CONTENTS

FIGURES

0 INTRODUCTION

0.1 In the course of only four decades, Information Technology (IT) has come to play an important, and often vital, role in almost all sectors of organised societies. As a consequence, security has become an essential aspect of Information Technology.

0.2 In this context, IT security means,

- confidentiality - prevention of the unauthorised disclosure of information;

- integrity - prevention of the unauthorised modification of information;

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

0.3 An IT system or product will have its own requirements for maintenance of confidentiality, integrity and availability. In order to meet these requirements it will implement a number of technical security measures, in this document referred to as security enforcing functions, covering, for example, areas such as access control, auditing, and error recovery. Appropriate confidence in these functions will be needed: in this document this is referred to as assurance, whether it is confidence in the correctness of the security enforcing functions (both from the development and the operational points of view) or confidence in the effectiveness of those functions.

0.4 Users of systems need confidence in the security of the system they are using. They also need a yardstick to compare the security capabilities of IT products they are thinking of purchasing. Although users could rely upon the word of the manufacturers or vendors of the systems and products in question, or they could test them themselves, it is likely that many users will prefer to rely on the results of some form of impartial assessment by an independent body. Such an evaluation of a system or product requires objective and well-defined security evaluation criteria and the existence of a certification body that can confirm that the evaluation has been properly conducted. System security targets will be specific to the particular needs of the users of the system in question, whereas product security targets will be more general so that products that meet them can be incorporated into many systems with

similar but not necessarily identical security requirements.

0.5 For a system, an evaluation of its security capabilities can be viewed as a part of a more formal procedure for accepting an IT system for use within a particular environment. Accreditation is the term often used to describe this procedure. It requires a number of factors to be considered before a system can be viewed as fit for its intended purpose: it requires assurance in the security provided by the system, a confirmation of management responsibilities for security, compliance with relevant technical and legal/regulatory requirements, and confidence in the adequacy of other non-technical security measures provided in the system environment. The criteria contained in this document are primarily concerned with technical security measures, but they do address some non-technical aspects, such as secure operating procedures for personnel, physical and procedural security (but only where these impinge on the technical security measures).

0.6 Much work has been done previously on the development of IT security evaluation criteria, although for slightly different objectives according to the specific requirements of the countries or bodies involved. Most important of these, and a precursor to other developments in many respects, was the Trusted Computer System Evaluation Criteria [TCSEC], commonly known as the TCSEC or "Orange Book", published and used for product evaluation by the US Department of Defense. Other countries, mostly European, also have significant experience in IT security evaluation and have developed their own IT security criteria. In the UK this includes CESG Memorandum Number 3 [CESG3], developed for government use, and proposals of the Department of Trade and Industry, the "Green Book" [DTIEC], for commercial IT security products. In Germany, the German Information Security Agency published a first version of its own criteria in 1989 [ZSIEC], and at the same time criteria were being developed in France, the so-called "Blue-White-Red Book" [SCSSI].

0.7 Seeing that work was going on in this area, and much still needed to be done, France, Germany, the Netherlands and the United Kingdom recognised that this work needed to be approached in a concerted way, and that common, harmonised IT security criteria should be put forward. There were three reasons for harmonisation:

a) much experience had been accumulated in the various countries, and there would be much to gain by jointly building on that experience;

b) industry did not want different security criteria in the different countries;

c) the basic concepts and approaches were the same, across countries and even across commercial, government and defence applications.

0.8 It was therefore decided to build on the various national initiatives, taking the best features of what had already been done and putting them in a consistent, structured perspective. Maximum applicability and compatibility with existing work, most notably the US TCSEC, was a constant consideration in this process. Though it was initially felt that the work would be limited to harmonisation of existing criteria, it has sometimes been necessary to extend what already existed.

0.9 One reason for producing these internationally harmonised criteria is to provide a compatible basis for **certification** by the national certification bodies within the four co-operating countries, with an eventual objective of permitting international mutual recognition of evaluation results.

0.10 This document sets out the harmonised criteria. Chapter 1 contains a short presentation of the scope of the harmonised criteria. Chapter 2 deals with security functionality, that is the definition and description of security requirements. Chapter 3 defines criteria for evaluating assurance in the effectiveness of a **Target of Evaluation** as a solution to those requirements. Chapter 4 extends this to consideration of the correctness of the solution. Chapter 5 describes the permitted results of an evaluation, and Chapter 6 contains a glossary of those terms that take a more precise or different meaning in the book than in normal English (on first use they are printed in bold: whereas italics are used for emphasis). The glossary is intended to help the reader not only with the definition of words, but also with ideas and concepts that are special to the harmonised criteria.

0.11 The evaluation criteria in Chapters 3 and 4 are set out in a standardised way, which specifies what must be provided by the **sponsor** of the evaluation (the person or organisation requesting evaluation) and what must be done by the **evaluator** (the independent person or organisation performing evaluation). This categorisation is intended to assist in ensuring the consistency and uniformity of evaluation results. For each area of evaluation, documentation that must be provided by the sponsor of the evaluation is identified. This is then followed by the

criteria for each relevant aspect or phase of evaluation of that area. These criteria are broken down into **requirements for content and presentation** of the relevant documentation that must be provided by the sponsor, **requirements for evidence** concerning what that documentation must show, and the **evaluator actions** required to be performed by the evaluator both to check the documentation provided and where necessary to perform additional tests or other activities. In the case of criteria concerning how the system or product is to be used operationally, the sponsor will not, in general, be able to provide evidence from actual use. Thus the evaluator must assume for the purposes of evaluation that the procedures specified by the sponsor will be followed in practice.

0.12 Within the criteria certain verbs are also used in a special way. *Shall* is used to express criteria which must be satisfied; may is used to express criteria which are not mandatory; and *will* is used to express actions to take place in the future. Similarly, the verbs *state, describe and explain* are used within criteria to require the provision of evidence of increasing levels of rigour. *State* means that relevant facts must be provided; describe means that the facts must be provided and their relevant characteristics enumerated; explain means that the facts must be provided, their relevant characteristics enumerated and justifications given.

0.13 Other than within Chapter 4, paragraphs are numbered sequentially within each chapter. In Chapter 4, criteria are set out separately for each evaluation level. The introductory paragraphs of that chapter are numbered as in other chapters, but then the criteria paragraphs are numbered sequentially for each level, with the same paragraph number covering the same topic at each level. However, each paragraph within the document is uniquely identified by the combination of chapter or level number and paragraph number.

0.14 This work draws from documents that have already been extensively discussed and used in practice; moreover, it is felt that the ideas and concepts have been carefully balanced and that the structure chosen for the ITSEC is the right one for maximum consistency and ease of use. The current version of the ITSEC benefits from significant revisions arising from widespread international review. The review process has been assisted by the Commission for the European Communities who organised an international conference at which version 1.0 was discussed, and a subsequent workshop at which an interim revision, version 1.1, was further refined. These events were supplemented by written comments from

reviewers, which the authors have sought to take into account in preparing version 1.2.

0.15 It is therefore expected that these criteria will receive broad acceptance and use by a wide range of potential users and market sectors; however, it is recognised that improvements can and will be made. Comments and suggestions are therefore invited, and may be sent to any of the following addresses, bearing the marking "ITSEC Comments":

Commission of the European Communities
Directorate XIII/F
SOG-IS Secretariat
Rue de la Loi 200
B-1049 BRUSSELS
Belgium

Or, for France:

Service Central de la S\curit\ des Syst\mes d'Information
Division Information et Syst\mes
18 Rue du Docteur Zamenhof
F-92131 ISSY LES MOULINEAUX

For Germany:

Bundesamt f\r Sicherheit in der Informationstechnik
Am Nippenkreuz 19
D-5300 BONN 2

For the Netherlands:

Netherlands National Comsec Agency
Bezuidenhoutseweg 67
P.O. Box 20061
NL-2500 EB THE HAGUE

For the United Kingdom:

Head of the Certification Body
UK IT Security Evaluation and Certification Scheme
Room 2/0805
Fiddlers Green Lane
CHELTENHAM
Glos GB-GL52 5AJ

0.16 Copies of the Community publication of ITSEC version 1.2 may be obtained from the Commission of the European Communities at the above address.

This page left blank

1 SCOPE

Technical Security Measures

1.1 A major part of the security of an IT system can often be achieved through non-technical measures, such as organisational, personnel, physical, and administrative controls. However, there is a growing tendency and need to employ technical IT security measures. Although the security criteria which follow are primarily concerned with technical security measures, they do address some non-technical aspects, most notably the related secure operating procedures for personnel, physical and procedural security of the systems or products involved (but only where these impinge on the technical security measures).

1.2 These criteria have been designed so as in the main part to be equally applicable to technical security measures implemented in hardware, software and firmware. Where particular aspects of evaluation are intended only to apply to certain methods of implementation, this is indicated as part of the relevant criteria.

1.3 These criteria are not intended to cover physical aspects of hardware security such as the provision of tamper resistant enclosures or the control of electromagnetic emanations.

Systems and Products

1.4 For the purposes of this document, the difference between systems and products can be explained as follows. An IT system is a specific IT installation with a particular purpose and known operational environment. An IT product is a hardware and/or software package that can be bought off the shelf and incorporated into a variety of systems. An IT system is generally constructed from a number of hardware and software components. Some components (for example, application software) will usually be specially constructed; other components (for example, hardware) will usually be standard products. For certain applications it may be possible to buy-in a single product to serve as a complete system, but usually at least some customisation and integration to meet system specific requirements will be necessary.

1.5 From the point of view of security, the main difference between systems and products lies in what is certain about their operational

environment. A system is designed to meet the requirements of a specific group of end-users. It has a real world environment which can be defined and observed in every detail; in particular the characteristics and requirements of its end-users will be known, and the threats to its security are real threats which can be determined. A product must be suitable for incorporation in many systems; the product designer can only make general assumptions about the operational environment of a system of which it may become a component. It is up to the person buying the product and constructing the system to make sure that these assumptions are consistent with the actual environment of the system.

1.6 It is important for the sake of consistency that the same security criteria are used for both products and systems; it will then be both easier and cheaper to evaluate systems containing products which have already been successfully evaluated. This is why these criteria deal with the security evaluation of both IT products and IT systems. Within the rest of this document, the term Target of Evaluation (TOE) is used to refer to a product or system to be evaluated.

1.7 A TOE can be constructed from several components. Some components will not contribute to satisfying the security objectives of the TOE. Other components will contribute to satisfying the security objectives; these components are called security enforcing. Finally there may be some components that are not security enforcing but must nonetheless operate correctly for the TOE to enforce security; these are called security relevant. The combination of both the security enforcing components and the security relevant components of a TOE is often referred to as a Trusted Computing Base (TCB) (see figures 1 and 2).

1.8 Most evaluation work will concentrate on the components of the TOE that are stated to be security enforcing and security relevant, but all other components within the TOE will need to be considered during evaluation and shown to be neither security enforcing nor security relevant.

Functionality and Assurance, Classes and Levels

1.9 In order for a TOE to meet its security objectives, it must incorporate appropriate security enforcing functions, covering, for example, areas such as access control, auditing and error recovery.

1.10 These functions must be defined in a way that is clear and understandable to both the sponsor of evaluation and the independent evaluator. They may either be individually specified, or they may be defined by reference to a predefined functionality class. These criteria include ten example functionality classes. These example classes are based upon classes defined in the German National Criteria [ZSIEC], including five classes that correspond closely to the functionality requirements of the US Trusted Computer System Evaluation Criteria [TCSEC].

1.11 In all cases, the sponsor of an evaluation must define the security target for the evaluation. This must define the security enforcing functions to be provided by the TOE, and will also contain other relevant information, such as the security objectives of the TOE and the envisaged threats to those objectives. Details may also be given of the particular security mechanisms that will be used to implement the security enforcing functions.

1.12 The security enforcing functions selected to satisfy the security objectives of a TOE form but one aspect of the security target of a product or system. No less important is assurance that the security objectives are achieved by the selected security enforcing functions and mechanisms.

1.13 Assurance needs to be addressed from several different points of view and, in these harmonised criteria, it has been decided to distinguish confidence in the correctness in the implementation of the security enforcing functions and mechanisms from confidence in their effectiveness.

