGN (informal)	–	–	–			
ARCHITECTURAL DESIGN (semiformal)				–	–	
ARCHITECTURAL DESIGN (formal)						–
DETAILED DESIGN (informal)			–			
DETAILED DESIGN (semiformal)				–	–	–
IMPLEMENTATION (hardware drawings and source code)				–	–	–
IMPLEMENTATION (object code)						–
OPERATION (user/administrator documents, delivery and configuration, startup and operation)	–	–	–	–	–	–

Figure 7 Information Used In A Vulnerability Analysis

INDEX