1.14 Evaluation of effectiveness assesses whether the security enforcing functions and mechanisms that are provided in the TOE will actually satisfy the stated security objectives. The TOE is assessed for suitability of functionality, binding of functionality (whether the chosen functions work together synergistically), the consequences of known and discovered vulnerabilities (both in the construction of the TOE and the way it will be used in live operation), and ease of use.

1.15 In addition, evaluation of effectiveness assesses the ability of the security mechanisms of the TOE to withstand direct attack (strength of mechanisms). Three strength levels are defined - basic, medium, and high - which represent ascending levels of confidence in the ability of the security mechanisms of the TOE to withstand direct attack.

1.16 Evaluation of correctness assesses whether the security enforcing functions and mechanisms are implemented correctly. Seven evaluation

levels labelled E0 to E6 have been defined, representing ascending levels of confidence in correctness. E0 represents inadequate confidence. E1 represents an entry point below which no useful confidence can be held, and E6 represents the highest level of confidence. The remaining levels represent an interpolation in between. Correctness is addressed from the point of view of construction of the TOE, covering both the development process and the development environment, and also the point of view of operation of the TOE.

1.17 The evaluation levels are defined within the context of the correctness criteria. The requirements for effectiveness (including strength of mechanisms) do not change by level, but rather build upon the correctness assessment and are performed using the documents provided by the sponsor for that assessment; of course, in practice the correctness and effectiveness assessment activities will be interleaved.

1.18 If a TOE fails any aspect of evaluation at a particular level, because of a lack of information or for any other reason, the deficiency must be remedied, or the TOE withdrawn from evaluation at that level. Otherwise the TOE will be assigned a result of E0.

1.19 The six successful evaluation levels E1 to E6 span a wide range of potential confidence. Not all of these levels will necessarily be needed by or appropriate for all market sectors that require independent evaluation of technical security measures. Not all combinations of functionality and confidence will necessarily be sensible or useful. For example, low confidence in the functionality required to support a military multilevel security requirement will not normally be appropriate. In addition, it is unlikely that high confidence in the correctness of a TOE will be combined with a requirement for a low strength of mechanisms.

1.20 These harmonised criteria 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 his TOE and to choose security functions to satisfy them. However for each evaluation level, the assurance part of the criteria can be thought of as a compulsory "security checklist" to be satisfied.

Assurance Profiles

1.21 The criteria in this document require the sponsor to state the

evaluation level as part of the security target. All of the security enforcing functions listed in the security target are then assessed to the same level of confidence, as required by the stated evaluation level.

1.22 For some TOEs, there may be a requirement to gain higher confidence in some security functions and lower confidence in others; for example, some security functions may be more important than others. In these circumstances, the sponsor may consider producing more than one security target for the TOE. The details of how this is achieved, and under what conditions, is beyond the scope of these criteria.

The Evaluation Process

1.23 The objective of the evaluation process is to enable the evaluator to prepare an impartial report stating whether or not a TOE satisfies its security target at the level of confidence indicated by the stated evaluation level.

1.24 The evaluation process is shown in context within figure 3. It requires the close involvement of the sponsor of the evaluation. The higher the evaluation level, the greater will need to be the involvement of the sponsor. Both users and vendors can act as sponsors for evaluation. It is likely that a system evaluation will be sponsored by the intended end-users of the system or their technical representatives, and that a product evaluation will be sponsored by the product manufacturer or a vendor of the product, but this need not be so. Any party that can supply the necessary technical information may sponsor an evaluation.

1.25 First the sponsor must determine the operational requirements and the threats the TOE is to counter. In the case of a system, there is a need to examine the real world operational environment for the system, in order to determine the relevant threats that must be addressed. For a product, there is a need to decide what threats to security the product should address. It is anticipated that industry organisations and international standardisation bodies will with time define standard functionality classes for use as product security targets. Product developers who have no predetermined specialist market niche or type of user in mind may find that such predefined functionality classes make good security targets to design their products to match.

1.26 The security objectives for the TOE can then be determined considering legal and other regulations. These form the contribution to security (confidentiality, integrity and availability) the TOE is intended to provide. Given the security objectives, the necessary security enforcing functions can then be established, possibly in an iterative way, together with the evaluation level that the TOE will have to achieve to provide the necessary level of confidence.

1.27 The results of this work - the definition of the security enforcing functions, the identified threats, the identified security objectives, any specific security mechanisms to be employed - becomes the security target for the development.

1.28 For each evaluation level, the criteria enumerate items to be delivered by the sponsor to the evaluator. The sponsor must ensure that these items are provided, taking care that any requirements for content and presentation are satisfied, and that the items clearly provide, or support the production of, the evidence that is called for.

1.29 In order that evaluation can be performed efficiently, and at minimum cost, the evaluator must work closely with the developer and sponsor of the TOE, ideally from the beginning of development, to build up a good understanding of the security target, and to be able to pinpoint the evaluation implications of decisions as they are made. However, the evaluator must remain independent and must not suggest how to design or implement the TOE. This is analogous to the role of an external financial auditor, who must likewise build up a good working relationship with a financial department, and in many cases will, after examination, make use of their internal records and controls. However, he too must remain independent and questioning.

1.30 Security test and analysis requirements within the criteria deserve special mention; in all cases the responsibility for testing and analysis will rest with the sponsor. For all evaluation levels except E1, the evaluator will primarily check test and analysis results supplied by the sponsor. The evaluator will perform test and analysis work only to audit the results supplied, to supplement the evidence provided, and to investigate vulnerabilities. At evaluation level E1 it is optional as to whether testing results are provided. If not, the evaluator must in addition perform functional testing against the security target.

The Certification Process

1.31 In order for these criteria to be of practical value, they will need to be supported by practical schemes for the provision and control of independent evaluation, run by appropriately qualified and recognised national certification bodies. These bodies will award certificates to confirm the rating of the security of TOEs, as determined by properly conducted independent evaluations. They will approve procedures, as required by these criteria, for guaranteeing the authenticity of the delivered TOE. They will also be responsible for the selection and control of approved evaluators. Details of the procedures to be used by such bodies are beyond the scope of these criteria.

1.32 These criteria have been designed to minimise the subjectivity inherent in evaluation results. It will be the responsibility of national certification bodies to maintain the uniformity of certified evaluation results. How this is achieved is beyond the scope of these criteria.

1.33 In order for the results of an evaluation against these criteria to be certified by a national certification body, the evaluator will have to produce a report containing the results of evaluation in a form acceptable for consideration by the certification body. The precise format and content of such reports are beyond the scope of these criteria.

1.34 Most security targets and TOEs will change with time. The maintenance of a certified rating following changes to a TOE (whether security-related or not) or following changes to the security target (such as new threats or security objectives) will be regulated by the appropriate national certification body. Re-evaluation will be necessary in some circumstances and not others. The details of such regulations and procedures are also a matter beyond the scope of these criteria.

Relationship to the TCSEC

1.35 The Trusted Computer System Evaluation Criteria [TCSEC], commonly known as the TCSEC or "Orange Book", is a widely known and accepted basis for the security evaluation of operating systems. Originally published in 1983, it is used by the US Department of Defense in the US product evaluation scheme operated by the National Computer Security Center (NCSC). The TCSEC criteria are intended to match the security policy of the US Department of Defense. This policy is primarily concerned with maintaining the confidentiality of nationally classified information.

1.36 The TCSEC defines seven sets of evaluation criteria called classes (D, C1, C2, B1, B2, B3 and A1), grouped into four divisions (D, C, B and A). Each criteria class covers four aspects of evaluation: Security Policy, Accountability, Assurance and Documentation. The criteria for these four areas become more detailed from class to class, and form a hierarchy whereby D is the lowest and A1 the highest. Each class covers both functionality and confidence requirements.

1.37 The criteria set out in the ITSEC permit selection of arbitrary security functions, and define seven evaluation levels representing increasing confidence in the ability of a TOE to meet its security target. Thus these criteria can be applied to cover a wider range of possible systems and products than the TCSEC. In general, for identical functionality at an equivalent level of confidence, a TOE has more architectural freedom to meet the ITSEC criteria than to meet the TCSEC, but is more constrained in its permissible development practices.

1.38 A number of example functionality classes have been defined to correspond closely to the functionality requirements of the TCSEC classes C1 to A1. They are included, as F-C1 to F-B3, amongst the example functionality classes given in Annex A. It is not possible, however, to relate the evaluation levels directly to the confidentiality requirements of the TCSEC classes, as the ITSEC levels have been developed by harmonisation of various European IT security criteria schemes which contain a number of requirements which do not appear in the TCSEC explicitly.

1.39 The intended correspondence between these criteria and the TCSEC classes is as follows:

These Criteria		TCSEC Class
E0	<--->	D
F-C1, E1	<--->	C1
F-C2, E2	<--->	C2
F-B1, E3	<--->	B1
F-B2, E4	<--->	B2

F-B3, E5	<--->	B3
F-B3, E6	<--->	A1

1.40 It should be noted that there is no functionality class F-A1 as the functionality requirements of TCSEC class A1 are the same as for class B3. A product which has been designed with the objective of successful evaluation against both the ITSEC and TCSEC, and which has been shown to meet one of the classes or combinations in the table above, should pass evaluation against the other criteria at the equivalent class or combination. However, at C1 the TCSEC requires evidence to be provided of system developer testing. Thus an [F-C1, E1] evaluation would only be equivalent to C1 evaluation if the sponsor had chosen to satisfy the optional E1 requirement to provide test documentation as evidence of adequate testing against the security target prior to evaluation.

1.41 Throughout the TCSEC, the combination of both the security enforcing and the security relevant portions of a TOE is referred to as a Trusted Computing Base (TCB). TCSEC TOEs representative of the higher classes in division B and division A derive additional confidence from increasingly rigorous architectural and design requirements placed on the TCB by the TCSEC criteria. TCSEC classes B2 and higher require that access control is implemented by a reference validation mechanism, a mechanism which implements the concept of a reference monitor [AND]. Such a reference validation mechanism must be tamper proof, it must always be invoked, and it must be small enough to be subject to analysis and tests, the completeness of which can be assured.

1.42 For compatibility with the TCSEC, the ITSEC example functionality classes F-B2 and F-B3 mandate that access control is implemented through use of such a mechanism. In addition, at higher evaluation levels the ITSEC places architectural and design constraints on the implementation of all the security enforcing functions. Combined with the ITSEC effectiveness requirements that security functionality is suitable and mutually supportive, this means that a TOE capable of meeting the higher ITSEC evaluation levels and which provides functionality matching these TCSEC-equivalent functionality classes, must necessarily satisfy the TCSEC requirements for a TCB and use of the reference monitor concept.

2 FUNCTIONALITY

Introduction

2.1 A Target of Evaluation (TOE) which provides security (some combination of confidentiality, integrity and availability) must contain appropriate security features. Normally, it will be necessary to determine that an appropriate level of confidence can be held in those features. In order for this to be done, the features themselves must be specified. The document or documents which specify the features, together with the desired evaluation level, make up the security target for the TOE.

2.2 In these criteria, security features are viewed at three levels. The most abstract view is of security objectives: the contribution to security which a TOE is intended to achieve. To achieve these objectives, the TOE must contain certain security enforcing functions. These security enforcing functions, in turn, must be implemented by specific security mechanisms. These three levels can be summarised as follows:

a) Security Objectives Why the functionality is wanted.

b) Security Enforcing Functions What functionality is actually provided.

c) Security Mechanisms How the functionality is provided.

The Security Target

2.3 The security target serves as both a specification of the security enforcing functions, against which the TOE will be evaluated, and as a description relating the TOE to the environment in which it will operate. The audience for the security target is therefore not confined solely to those responsible for the production of the TOE and its evaluation, but also includes those responsible for managing, purchasing, installing, configuring, operating and using the TOE.

2.4 The required 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.

Each of these is described in greater detail below.

2.5 The requirements for the presentation of the security target depend on the target evaluation level. The evaluation level also determines other TOE documentation that must be supplied for evaluation, together with requirements on its content and presentation, and requirements for the evidence to be provided to show that the TOE satisfies the security target.

2.6 The security target may be presented as a single document, or as multiple documents. Where multiple documents are used, their relationships to one another shall be clearly indicated.

2.7 The sponsor of an evaluation is responsible for the provision and accuracy of the security target for the evaluation.

System Security Policy

2.8 The contents of a security target depend on whether the TOE is a system or product. In the case of a system, the actual environment within which the TOE will be used is known, its actual security objectives can be determined and actual threats and existing countermeasures can be considered. These details are given in a System Security Policy.

2.9 The System Security Policy specifies the set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system. It shall identify the security objectives of the system and the threats to the system. These security objectives shall be addressed by a combination of system security enforcing functions (implemented within the TOE), and also by physical, personnel, or procedural means associated with the system. The System Security Policy shall cover all aspects of security relating to

the system, including these associated physical, procedural and personnel security measures.

2.10 All organisations will have general security standards that apply to all systems within the organisation and define the security relationship between the organisation and the outside world. These standards can be considered to be a **Corporate Security Policy**: the set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed within the organisation. Many organisations will have an explicit written Corporate Security Policy, which will specify the rules and practices and applicable national and international laws to which they conform. Where this is the case, it shall be referenced from the System Security Policy. Otherwise, all relevant aspects shall be stated within each System Security Policy of the organisation.

2.11 The primary responsibility of the Corporate Security Policy is to provide the context for the identification of system security objectives. Identifying relevant corporate assets, general threats, and the results from risk analysis will assist in the identification of these system security objectives. Discussion of the process of risk analysis is outside the scope of these criteria.

2.12 In the context of an individual system, the System Security Policy shall define the security measures to be used to satisfy the system security objectives in a way which is consistent with the Corporate Security Policy. The security measures required by the System Security Policy will be implemented by a combination of security enforcing functions implemented by the TOE, and by physical, personnel, and procedural means. The System Security Policy shall clearly indicate the division of responsibility between the security enforcing functions and the other means.

2.13 The IT security measures of a System Security Policy may be separated from the remainder of the System Security Policy, and defined in a separate document: a **Technical Security Policy**. This is the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the hardware and software of an IT system.

2.14 In many cases it may be convenient to include the specification of security enforcing functions as part of the System or Technical Security Policy.

2.15 The System or Technical Security Policy may be used as a basis for

selecting suitable IT security products for incorporation within the system; such product selection is outside the scope of these criteria.

Product Rationale

2.16 In the case of a product, the precise environment within which the TOE will be used is not known to its developer, since it may be incorporated into more than one specific system and system environment. Instead, a rationale statement shall be provided giving the necessary information for a prospective purchaser to decide whether it will help to satisfy his system security objectives, and to define what else must be done for those system security objectives to be fully met.

2.17 The product rationale shall identify the intended method of use for the product, the intended environment for use of the product and the assumed threats within that environment. It shall include a summary of the product's security features, and define all assumptions about the environment and way in which the product will be used. This shall include personnel, physical, procedural and IT security measures required to support the product, and its dependencies on system hardware, software, and/or firmware not supplied as part of the product.

Specification of Security Enforcing Functions

2.18 The security target shall include a specification of the security enforcing functions to be provided by the TOE. These functions may be stated explicitly, or by reference to one or more predefined functionality classes, or by reference to an accepted standard that defines security functionality. Predefined classes are considered later in this chapter.

2.19 One or more standards documents which address security may form part of a security target, by reference or by inclusion within the target. Where the standard allows options, the selected ones shall be clearly identified. Where a standard does not provide all the information required, the necessary supplementary information shall be provided explicitly within the security target.

2.20 In the case of a system, the security enforcing functions shall be correlated to the security objectives, so that it can be seen which functions satisfy which objectives. (A function may satisfy, or help to satisfy, more than one objective.) Every function in the specification of security enforcing functions shall at a minimum help to satisfy at least

one objective. The specification of security enforcing functions shall also show why the functions are adequate to counter the identified or stated threats to the security objectives.

2.21 In the case of a product, the security enforcing functions shall be correlated to the intended method of use of the product and the assumptions about the environment into which the product will be installed given in the product rationale. This correlation shall include any dependencies on other security enforcing functions and nonIT security measures assumed to be provided by the environment.

2.22 From the point of view of evaluation, the specification of security enforcing functions is the most important part of the security target. These functions shall always be specified in an informal style, using natural language. In addition, at higher evaluation levels they must also be specified using a semiformal or formal style of presentation. Details of such presentation styles are given later in this chapter.

Definition of Required Security Mechanisms

2.23 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).

2.24 Where security mechanisms are prescribed by the security target, it is the task of the developer to implement the required mechanisms. Otherwise, it is the task of the developer of the TOE to develop and produce mechanisms which, when combined, implement the required security enforcing functions.

Claimed Rating of Minimum Strength of Mechanisms

2.25 Every security target shall specify a claimed rating of the minimum strength of the 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 these criteria.

Target Evaluation Level

2.26 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 these criteria.

Examples of the Use of Existing Security Policy Documents

2.27 These criteria aim to permit the use of existing security policy documents developed to other criteria or standards as part or all of the security target for a system. Therefore, the precise contents of the documents comprising the security target are not prescribed. The minimum information required for evaluation against these criteria has been stated above. Since a security target may consist of more than one document, existing styles of policy document can be accommodated (although supplementary documents may be required to complete the information required for the security target).

2.28 Two examples are given below as to how particular types of security policy documents can meet the requirements for a security target.

2.29 In the UK it is mandatory to produce a System Security Policy (SSP) for all systems that will process nationally classified information. If the authorising authority decides that security evaluation is necessary, a System Electronic Information Security Policy (SEISP) must also be produced. For some target evaluation levels, a Security Policy Model (SPM) must also be produced. The SSP contains a definition of the scope of the system, the security objectives of the system, the security measures to be enforced and the allocation of responsibilities for enforcing them (i.e. it corresponds closely to a System Security Policy as described in these criteria). It also contains a derivation of the required target evaluation level based on key characteristics of the system and its environment. If necessary, an SEISP is developed from the SSP. It is a more detailed statement of the hardware and software security aspects of the SSP, but still in an informal style: it corresponds to a Technical Security Policy as described in these criteria. The SPM is a parallel specification of the security enforcing functions of an SEISP in a formal or semiformal style. It is produced where such a parallel specification is required for the target evaluation level.

2.30 A Claims Document is a list of claims about security enforcing functionality provided by a product, made by the developer of the product, and expressed in a semiformal style using the Claims Language defined in Annex B of this document. It includes assumptions and constraints about the way the product must be used for these claims to be valid. It also includes an identification of security objectives, an informal specification of the claims, a correlation of claimed security enforcing

functions to security objectives, and the desired evaluation level, in order to complete a product security target as required by these criteria.

Generic Headings

2.31 It will be easier to understand a security target if the specification of its security enforcing functions has been presented in a sensible order. This will aid the comparison of security targets and simplify the work of evaluators. There exist natural groupings of security enforcing functions to give such ordering, and a recommended set of eight generic headings for one such grouping is included as part of these criteria.

2.32 The recommended headings are:

Identification and Authentication
Access Control
Accountability
Audit
Object Reuse
Accuracy
Reliability of Service
Data Exchange.

2.33 It is recommended that these standard headings are used whenever possible. Their use will simplify comparison with other security targets and make it easier to determine whether or not a particular security target includes, or precludes, functions of a particular type.

Identification and Authentication

2.34 In many TOEs there will be requirements to determine and control the users who are permitted access to resources controlled by the TOE. This involves not only establishing the claimed identity of a user, but also verifying that the user is indeed the user claimed. This is done by the user providing the TOE with some information that is known by the TOE to be associated with the user in question.

2.35 This heading shall cover any functions intended to establish and verify a claimed identity.

2.36 This heading shall include any functions to enable new user identities to be added, and old user identities to be removed or invalidated. Similarly, it shall include any functions to generate,

change, or allow authorised users to inspect, the authentication information required to verify the identity of particular users. It shall also include functions to assure the integrity of, or prevent the unauthorised use of, authentication information. It shall include any functions to limit the opportunity for repeated attempts to establish a false identity.

Access Control

2.37 In many TOEs there will be requirements to ensure that users and processes acting on their behalf are prevented from gaining access to information or resources that they are not authorised to access or have no need to access. Similarly, there will be requirements concerning the unauthorised creation or amendment (including deletion) of information.

2.38 This heading shall cover any functions intended to control the flow of information between, and the use of resources by, users, processes and objects. This includes the administration (i.e. the granting and revocation) of access rights and their verification.

2.39 This heading shall include any functions to set up and maintain any lists or rules governing the rights to perform different types of access. It shall include any functions concerned with temporarily restricting access to objects that are simultaneously accessible by several users or processes and are needed to maintain the consistency and accuracy of such objects. It shall include any functions to ensure that upon creation, default access lists or access rules apply to objects. It shall include any functions to control the propagation of access rights to objects. It shall also include any functions to control the inference of information by the aggregation of data from otherwise legitimate accesses.

Accountability

2.40 In many TOEs there will be requirements to ensure that relevant information is recorded about actions performed by users or processes acting on their behalf so that the consequences of those actions can later be linked to the user in question, and the user held accountable for his actions.

2.41 This heading shall cover any functions intended to record the exercising of rights which are relevant to security.

2.42 This heading shall include functions related to the collection, protection and analysis of such information. Certain functions may satisfy requirements for both accountability and auditability and so berelevant to both headings. Such functions may be included under either heading, but shall be crossreferenced to the other heading.

Audit

2.43 In many TOEs there will be requirements to ensure that sufficient information is recorded about both routine and exceptional events that later investigations can determine if security violations have actually occurred, and if so what information or other resources were compromised.

2.44 This heading shall cover any functions intended to detect and investigate events that might represent a threat to security.

2.45 This heading shall include functions related to the collection, protection and analysis of such information. Such analysis may also include trend analysis used to attempt to detect potential violations of the security target before a violation occurs. Certain functions may satisfy requirements for both accountability and auditability and so be relevant to both headings. Such functions may be included under either heading, but shall be crossreferenced to the other heading.

Object Reuse

2.46 In many TOEs there will be requirements to ensure that resources such as main memory and areas of disk storage can be reused while preserving security.

2.47 This heading shall cover any functions intended to control the reuse of data objects.

2.48 This heading shall include functions to initialise or clear unallocated or reallocated data objects. It shall include any functions to initialise or clear reusable media such as magnetic tapes, or to clear output devices such as display screens when not in use.

Accuracy

2.49 In many TOEs there will be requirements to ensure specific relationships between different pieces of data are maintained correctly, and that data is passed between processes without alteration.

2.50 This heading shall cover any functions intended to ensure that

data has not been modified in an unauthorised manner.

2.51 This heading shall include functions to determine, establish and maintain the accuracy of the relationships between related data. It shall also include functions to ensure that when data is passed between processes, users and objects, it is possible to detect or prevent loss, addition or alteration, and that it is not possible to change the claimed or actual source and destination of the data transfer.

Reliability of Service

2.52 In many TOEs there will be requirements to ensure that time critical tasks are performed when they are necessary, and not earlier or later, and that nontime critical tasks cannot be made time critical. Similarly, in many TOEs there will be requirements to ensure that access to resources is possible when it is needed, and that resources are not requested or retained unnecessarily.

2.53 This heading shall cover any functions intended to ensure that resources are accessible and usable on demand by an authorised entity (i.e. a user or a process acting on his behalf) and to prevent or limit interference with timecritical operations.

2.54 This heading shall include error detection and error recovery functions intended to restrict the impact of errors on the operation of the TOE and so minimise disruption or loss of service. It shall also include any scheduling functions that ensure that the TOE responds to external events and produces outputs within specified deadlines.

Data Exchange

2.55 In many TOEs there will be requirements for the security of data during transmission over communications channels. This is normally referred to as communications security, as distinct from computer (IT) security.

2.56 This heading shall cover any functions intended to ensure the security of data during transmission over communications channels. It is recommended that such functions are broken down under the following subheadings taken from the OSI Security Architecture:

Authentication
Access Control
Data Confidentiality
Data Integrity
NonRepudiation

2.57 Functions shall be grouped under these subheadings in a way consistent with their usage and definition in the OSI Security Architecture [OSI].

2.58 Certain functions may satisfy requirements for both computer and communications security and so be relevant to other headings. In this case there shall be a crossreference to the other relevant headings.

Predefined Classes

2.59 Many systems will have similar security objectives; it will often be possible to identify common sets of security enforcing functions that meet such objectives. Similarly, many security products will be aimed at satisfying the same market need and thus possess similar functionality. Such predefined classes of common functions can be used as the basis for individual system and product security targets, or can be used as guidelines, to assist users in selecting appropriate security functionality to meet their particular security objectives, and to help manufacturers select functions to include within products. To obtain the maximum benefit from such commonality, it is desirable that standards for predefined functionality classes exist. These criteria have therefore been designed to permit reference within security targets to predefined classes of security enforcing functions. Any security target may reference one or more predefined classes to define part or all of its security enforcing functions.

2.60 Organisations for standardisation or representing particular market sectors have already developed some standard definitions. It is anticipated that the availability of these criteria will encourage the development of predefined classes, in a form consistent for use with these criteria. However, since IT security will continue to evolve rapidly, it will be necessary to define further predefined classes in the future as new groups of functions become sufficiently common to make such classes worthwhile.

2.61 As well as the specification of its security functions, each predefined class shall state the objective of the class, giving its envisaged use, and reasons for the choice of the particular functions in-

cluded. Predefined classes may also contain other information necessary for inclusion within a security target, such as the details of any mechanisms which are mandated for a class. Provided that details of the contents of such classes are publicly available, the details need not be repeated within each security target that references them.

2.62 The use of predefined classes is not obligatory. There will be cases where a sponsor of evaluation will wish not to use them, and cases where they cannot be used, for example because no predefined class describes the desired security features. As an alternative to the use of predefined classes, the security enforcing functions can always be specified individually. A statement of individual functions can be used in combination with one or more predefined classes which partially, but not entirely, describe a security target. However, a predefined class shall only be specified as part of a security target if all aspects of that class form part of the target.

2.63 Ten example predefined classes are given in Annex A. These have been derived from functionality classes given in [ZSIEC]. All are presented in informal style, and in the current version of the ITSEC are in draft form only. They are:

a) Example functionality classes FC1, FC2, FB1, FB2 and FB3 are hierarchically ordered confidentiality classes which correspond closely to the functionality requirements of the TCSEC classes C1 to A1 [TCSEC].

b) Example functionality class FIN is for TOEs with high integrity requirements for data and programs. Such requirements may be necessary in database TOEs, for example.

c) Example functionality class FAV sets high requirements for the availability of a complete TOE or special functions of a TOE. Such requirements are significant for TOEs that control manufacturing processes, for example.

d) Example functionality class FDI sets high requirements with regard to the safeguarding of data integrity during data communication.

e) Example functionality Class FDC is intended for TOEs with high demands on the confidentiality of data during data communication. An example candidate for this class is a cryptographic device.

f) Example functionality class FDX is intended for networks with high demands on the confidentiality and integrity of the information to be communicated. For example, this can be the case when sensitive information has to be communicated via insecure (for example: public) networks.

2.64 There is no restriction on the specific functionality which can be claimed or required as a security target. The security enforcing functions of any security target can be fully described within the available specification formats. The existence of predefined classes will not therefore restrict product manufacturers seeking to advance the state of the art, but will lessen the work involved in specifying products or systems which are similar to the stereotypes described, and will provide a basis for comparison of functionality offered. Product security targets may, even when claiming conformance to a predefined class, specify additional constraints and details of the required surrounding environment in order to assist potential users to determine if the product would be suitable for their actual realworld environment.

Specification Style

2.65 These criteria do not prescribe the use of particular proprietary or standardised methods or styles for the specification of security functions. Nor are any methods or styles precluded, so long as the requirements for presentation and evidence of the target evaluation level are met. For the purpose of categorising possible approaches to specification, three types of style have been identified within these criteria: informal, semiformal, and formal. Each type of style is further described below.

2.66 Not all people who will need to use a security target will be familiar with specifications written in a semiformal or formal style. Thus all security targets shall contain a specification of the security enforcing functions using an informal style. Although informal specifications do not require special training to understand, they are prone to ambiguity and imprecision. Semiformal and formal specifications reduce that possibility of ambiguity and imprecision. Thus at the higher evaluation levels, the informal specification of the security enforcing functions shall be supported by a parallel semiformal or formal specification.

2.67 The specification technique or style used within a security target for defining the security objectives, and for defining any prescribed or claimed security mechanisms, is outside the scope of these criteria.

2.68 If a security target is required to contain a specification of the security enforcing functions in a particular type of style, that specification may be wholly or partially replaced by a reference to one or more predefined classes written in such a style.

2.69 Whenever a specification in any style is required, it may be presented as a single document, or multiple documents. Where multiple documents are used, their relationships shall be clearly indicated.

Informal Specification

2.70 An informal specification is written in natural language, rather than a notation requiring special restrictions or conventions. Natural language is the term for communication in any commonly spoken tongue (for example: Dutch, English, French, German). Specifications written in natural language are not subject to any special restrictions, but do need to conform to the ordinary conventions for that language (for example: grammar and syntax).

2.71 A natural language specification shall be written with the aim of minimising ambiguity, by (as a minimum) ensuring that all terms are used consistently, and by ensuring that any terms with a specialised meaning (a meaning not defined in a widely used dictionary) are defined in one or more glossaries, which is included or referenced. It is unlikely that ambiguity can be completely eliminated. Evaluation will seek to identify and resolve any ambiguities that remain.

Semiformal Specification

2.72 A semiformal style of specification requires the use of some restricted notation (or notations), in accordance with a set of conventions which are included in or referenced by the specification. The conventions are specified informally. Such a notation shall allow the specification of both the effect of a function and all exceptional or error conditions associated with that function.

2.73 A semiformal style may either be graphical in presentation, or based on restricted use of natural language (for instance, restricted sentence structure and keywords with special meanings). Examples of semiformal styles include dataflow diagrams, state transition diagrams, entityrelationship diagrams, data structure diagrams, process or program

structure diagrams, and the CCITT recommended specification notation SDL.

2.74 Structured design and development methods normally incorporate at least one such semiformal notation for requirements capture, together with prescriptive guidance (for instance, measures of complexity and management methods) on how to use the notation. Examples of structured design methods including such notations are: the Yourdon Structured Method [YSM], Structured Analysis and Design Technique [SADT], Structured Systems Analysis and Design Method [SSADM], and the Jackson Structured Design [JSD] and Jackson Structured Programming [JSP] methods.

2.75 A particular example of a semiformal notation that has been successfully used in the definition of security targets is the Claims Language. The Claims Language is a subset of English; both the vocabulary and the syntactic form of claim sentences are restricted. It was designed (as the name suggests) to provide a structured way in which claims could be made about the security features of IT products. The Claims Language provides for the use of natural language to express those parts of the definition of a security target which support the definition of the claimed security enforcing functions. A full definition of the Claims Language, consistent with these criteria, can be found in Annex B.

Formal Specification

2.76 A formal style of specification is written in a formal notation based upon wellestablished mathematical concepts. The concepts are used to define the syntax and semantics of the notation, and the proof rules supporting logical reasoning. Formal specifications must be capable of being shown to be derivable from a set of stated axioms, and must be capable of showing the validity of key properties such as the delivery of a valid output for all possible inputs. Where hierarchical levels of specification exist, it must be possible to demonstrate that each level maintains the properties established for the previous level.

2.77 The syntactic and semantic rules supporting a formal notation used in a security target shall define how to recognise constructs unambiguously and determine their meaning. Where proof rules are used to support logical reasoning, there shall be evidence that it is impossible to derive contradictions. All rules supporting the notation shall be defined or referenced. All constructs used in a formal specification shall be completely described by the supporting rules. The formal notation shall allow the specification of both the effect of a function and all exceptional or error conditions associated with that function.

2.78 Example formal notations are VDM, described in [SSVDM], Z,

described in [ZRM], the RAISE Specification Language, described in [RSL], Ina Jo, described in [IJRM], the Gypsy Specification Language, described in [GYPSY], and the ISO protocol specification language [LOTOS]. The use of constructs from predicate (or other) logic and set theory as a formal notation is acceptable, provided that the conventions (supporting rules) are documented or referenced (as set out above).

Consistency of Parallel Specifications in Different Styles

2.79 Parallel specifications shall be presented in such a way that the relationships between the specifications are clear, and that where each specification addresses the same point, that point is addressed consistently. Parallel specifications may be presented as separate documents, or may be interleaved in a single document.

2.80 Where ambiguity exists in an informal specification, the corresponding formal or semiformal specification shall resolve the ambiguity. However, it shall be an error for parallel specifications to be inconsistent. Any such error must be resolved by reference to further information outside the security target and one or both specifications amended.

Formal Models of Security Policy

2.81 At evaluation levels E4 and above, a TOE must implement an underlying model of security policy, i.e. there must be an abstract statement of the important principles of security that the TOE will enforce. This shall be expressed in a formal style, as a formal model of security policy. All or part of a suitable published model can be referenced, otherwise a model shall be provided as part of the security target. Any of the formal specification styles identified above may be used to define such a model.

2.82 The formal model need not cover all the security enforcing functions specified within the security target. However, an informal interpretation of the model in terms of the security target shall be provided, and shall show that the security target implements the underlying security policy and contains no functions that conflict with that underlying policy.

2.83 Examples of published formal models of security policy are:

a) The BellLa Padula model [BLP] modelling access control requirements typical of a national security policy for confidentiality.

b) The Clark and Wilson model [CWM] modelling the integrity requirements of commercial transaction processing systems.

c) The Brewer Nash model [BNM] modelling access control requirements for client confidentiality, typical of a financial services institution.

d) The Eizenberg model [EZBM] modelling access control rights that vary with time.

e) The Landwehr model [LWM] modelling the data exchange requirements of a message processing network.

3 ASSURANCE - EFFECTIVENESS

Introduction

3.1 This chapter sets out evaluation criteria addressing the effectiveness aspect of assurance for a Target of Evaluation (TOE). The baseline for evaluation is the security target, as defined in Chapter 2, which is simultaneously evaluated for effectiveness, in accordance with the criteria set out in this chapter, and correctness, in accordance with the criteria set out in Chapter 4 following.

Description of the Approach

3.2 Assessment of effectiveness involves consideration of the following aspects of the TOE:

a) the suitability of the TOE's security enforcing functions to counter the threats to the security of the TOE identified in the security target;

b) the ability of the TOE's security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole;

c) the ability of the TOE's security mechanisms to withstand direct attack;

d) whether known security vulnerabilities in the construction of the TOE could in practice compromise the security of the TOE;

e) 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;

f) whether known security vulnerabilities in the operation of the TOE could in practice compromise the security of the TOE.

3.3 The assessment of each of the aspects of effectiveness identified above is performed using documentation supplied by the sponsor and also documentation and evaluation results from the evaluation of correctness of the TOE. This means that although evaluation of effectiveness can proceed in parallel with the evaluation of correctness, it cannot be completed until after the final results of the assessment of correctness are available.

3.4 Specifically, the assessment of effectiveness is based on a vulnerability analysis of the TOE. This analysis has the objective of searching for all the ways in which it is possible for a user of the TOE to deactivate, bypass, corrupt, circumvent, directly attack, or otherwise defeat the security enforcing functions and mechanisms of the TOE. As a minimum, the sponsor's vulnerability analysis must consider all the information specified in figure 4 for the evaluation level in question (i.e. a search for vulnerabilities is to be performed using part of the total information provided by the sponsor for that evaluation level). As the evaluation level increases, the correctness criteria of Chapter 4 requires the information specified in figure 4 to be provided at increasing levels of rigour, as indicated by the use of the verbs state, describe, and explain.

3.5 All critical security mechanisms (i.e. those mechanisms whose failure would create a security weakness) are assessed for their ability to withstand direct attack. The minimum strength of each critical mechanism shall be rated either basic, medium or high.

3.6 For the minimum strength of a critical mechanism to be rated basic it shall be evident that it provides protection against random accidental subversion, although it may be capable of being defeated by knowledgeable attackers.

3.7 For the minimum strength of a critical mechanism to be rated medium it shall be evident that it provides protection against attackers with limited opportunities or resources.

3.8 For the minimum strength of a critical mechanism to be rated high it shall be evident that it could only be defeated by attackers possessing a high level of expertise, opportunity and resources, successful attack being judged to be beyond normal practicality.

3.9 A TOE will only fail evaluation on effectiveness grounds if an exploitable vulnerability, which is found during evaluation of effectiveness, has not been eliminated before the end of evaluation. This includes methods of successful direct attack found during the assessment

of minimum strength of mechanisms which invalidates the claimed rating. If any such vulnerability exists the TOE will be awarded an overall evaluation level of E0, indicating that it would be unsuitable for use as proposed.

3.10 Effectiveness of a TOE is always assessed in the context of the given security target. For example, a security product sold for incorporation within systems may contain known covert channels. If, however, the system security target has no access control requirements for confidentiality, then the presence of covert channels in the product is irrelevant and will not effect the ability of the TOE to meet its security target, and will not cause the TOE to fail evaluation. If there are system access control requirements for confidentiality, then the system security target may specify acceptable maximum covert channel bandwidths. If covert channels are identified which exceed these bandwidths, or if no bandwidth is actually specified, then the evaluator must determine if the identified covert channels will cause the TOE to fail evaluation on the grounds of unsuitable functionality.

Systems and Products

3.11 There are different requirements and options for the content of a security target for a TOE, depending on whether the TOE is being evaluated as a system or product. These differences are set out under Construction - Phase 1 - Requirements in Chapter 4, and further explained in Chapter 2.

Effectiveness Criteria - Construction

Documentation

3.12 The sponsor shall provide the following documentation in addition to that required for evaluation of correctness:

- Suitability Analysis
- Binding Analysis
- Strength of Mechanisms Analysis
- List of Known Vulnerabilities in Construction.

Aspect 1 - Suitability of Functionality

Definition

3.13 As part of the documentation required for the evaluation of correctness, the sponsor will provide a security target. As part of the assessment of correctness, that target is examined for coverage and consistency. For this aspect of effectiveness the security target is used to determine whether 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.

Requirements for Content and Presentation

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.

Requirements for Evidence

3.15 The suitability 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 for the evaluation level in question.

Evaluator Actions

3.16 Check that the suitability analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 for the evaluation level in question.

Aspect 2 - Binding of Functionality

Definition

3.17 This aspect of effectiveness investigates the ability of the security enforcing functions and mechanisms of the TOE to work together in a way that is mutually supportive and provides an integrated and effective whole.

Requirements for Content and Presentation

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

Requirements for Evidence

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

Evaluator Actions

3.20 Check that the binding analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 for the evaluation level in question.

Aspect 3 - Strength of Mechanisms

Definition

3.21 Even if a security enforcing mechanism cannot be bypassed, deactivated, corrupted, or circumvented, it may still be possible to defeat it by a direct attack based on deficiencies in its underlying algorithms, principles or properties. For this aspect of effectiveness the ability of these mechanisms to withstand such direct attack is assessed. This aspect of effectiveness is distinguished from other aspects in that it requires consideration of the level of resources that would be needed for an attacker to execute a successful attack.

Requirements for Content and Presentation

3.22 The strength 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.

Requirements for Evidence

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: 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 for the evaluation level in question.

Evaluator Actions

3.24 Check that all mechanisms that are critical have been identified as such. Check that the strength of mechanisms analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 for the evaluation level in question. Check that the specifications/definitions of all critical mechanisms support the claimed minimum strength rating. Perform **penetration testing** where necessary to confirm or disprove the claimed minimum strength of mechanisms.

Aspect 4 - Construction Vulnerability Assessment

Definition

3.25 Before and during the other aspects of evaluation of the TOE, various vulnerabilities in the construction of the TOE (such as ways of deactivating, bypassing, corrupting, or circumventing security enforcing functions and mechanisms) will have been identified by both sponsor and evaluator. For this aspect of effectiveness these known vulnerabilities are assessed to determine whether they could in practice compromise the security of the TOE as specified by the security target.

Requirements for Content and Presentation

3.26 The list 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.

Requirements for Evidence

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.

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

Evaluator Actions

3.28 Check that the list of known vulnerabilities in construction meets all requirements for content and presentation and evidence given above. Check that the analysis of the potential impact of each vulnerability has considered all of the information given in figure 4 for the evaluation level in question. Perform an independent vulnerability analysis, taking into account both the listed and any other known construction vulnerabilities found during evaluation. Check that all combinations of known vulnerabilities have been addressed. Check that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures have been appropriately documented. Perform penetration testing to confirm or disprove whether the known vulnerabilities are actually exploitable in practice.

Effectiveness Criteria - Operation

Documentation

3.29 The sponsor shall provide the following documentation in addition to that required for evaluation of correctness:

- Ease of Use Analysis
- List of Known Vulnerabilities in Operational Use.

Aspect 1 - Ease of Use

Definition

3.30 This aspect of effectiveness investigates whether the TOE can 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.

Requirements for Content and Presentation

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.

Requirements for Evidence

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. 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 for the evaluation level in question.

Evaluator Actions

3.33 Check that the ease of use analysis provided meets all requirements for content and presentation and evidence. Check that the analysis has considered all of the information given in figure 4 for the evaluation level in question. Check the analysis for undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures (such as

external procedural, physical and personnel controls) have been appropriately documented. Repeat any configuration and installation procedure to check that the TOE can be configured and used securely, using only the user and administration documentation for guidance. Perform other testing where necessary to confirm or disprove the ease of use analysis.

Aspect 2 - Operational Vulnerability Assessment

Definition

3.34 Before and during the other aspects of evaluation of the TOE, various vulnerabilities in operation of the TOE will have been identified by both sponsor and evaluator. For this aspect of effectiveness these known vulnerabilities are assessed to determine whether they could in practice compromise the security of the TOE as specified by the security target.

Requirements for Content and Presentation

3.35 The list 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.

Requirements for Evidence

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.

The analysis shall be performed using, at minimum, all the information given in figure 4 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.

Evaluator Actions

3.37 Check that the list of known vulnerabilities in operation meets all requirements for content and presentation and evidence given above. Check that the analysis of the potential impact of each vulnerability has considered all of the information given in figure 4 for the evaluation level in question. Perform an independent vulnerability analysis, taking into account both the listed and any other known operational vulnerabilities found during evaluation. Check that all combinations of known vulnerabilities have been addressed. Check that the analyses of the potential impact of vulnerabilities contain no undocumented or unreasonable assumptions about the intended environment. Check that all assumptions and requirements for external security measures have been appropriately documented. Perform penetration testing to confirm or disprove whether the known vulnerabilities are actually exploitable in practice.

INFORMATION OBTAINED FROM A CORRECTNESS ASSESSMENT WHICH IS USED TO PERFORM A VULNERABILITY ANALYSIS

4 ASSURANCE - CORRECTNESS

Introduction

4.1 This chapter sets out evaluation criteria addressing the correctness aspect of assurance for a Target of Evaluation (TOE). The baseline for evaluation is a security target defined in accordance with Chapter 2. The security target shall contain the necessary elements specified in Chapter 2 for a system or product as appropriate. This shall include the target evaluation level and the claimed rating for minimum strength of mechanisms. The effectiveness aspect of assurance is covered by the criteria detailed in Chapter 3.

Characterisation

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

4.3 The seven evaluation levels can be characterised as follows:

Level E0

4.4 This level represents inadequate assurance.

Level E1

4.5 At this level there shall be a security target and an informal description of the architectural design of the TOE. Functional testing shall indicate that the TOE satisfies its security target.

Level E2

4.6 In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.

Level E3

4.7 In addition to the requirements for level E2, the source code

and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.

Level E4

4.8 In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semiformal style.

Level E5

4.9 In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.

Level E6

4.10 In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

Summary of Requirements

4.11 Remaining sections of this chapter contain the detailed criteria to be satisfied at each correctness evaluation level, under detailed headings, repeated for each of the levels E1 to E6. The major differences between levels follow from additional requirements in the investigation of the Development Process. To assist understanding of these differences, the following diagrams show the relationship between key items to be supplied by the sponsor and the evaluation level at which they are first required by the evaluator.

CORRECTNESS CRITERIA BY LEVEL - DEVELOPMENT PROCESS

CORRECTNESS CRITERIA BY LEVEL - DEVELOPMENT ENVIRONMENT

CORRECTNESS CRITERIA BY LEVEL - OPERATION

Approach to Descriptions

4.12 The evaluation criteria for assessment of correctness distinguish between criteria concerning the way the TOE is developed (construction) and criteria concerning the way it will be used (operation). For each evaluation level, these evaluation criteria are further broken down under various phases and aspects.

4.13 For each aspect or phase, documentation that must be provided for examination is identified, followed by requirements for its content and presentation or for the procedures and standards it must define, followed by the evidence required to show that the criteria in question have been met and finally the actions to be performed by the evaluator are stated.

4.14 For clarity, since there are significantly different requirements for each evaluation level, the criteria for each level are set out separately. New or changed criteria at each level are printed in bold. There is a general need for greater rigour and depth in the evidence provided at higher evaluation levels. This is reflected in the progressive use of the verbs state, describe and explain at different levels in many criteria for content and presentation which do not otherwise change.

4.15 Except at E1, the burden for the provision of evidence is on the sponsor. This is then checked or audited by the evaluator. An additional requirement to produce evidence is only placed on the evaluator when independent action is required to provide the necessary confidence. For example, there are requirements to provide evidence of dynamic testing placed on both sponsor and evaluator. The major requirement is for the sponsor to provide evidence, in particular test plans and test results, produced as part of the normal development process for the system or product in question. The requirement placed on the evaluator is to show that he has examined the results provided by the sponsor but has also performed his own tests to check the completeness, comprehensiveness and accuracy of sponsor supplied testing, and also to address any points of apparent inconsistency or error found in the results of those tests.

4.16 Testing is seen as just one aspect of quality assurance. Throughout the criteria it is assumed that a Quality Assurance Programme has been introduced and is active throughout the whole lifecycle of the TOE. This Quality Assurance Programme has to encompass the creation, maintenance and destruction of all documents, programs and hardware with respect to the TOE. The criteria laid down in this document can guide quality assurance assessors as to whether the programme is adequate for the evaluation level at which the TOE is targeted.

Layout of Correctness Criteria

4.17 The following paragraphs describe the layout and content of criteria which will be used for each evaluation level from E1 to E6. They are relevant to each level and will not be repeated for each of them. The individual paragraphs within each evaluation level are numbered as follows:

<level designator>.<paragraph number within level>

so, for example, the 3rd paragraph of level E2 is numbered E2.3. Null paragraphs are inserted where necessary at each level so that the same numbered paragraph within each level refers to the same topic.

Construction - The Development Process

4.18 A major source of confidence in the correctness of the security aspects of a TOE is understanding the way it was developed. For the purposes of these criteria, four phases are identified in the development process. Factors contributing to the development of confidence are identified in the criteria for each of these phases in turn. Regardless of how a TOE is actually produced the evidence shall be presented to match these phases.

Phase 1 - Requirements

4.19 This first phase of the development process covers the production of a security target for the system or product. The security target is the baseline for evaluation. It will include the target evaluation level and the claimed rating for minimum strength of mechanisms.

Phase 2 - Architectural Design

4.20 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). It is particularly important that the architectural design

provides for a clear and effective separation between security-enforcing and other components. Separation may be achieved physically, or by supporting protection mechanisms provided by hardware or firmware, or by other means. 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. Phase 3 - Detailed Design

4.21 This phase of the development process covers the refinement of the architectural design of the TOE to a level of detail that can be used as a basis for programming and/or hardware construction, i.e. all stages of design and specification below the initial top level specification. Components identified at the lowest level of specification are called basic components; it is from the basic component specifications that the actual software and/or hardware will be produced. At this level, security enforcing components will be identified. Also at this level, some non-security-enforcing components may be identified whose failure or misuse could compromise security. These components are security relevant, as their correct operation is relied upon for the TOE to enforce security. Intermediate levels of specification may exist, depending on the development method employed and the complexity of the TOE. It is important that as the specifications of the TOE become more detailed and less abstract, the transformation is performed in a way that correctly preserves the intent of the top level description.

Phase 4 - Implementation

4.22 This phase of the development process covers the implementation of the detailed design of the TOE in hardware and/or software. Each basic component is first programmed or built from the basic component specifications. These individual basic components are then to be checked and tested against their specifications. Individual basic components are then integrated together in a controlled manner until the complete TOE exists. The complete TOE is then to be checked and tested as a whole against the security target. It is to be recognized that testing a basic component or larger unit against its specification can only show errors or deviations from the specification, never the absence of errors. Therefore it will be necessary at higher evaluation levels to supplement testing by analysis.

Construction - The Development Environment

4.23 The development environment comprises the measures, procedures and standards used by the developer whilst developing, producing and maintaining the TOE.

Aspect 1 - Configuration Control

4.24 Configuration control covers the controls imposed by the developer on his development, production and maintenance processes; for example, to ensure that each representation of the design or its implementation is produced and changed in a controlled manner, and can be shown to correspond correctly to the previous representations on which it is based. Assessment of configuration control will include understanding the developer's quality management procedures. Following delivery of the first version of a TOE, it is almost inevitable that correction of flaws, or modification to meet changed objectives, will mean that further versions of the TOE will need to be developed and issued. It is therefore necessary that configuration control of the TOE and its documentation is maintained following initial release and delivery. Configuration control is important as a way for the developer to ensure that the TOE is not modified in such a way as to invalidate the results of evaluation.

Aspect 2 - Programming Languages and Compilers

4.25 This aspect applies to basic components implemented in software and firmware only. It includes requirements concerning the programming languages, the compiling tools and the runtime supporting libraries used to develop the TOE.

Aspect 3 - Developers Security

4.26 Developer Security covers the physical, procedural, technical and personnel measures used in the development environment. It includes the physical security of the development location(s), and controls on the selection and vetting of development staff. Its objective is to protect development from deliberate attack and to maintain the confidentiality of information as appropriate.

Operation - The Operational Documentation

4.27 Operational Documentation provides the major means by which the developer of a TOE and his customers communicate. Its understandability, coverage and correctness are therefore important factors in secure operation of the TOE. It can be considered to fall into two classes: information for end-users (user documentation) and information for administrators (administration documentation).

Aspect 1 - User Documentation

4.28 User documentation is the information about the TOE supplied by the developer for use by end-users. This documentation should help the end-user understand the security capabilities of the TOE, and the end-user's contribution to maintaining security during use.

Aspect 2 - Administration Documentation

4.29 Administration documentation is the information about the TOE supplied by the developer for use by the administrator. This information may include information not relevant or appropriate to end-users. This documentation should help the administrator set up and operate the TOE in a way which is secure.

Operation - The Operational Environment

4.30 The operational environment comprises the measures, procedures and standards concerned with secure delivery, installation and operational use of a TOE. In the case of a system which is already in use, it is possible to assess the actual operational procedures. In other circumstances, it is only possible to evaluate proposed procedures.

Aspect 1 - Delivery and Configuration

4.31 This section covers the procedures used to maintain security during transfer of the TOE or its component parts to the user, both on initial delivery and as part of subsequent modification. It includes any special procedures or operations required to configure the TOE during installation, or to demonstrate the authenticity of the delivered TOE. Such procedures and measures are the basis for ensuring that the security protection offered by the TOE is not compromised during transfer or by interference with the security features during installation and configuration at the user's site.

Aspect 2 - Start-up and Operation

4.32 This covers the procedures used by the administrator in order to operate the TOE in a secure manner on a daily basis. It shall cover not only day-to-day operation (matters such as starting the system up) but also other routine activities such as necessary backups and maintenance, and exceptional activities such as start-up and recovery following a failure. Almost all TOEs require maintenance, either to meet changed objectives, or to address failures. Thus these procedures shall provide

for authorised modifications, replacements or additions to the TOE.

LEVEL E1

Construction - The Development Process

E1.1 The sponsor shall provide the TOE, and the following documentation:

- **The security target for the TOE**
- **Informal description of the architecture of the TOE**
- **Test documentation (optional)**
- **Library of test programs and tools used for testing the TOE (optional)**

Phase 1 - Requirements

Requirements for Content and Presentation

E1.2 **The security 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.**

Requirements for Evidence

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. 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.

Evaluator Actions

E1.4 **Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target.**

Phase 2 - Architectural Design

Requirements for Content and Presentation

E1.5 **The description 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.**

Requirements for Evidence

E1.6 **The description of the architecture shall state how the security enforcing functions of the security target will be provided.**

Evaluator Actions

E1.7 **Check that the information provided meets all requirements for content and presentation and evidence.**

Phase 3 - Detailed Design

Requirements for Content and Presentation

E1.8 **No Requirement.**

Requirements for Evidence

E1.9 **No Requirement.**

Evaluator Actions

E1.10 **No Action.**

Phase 4 - Implementation

Requirements for Content and Presentation

E1.11 **Test documentation 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.** Requirements for Evidence

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

Evaluator Actions

E1.13 **Check that the TOE satisfies the security target by performing tests covering all security enforcing functions identified in the security target. Perform additional tests to search for errors. The evaluator need not duplicate testing performed by or for the sponsor where adequate evidence of that testing is provided, but shall check by sampling the results of such tests.**

Construction - The Development Environment

E1.14 The sponsor shall provide the following documentation:

- **Configuration list identifying the version of the TOE for evaluation**

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E1.15 **The configuration list shall state where the TOE is uniquely identified (version number).**

Requirements for Evidence

E1.16 **The configuration list shall state how the TOE is uniquely identified.**

Evaluator Actions

E1.17 **Check that the information provided meets all requirements for content and presentation and evidence.**

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E1.18 **No Requirement.**

Requirements for Evidence

E1.19 **No Requirement.**

Evaluator Actions

E1.20 **No Action.**

Aspect 3 - Developers Security

Requirements for Content and Presentation

E1.21 **No Requirement.**

Requirements for Evidence

E1.22 **No Requirement.**

Evaluator Actions

E1.23 **No Action.**

Operation - The Operational Documentation

E1.24 The sponsor shall provide the following documentation:

- **User documentation**

- **Administration documentation**

Aspect 1 - User Documentation

Requirements for Content and Presentation

E1.25 **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.**

Requirements for Evidence

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

Evaluator Actions

E1.27 **Check that the information provided meets all requirements for content and presentation and evidence.**

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E1.28 **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. 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.

Requirements for Evidence

E1.29 **The administration documentation shall state how the TOE is administered in a secure manner.**

Evaluator Actions

E1.30 **Check that the information provided meets all requirements for content and presentation and evidence.**

Operation - The Operational Environment

E1.31 The sponsor shall provide the following documentation:

- **Delivery and Configuration Documentation**
- **Start-up and Operation Documentation**

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

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

Requirements for Evidence

E1.33 **The information supplied shall state how the procedures maintain security.**

Evaluator Actions

E1.34 **Check that the information provided meets all requirements for content and presentation and evidence.**

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E1.35 **The procedures for secure start-up and operation shall be stated.**

Requirements for Evidence

E1.36 **The information supplied shall state how the procedures maintain security.**

Evaluator Actions

E1.37 **Check that the information provided meets all requirements for content and presentation and evidence.**

LEVEL E2

Construction - The Development Process

E2.1 The sponsor shall provide the TOE, and the following documentation:

- The security target for the TOE
- Informal description of the architecture of the TOE
- **Informal description of the detailed design**
- **Test documentation**
- **Library of test programs and tools used for testing the TOE**

Phase 1 - Requirements

Requirements for Content and Presentation

E2.2 The security 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.

Requirements for Evidence

E2.3 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. 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.

Evaluator Actions

E2.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target.

Phase 2 - Architectural Design

Requirements for Content and Presentation

E2.5 The description 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.**

Requirements for Evidence

E2.6 The description 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.**

Evaluator Actions

E2.7 Check that the information provided meets all requirements for content and presentation and evidence. **Check that the separation of security enforcing and other components is valid.**

Phase 3 - Detailed Design

Requirements for Content and Presentation

E2.8 **The detailed 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.**

Requirements for Evidence

E2.9 **The detailed 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.**

Evaluator Actions

E2.10 **Check that the information provided meets all requirements for content and presentation and evidence.**

Phase 4 - Implementation

Requirements for Content and Presentation

E2.11 **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.**

Requirements for Evidence

E2.12 **The test documentation shall state the correspondence between tests and the security enforcing functions defined in the security target.**

Evaluator Actions

E2.13 **Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. Perform additional tests to search for errors.**

Construction - The Development Environment

E2.14 The sponsor shall provide the following documentation:

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

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

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E2.15 **The development 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.**

Requirements for Evidence

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.**

Evaluator Actions

E2.17 **Check that the documented procedures are being applied.** Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E2.18 No Requirement.

Requirements for Evidence

E2.19 No Requirement.

Evaluator Actions

E2.20 No Action.

Aspect 3 - Developers Security

Requirements for Content and Presentation

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

Requirements for Evidence

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.**

Evaluator Actions

E2.23 **Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.**

Operation - The Operational Documentation

E2.24 The sponsor shall provide the following documentation:

- User documentation
- Administration documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

E2.25 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.

Requirements for Evidence

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

Evaluator Actions

E2.27 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E2.28 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. 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.

Requirements for Evidence

E2.29 The administration documentation shall state how the TOE is administered in a secure manner.

Evaluator Actions

E2.30 Check that the information provided meets all requirements for content and presentation and evidence.

Operation - The Operational Environment

E2.31 The sponsor shall provide the following documentation:

- Delivery and Configuration Documentation

- Start-up and Operation Documentation

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

E2.32 If different 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.**

Requirements for Evidence

E2.33 The information supplied shall state how the procedures maintain security.

Evaluator Actions

E2.34 Check that the information provided meets all requirements for content and presentation and evidence. **Check the correct application of the delivery procedures. Search for errors in the system generation procedures.**

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E2.35 The procedures for secure start-up and operation shall be stated. **If any security enforcing functions can be deactivated or modified during start-up, 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.**

Requirements for Evidence

E2.36 The information 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 start-up and operation.**

Evaluator Actions

E2.37 Check that the information provided meets all requirements for content and presentation and evidence. **Check the example evidence required for start-up and operation. Search for errors in the procedures.**

LEVEL E3

Construction - The Development Process

E3.1 The sponsor shall provide the TOE, and the following documentation:

- The security target for the TOE
- Informal description of the architecture of the TOE
- Informal description of the detailed design
- 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**

Phase 1 - Requirements

Requirements for Content and Presentation

E3.2 The security 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.

Requirements for Evidence

E3.3 In the 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.

Evaluator Actions

E3.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target.

Phase 2 - Architectural Design

Requirements for Content and Presentation

E3.5 The description 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.

Requirements for Evidence

E3.6 The description 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.

Evaluator Actions

E3.7 Check that the information provided meets all requirements for content and presentation and evidence. Check that the separation of security enforcing and other components is valid.

Phase 3 - Detailed Design

Requirements for Content and Presentation

E3.8 **The detailed 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.

Requirements for Evidence

E3.9 The detailed 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.

Evaluator Actions

E3.10 Check that the information provided meets all requirements for content and presentation and evidence.

Phase 4 - Implementation

Requirements for Content and Presentation

E3.11 **The description 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.

Requirements for Evidence

E3.12 The test 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.

Evaluator Actions

E3.13 Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. **Check that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Check all retesting following the correction of errors.** Perform additional tests to search for errors.

Construction - The Development Environment

E3.14 The sponsor shall provide the following documentation:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system
- **Information on the acceptance procedure**
- Information on the security of the development environment
- **Description of all implementation languages used**

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E3.15 The development 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.

Requirements for Evidence

E3.16 The information 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.

Evaluator Actions

E3.17 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E3.18 **Any 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.**

Requirements for Evidence

E3.19 **The definition of the programming languages shall define unambiguously the meaning of all statements used in the source code.**

Evaluator Actions

E3.20 **Check that the information provided meets all requirements for content and presentation and evidence.**

Aspect 3 - Developers Security

Requirements for Content and Presentation

E3.21 The document 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**.

Requirements for Evidence

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

Evaluator Actions

E3.23 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.

Operation - The Operational Documentation

E3.24 The sponsor shall provide the following documentation:

- User documentation
- Administration documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

E3.25 The user 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.

Requirements for Evidence

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

Evaluator Actions

E3.27 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E3.28 The administration 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.

Requirements for Evidence

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

Evaluator Actions

E3.30 Check that the information provided meets all requirements for content and presentation and evidence.

Operation - The Operational Environment

E3.31 The sponsor shall provide the following documentation:

- Delivery and Configuration Documentation

- Start-up and Operation Documentation

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

E3.32 If different 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.

Requirements for Evidence

E3.33 The information supplied shall **describe** how the procedures maintain security.

Evaluator Actions

E3.34 Check that the information provided meets all requirements for content and presentation and evidence. Check the correct application of the delivery procedures. Search for errors in the system generation procedures.

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E3.35 The procedures for secure start-up and operation shall be **described**. If any security enforcing functions can be deactivated or modified during start-up, 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.

Requirements for Evidence

E3.36 The information 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 start-up and operation.

Evaluator Actions

E3.37 Check that the information provided meets all requirements for content and presentation and evidence. Check the example evidence required for start-up and operation. Search for errors in the procedures.

LEVEL E4

Construction - The Development Process

E4.1 The sponsor shall provide the TOE, and the following documentation:

- The security target for the TOE
- **Definition or reference to an underlying formally specified model of security**
- **Informal interpretation of the underlying model in terms of the security target**
- **Semiformal** description of the architecture of the TOE
- **Semiformal** description of the detailed design
- 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

Phase 1 - Requirements

Requirements for Content and Presentation

E4.2 The security 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.

Requirements for Evidence

E4.3 In the 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.**

Evaluator Actions

E4.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target. **Check that there are no security features in the security target that conflict with the underlying security policy.**

Phase 2 - Architectural Design

Requirements for Content and Presentation

E4.5 **A semiformal 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.

Requirements for Evidence

E4.6 The description 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.**

Evaluator Actions

E4.7 Check that the information provided meets all requirements for content and presentation and evidence. Check that the separation of security enforcing and other components is valid.

Phase 3 - Detailed Design

Requirements for Content and Presentation

E4.8 **A semiformal 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.

Requirements for Evidence

E4.9 The detailed 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.

Evaluator Actions

E4.10 Check that the information provided meets all requirements for content and presentation and evidence.

Phase 4 - Implementation

Requirements for Content and Presentation

E4.11 The description 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.

Requirements for Evidence

E4.12 The test 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.

Evaluator Actions

E4.13 Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. Check that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Check all retesting following the correction of errors. Perform additional tests to search for errors.

Construction - The Development Environment

E4.14 The sponsor shall provide the following documentation:

- Configuration list identifying the version of the TOE for evaluation

- Information on the configuration control system and its

tools

- **Audit information on modifications of all parts of the TOE subject to configuration control**

- Information on the acceptance procedure

  - Information on the security of the development environment

  - Description of all implementation languages and compilers used

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E4.15 The development 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.**

Requirements for Evidence

E4.16 The information 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.

Evaluator Actions

E4.17 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. **Use the developers tools to rebuild selected parts of the TOE and compare with the submitted version of the TOE.**

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E4.18 Any 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.**

Requirements for Evidence

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

Evaluator Actions

E4.20 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 3 - Developers Security

Requirements for Content and Presentation

E4.21 The document 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.

Requirements for Evidence

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

Evaluator Actions

E4.23 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.

Operation - The Operational Documentation

E4.24 The sponsor shall provide the following documentation:

- User documentation
- Administration documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

E4.25 The user 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.

Requirements for Evidence

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

Evaluator Actions

E4.27 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E4.28 The administration 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.

Requirements for Evidence

E4.29 The administration documentation shall describe how the TOE is administered in a secure manner.

Evaluator Actions

E4.30 Check that the information provided meets all requirements for content and presentation and evidence.

Operation - The Operational Environment

E4.31 The sponsor shall provide the following documentation:

- Delivery and Configuration Documentation
- Start-up and Operation Documentation

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

E4.32 If different 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.

Requirements for Evidence

E4.33 The information supplied shall describe how the procedures maintain security.

Evaluator Actions

E4.34 Check that the information provided meets all requirements for content and presentation and evidence. Check the correct application of the delivery procedures. Search for errors in the system generation procedures.

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E4.35 The procedures for secure start-up and operation shall be described. If any security enforcing functions can be deactivated or modified during start-up, 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.

Requirements for Evidence

E4.36 The information 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 start-up and operation.

Evaluator Actions

E4.37 Check that the information provided meets all requirements for content and presentation and evidence. Check the example evidence required for start-up and operation. Search for errors in the procedures.

LEVEL E5

Construction - The Development Process

E5.1 The sponsor shall provide the TOE, and the following documentation:

- The security target for the TOE
- Definition or reference to an underlying formally specified model of security
- Informal interpretation of the underlying model in terms of the security target
- Semiformal description of the architecture of the TOE
- Semiformal description of the detailed design
- 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

Phase 1 - Requirements

Requirements for Content and Presentation

E5.2 The security 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.

Requirements for Evidence

E5.3 In the 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.

Evaluator Actions

E5.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target. Check that there are no security features in the security target that conflict with the underlying security policy.

Phase 2 - Architectural Design

Requirements for Content and Presentation

E5.5 A semiformal 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.**

Requirements for Evidence

E5.6 The description 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.**

Evaluator Actions

E5.7 Check that the information provided meets all requirements for content and presentation and evidence. Check that the separation of security enforcing and other components is valid.

Phase 3 - Detailed Design

Requirements for Content and Presentation

E5.8 A semiformal 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.

Requirements for Evidence

E5.9 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.

Evaluator Actions

E5.10 Check that the information provided meets all requirements for content and presentation and evidence.

Phase 4 - Implementation

Requirements for Content and Presentation

E5.11 The 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.

Requirements for Evidence

E5.12 The test 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.

Evaluator Actions

E5.13 Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. Check

that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Check all retesting following the correction of errors. Perform additional tests to search for errors.

Construction - The Development Environment

E5.14 The sponsor shall provide the following documentation:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- Audit information on modifications of all objects of the TOE subject to configuration control
- Information on the acceptance procedure
- **Information on the integration procedure**
- Information on the security of the development environment
- Description of all implementation languages and compilers used
- **Source code of all runtime libraries used**

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E5.15 The development 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.**

Requirements for Evidence

E5.16 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. **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.**

Evaluator Actions

E5.17 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. **Check the example audit trail output.** Use the developers tools to create selected parts of the TOE and compare with the submitted version of the TOE.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E5.18 Any 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.**

Requirements for Evidence

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

Evaluator Actions

E5.20 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 3 - Developers Security

Requirements for Content and Presentation

E5.21 The document 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**.

Requirements for Evidence

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

Evaluator Actions

E5.23 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.

Operation - The Operational Documentation

E5.24 The sponsor shall provide the following documentation:

- User documentation

- Administration documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

E5.25 The user 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.

Requirements for Evidence

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

Evaluator Actions

E5.27 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E5.28 The administration 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.

Requirements for Evidence

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

Evaluator Actions

E5.30 Check that the information provided meets all requirements for content and presentation and evidence.

Operation - The Operational Environment

E5.31 The sponsor shall provide the following documentation:

- Delivery and Configuration Documentation
- Start-up and Operation Documentation

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

E5.32 If different 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.

Requirements for Evidence

E5.33 The information supplied shall **explain** how the procedures maintain security.

Evaluator Actions

E5.34 Check that the information provided meets all requirements for content and presentation and evidence. Check the correct application of the delivery procedures. Search for errors in the system generation procedures.

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E5.35 The procedures for secure start-up and operation shall be **explained**. If any security enforcing functions can be deactivated or modified during start-up, 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.

Requirements for Evidence

E5.36 The information 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 start-up and operation.

Evaluator Actions

E5.37 Check that the information provided meets all requirements for content and presentation and evidence. Check the example evidence required for start-up and operation. Search for errors in the procedures.

Construction - The Development Process

E6.1 The sponsor shall provide the TOE, and the following documentation:

- The security target for the TOE
- Definition or reference to an underlying formally specified model of security
- Informal interpretation of the underlying model in terms of the security target
- Formal description of the architecture of the TOE
- Semiformal description of the detailed design
- 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**

Phase 1 - Requirements

Requirements for Content and Presentation

E6.2 The security 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.

Requirements for Evidence

E6.3 In the 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.

Evaluator Actions

E6.4 Check that the information provided meets all requirements for content and presentation and evidence. Check that there are no inconsistencies in the security target. Check that there are no security features in the security target that conflict with the underlying security policy.

Phase 2 - Architectural Design

Requirements for Content and Presentation

E6.5 A **formal** 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.

Requirements for Evidence

E6.6 The description 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.**

Evaluator Actions

E6.7 Check that the information provided meets all requirements for content and presentation and evidence. Check that the separation of security enforcing and other components is valid. **Check that formal arguments are valid.**

Phase 3 - Detailed Design

Requirements for Content and Presentation

E6.8 A semiformal 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.

Requirements for Evidence

E6.9 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.

Evaluator Actions

E6.10 Check that the information provided meets all requirements for content and presentation and evidence.

Phase 4 - Implementation

Requirements for Content and Presentation

E6.11 The 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. **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.

Requirements for Evidence

E6.12 The test 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.

Evaluator Actions

E6.13 Check that the information provided meets all requirements for content and presentation and evidence. Use the library of test programs to check by sampling the results of tests. Check that tests cover all security enforcing functions identified in the security target. Check that the tests cover all security enforcing and security relevant functions identified in the detailed design and all security mechanisms identifiable in the source code or hardware drawings. Check all retesting following the correction of errors. Perform additional tests to search for errors. **Investigate any suspected inconsistencies between source code and executable code found during testing using the sponsor supplied tools.**

Construction - The Development Environment

E6.14 The sponsor shall provide the following documentation:

- Configuration list identifying the version of the TOE for evaluation
- Information on the configuration control system and its tools
- Audit information on modifications of all objects of the TOE subject to configuration control
- Information on the acceptance procedure
- Information on the integration procedure
- Information on the security of the development environment
- Description of all implementation languages and compilers used
- Source code of all runtime libraries used

Aspect 1 - Configuration Control

Requirements for Content and Presentation

E6.15 The development 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.

Requirements for Evidence

E6.16 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. 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.

Evaluator Actions

E6.17 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Check the example audit trail output. Use the developers tools to create selected parts of the TOE and compare with the submitted version of the TOE.

Aspect 2 - Programming Languages and Compilers

Requirements for Content and Presentation

E6.18 Any 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.

Requirements for Evidence

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

Evaluator Actions

E6.20 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 3 - Developers Security

Requirements for Content and Presentation

E6.21 The document 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.

Requirements for Evidence

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

Evaluator Actions

E6.23 Check that the documented procedures are being applied. Check that the information provided meets all requirements for content and presentation and evidence. Search for errors in the procedures.

Operation - The Operational Documentation

E6.24 The sponsor shall provide the following documentation:

- User documentation
- Administration documentation

Aspect 1 - User Documentation

Requirements for Content and Presentation

E6.25 The user 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.

Requirements for Evidence

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

Evaluator Actions

E6.27 Check that the information provided meets all requirements for content and presentation and evidence.

Aspect 2 - Administration Documentation

Requirements for Content and Presentation

E6.28 The administration 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.

Requirements for Evidence

E6.29 The administration documentation shall explain how the TOE is administered in a secure manner.

Evaluator Actions

E6.30 Check that the information provided meets all requirements for content and presentation and evidence.

Operation - The Operational Environment

E6.31 The sponsor shall provide the following documentation:

- Delivery and Configuration Documentation
- Start-up and Operation Documentation

Aspect 1 - Delivery and Configuration

Requirements for Procedures and Standards

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. 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.

Requirements for Evidence

E6.33 The information supplied shall explain how the procedures maintain security.

Evaluator Actions

E6.34 Check that the information provided meets all requirements for content and presentation and evidence. Check the correct application of the delivery procedures. Search for errors in the system generation procedures.

Aspect 2 - Start-up and Operation

Requirements for Procedures and Standards

E6.35 The procedures for secure start-up and operation shall be explained. If any security enforcing functions can be deactivated or modified during start-up, 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.

Requirements for Evidence

E6.36 The information 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 start-up and operation.

Evaluator Actions

E6.37 Check that the information provided meets all requirements for content and presentation and evidence. Check the example evidence required for start-up and operation. Search for errors in the procedures.

5 RESULTS OF EVALUATION

Introduction

5.1 Evaluation of a TOE in accordance with the correctness and effectiveness criteria set out in this document provides a measure of the assurance that the TOE will meet its security target. This is indicated by the evaluation level achieved and a rating for the minimum strength of the security mechanisms of the TOE.

Rating

5.2 The rating awarded to a TOE as the results of evaluation shall consist of the following:

- a reference to the security target for the TOE used as the baseline for evaluation;
- the evaluation level achieved by assessment of correctness and consideration of effectiveness;
- the confirmed rating of the minimum strength of the security mechanisms of the TOE.

5.3 The security target shall be specified in a manner that is suitable for evaluation by an independent body and which is in accordance with the criteria for the stated evaluation level and type of TOE.

5.4 The evaluation level awarded shall only be E0, E1, E2, E3, E4, E5 or E6.

5.5 The confirmed rating of minimum strength shall only be awarded if the TOE has been successfully evaluated, ie. it is not awarded E0. The rating awarded shall only be basic, medium or high.

5.6 A TOE that satisfies all the correctness criteria for its targeted evaluation level and passes all aspects of consideration of effectiveness at that level, including the claimed minimum strength of mechanisms, shall be awarded the rating of that evaluation level and minimum strength of mechanisms.

5.7 A TOE that is found to contain an exploitable vulnerability that has not been eliminated during the course of evaluation shall be withdrawn from evaluation or awarded E0.

5.8 A TOE that fails to provide satisfactory evidence to satisfy the criteria for its targeted evaluation level but where no exploitable vulnerability has been found may be awarded a lower evaluation level where the evidence in question is not required to satisfy the criteria for that level. If there is insufficient time or resources to consider the TOE against that lower level, or if unanswered questions exist, it shall either be withdrawn from evaluation or awarded E0.

5.9 A TOE will only fail evaluation on grounds of effectiveness if an exploitable vulnerability is found and not eliminated. In this case it must be withdrawn from evaluation or awarded E0.

5.10 A TOE assigned a rating of E0 will have no rating for the minimum strength of mechanisms since it has been demonstrated that there is inadequate assurance in the TOE.

5.11 The report produced by the evaluator containing and supporting the evaluation results shall be presented in a form acceptable for consideration by the appropriate national certification body.

6 GLOSSARY AND REFERENCES

Introduction

6.1 This chapter contains definitions of technical terms that are used with a meaning specific to this document. Technical terms used within this document that are not defined here are used throughout the document in a manner consistent with their generally accepted meaning.

Definitions

6.2 Acceptance Procedure: a procedure which takes objects produced during the development, production and maintenance processes for a Target of Evaluation and, as a positive act, places them under the controls of a Configuration Control system.

6.3 **Accreditation**: has two definitions according to circumstances:

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

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

6.4 **Administration Documentation**: the information about a Target of Evaluation supplied by the developer for use by an administrator.

6.5 **Administrator**: a person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.

6.6 **Architectural Design**: a phase of the Development Process wherein the top level definition and design of a Target of Evaluation is specified.

6.7 **Assurance**: the confidence that may be held in the security provided by a Target of Evaluation.

6.8 **Assurance Profile**: an assurance requirement for a TOE whereby different levels of confidence are required in different security enforcing

functions.

6.9 **Availability**: the prevention of the unauthorised withholding of information or resources. 6.10 Basic Component: a component that is identifiable at the lowest hierarchical level of specification produced during Detailed Design.

6.11 **Binding of Functionality**: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security enforcing functions and mechanisms to work together in a way which is mutually supportive and provides an integrated and effective whole.

6.12 **Certification**: the issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were correctly applied.

6.13 **Certification Body**: an independent and impartial national organisation that performs certification.

6.14 **Component**: an identifiable and self-contained portion of a Target of Evaluation.

6.15 **Confidentiality**: the prevention of the unauthorised disclosure of information.

6.16 **Configuration**: the selection of one of the sets of possible combinations of features of a Target of Evaluation.

6.17 **Configuration Control**: a system of controls imposed on changing controlled objects produced during the development, production and maintenance processes for a Target of Evaluation.

6.18 **Construction**: the process of creating a Target of Evaluation.

6.19 **Corporate Security Policy**: the set of laws, rules and practices that regulate how assets including sensitive information are managed, protected and distributed within a user organisation.

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

6.21 **Covert Channel**: the use of a mechanism not intended for communication to transfer information in a way which violates security.

6.22 **Critical Mechanism**: a mechanism within a Target of Evaluation whose failure would create a security weakness.

6.23 **Customer**: the person or organisation that purchases a Target of Evaluation.

6.24 **Delivery**: the process whereby a copy of the Target of Evaluation is transferred from the developer to a customer.

6.25 **Detailed Design**: a phase of the Development Process wherein the top level definition and design of a Target of Evaluation is refined and expanded to a level of detail that can be used as a basis for implementation.

6.26 **Developer**: the person or organisation that manufactures a Target of Evaluation.

6.27 **Developer Security**: the physical, procedural and personnel security controls imposed by a developer on his Development Environment.

6.28 **Development Environment**: the organisational measures, procedures and standards used whilst constructing a Target of Evaluation.

6.29 **Development Process**: The set of phases and tasks whereby a Target of Evaluation is constructed, translating requirements into actual hardware and software.

6.30 **Documentation**: the written (or otherwise recorded) information about a Target of Evaluation required for an evaluation. This information may, but need not, be contained within a single document produced for the specified purpose.

6.31 **Ease of Use**: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely that it cannot be configured or used in a manner which is insecure but which an administrator or end-user would reasonably believe to be secure.

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

6.33 **End-user**: a person in contact with a Target of Evaluation who

makes use only of its operational capability.

6.34 **Evaluation**: the assessment of an IT system or product against defined evaluation criteria.

6.35 **Evaluator**: the independent person or organisation that performs an evaluation.

6.36 **Evaluator Actions**: a component of the evaluation criteria for a particular phase or aspect of evaluation, identifying what the evaluator must do to check the information supplied by the sponsor of the evaluator, and the additional activities he must perform.

6.37 **Formal Model of Security Policy**: an underlying model of security policy expressed in a formal style, i.e. an abstract statement of the important principles of security that a TOE will enforce.

6.38 **Functional Unit**: a functionally distinct part of a basic component.

6.39 **Functionality Class**: a predefined set of complementary security enforcing functions capable of being implemented in a Target of Evaluation.

6.40 **Implementation**: a phase of the Development Process wherein the detailed specification of a Target of Evaluation is translated into actual hardware and software.

6.41 **Integrity**: the prevention of the unauthorised modification of information.

6.42 **Object**: a passive entity that contains or receives information.

6.43 **Operating Procedure**: a set of rules defining correct use of a Target of Evaluation.

6.44 **Operation**: the process of using a Target of Evaluation.

6.45 **Operational Documentation**: the information produced by the developer of a Target of Evaluation to specify and explain how customers should use it.

6.46 **Operational Environment**: the organisational measures, procedures

and standards to be used whilst operating a Target of Evaluation.

6.47 **Penetration Testing**: tests performed by an evaluator on the Target of Evaluation in order to confirm whether or not known vulnerabilities are actually exploitable in practice.

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

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

6.50 **Production**: the process whereby copies of the Target of Evaluation are generated for distribution to customers.

6.51 **Programming Languages and Compilers**: the tools used within the Development Environment in the construction of the software and/or firmware of a Target of Evaluation.

6.52 **Rating**: a measure for the assurance that may be held in a Target of Evaluation, consisting of a reference to its security target, an evaluation level established by assessment of the correctness of its implementation and consideration of its effectiveness in the context of actual or proposed operational use, and a confirmed rating of the minimum strength of its security mechanisms.

6.53 **Requirements**: a phase of the Development Process wherein the security target of a Target of Evaluation is produced.

6.54 **Requirements for Content and Presentation**: a component of the evaluation criteria for a particular phase or aspect of evaluation identifying what each item of documentation identified as relevant to that phase or aspect of evaluation shall contain and how its information is to be presented.

6.55 **Requirements for Evidence**: a component of the evaluation criteria for a particular phase or aspect of evaluation defining the nature of the evidence to show that the criteria for that phase or aspect have been satisfied.

6.56 **Requirements for Procedures and Standards**: a component of the evaluation criteria for a particular phase or aspect of evaluation identifying the nature and/or content of procedures or standard approaches

that shall be adopted or utilised when the TOE is placed into live operation.

6.57 **Security**: the combination of confidentiality, integrity and availability.

6.58 **Security Enforcing**: that which directly contributes to satisfying the security objectives of the Target of Evaluation.

6.59 **Security Mechanism**: the logic or algorithm that implements a particular security enforcing or security relevant function in hardware and software.

6.60 **Security Objectives**: the contribution to security which a Target of Evaluation is intended to achieve.

6.61 **Security Policy**: see Corporate Security Policy, System Security Policy, Technical Security Policy.

6.62 **Security Relevant**: that which is not security enforcing, but must function correctly for the Target of Evaluation to enforce security.

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

6.64 **Sponsor**: the person or organisation that requests an evaluation.

6.65 **Storage Object**: an object that supports both read and write accesses [TCSEC].

6.66 **Strength of Mechanisms**: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely the ability of its security mechanisms to withstand direct attack against deficiencies in their underlying algorithms, principles and properties.

6.67 **Subject**: an active entity, generally in the form of a person, process, or device [TCSEC].

6.68 **Suitability of Functionality**: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely the suitability of its security enforcing functions and mechanisms to in fact counter the threats to the security of the Target of Evaluation identified in its security target.

6.69 **System**: a specific IT installation, with a particular purpose and operational environment.

6.70 **System Security Policy**: the set of laws, rules and practices that regulate how sensitive information and other resources are managed, protected and distributed within a specific system.

6.71 **Target of Evaluation**: an IT system or product which is subjected to security evaluation.

6.72 **Technical Security Policy**: the set of laws, rules and practices regulating the processing of sensitive information and the use of resources by the hardware and software of an IT system or product.

6.73 **Threat**: an action or event that might prejudice security.

6.74 **Tool**: a product used in the construction and/or documentation of a Target of Evaluation.

6.75 **User Documentation**: the information about a Target of Evaluation supplied by the developer for use by its end-users.

6.76 **Vulnerability**: a security weakness in a Target Of Evaluation (for example, due to failures in analysis, design, implementation or operation).

6.77 **Vulnerability Assessment**: an aspect of the assessment of the effectiveness of a Target of Evaluation, namely whether known vulnerabilities in that Target of Evaluation could in practice compromise its security as specified in the security target.

References

6.78 The following books and papers are referenced in the text:

AND Computer Security Technology Planning Study
J. P. Anderson
ESD-TR-73-51, ESD/AFSC, US Air Force, Bedford, Mass., October 1972.

BLP Secure Computer Systems: Unified Exposition and Multics Interpretation
D.E. Bell and L.J. LaPadula
Report MTR-2997 Rev. 1, MITRE Corporation, Bedford, Mass, 1976.

BNM The Chinese Wall Security Policy
D.F.C. Brewer and M.J. Nash
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, May 1989, pp. 206-214.

CESG3 UK Systems Security Confidence Levels, CESG Memorandum No. 3,
Communications-Electronics Security Group, United Kingdom, January 1989.

CWM A Comparison of Commercial and Military Computer Security Policies
D. D. Clark and D. R. Wilson
Proceedings of the IEEE Symposium on Security and Privacy, Oakland, April 1987, pp. 184-194.

DTIEC DTI Commercial Computer Security Centre Evaluation Levels Manual,
V22
Department of Trade and Industry, United Kingdom, February 1989.

DTIFN DTI Commercial Computer Security Centre Security Functionality
Manual, V21
Department of Trade and Industry, United Kingdom, February 1989. EZBM Mandatory Policy: Secure Systems Model
G. Eizenberg
ONERA/CERT/DERI, Toulouse, France, undated.

GYPSY Report on Gypsy 2.05
D.I. Good, R.L. Akers and L.M. Smith
Report ICSCA-CMP-48, University of Texas at Austin, February 1986.

IJRM The Ina Jo Specification Language Reference Manual
Unisys Corporation
Culver City, California, United States of America, 1989.

JSD System Development
M.A. Jackson
Prentice-Hall International, 1983.

JSP Principles of Program Design
M.A. Jackson
Academic Press, New York, 1975

LOTOS Information Processing Systems - Open Systems Interconnection -
LOTOS - A Formal Description Technique Based on the Temporal
Ordering of Observational Behaviour
International Standard ISO 8807
International Organization for Standardization, 1989.

LWM A Security Model for Military Message Systems
C.E. Landwehr, C.L. Heitmeyer and J. McLean
ACM Transactions on Computer Systems, Vol. 2 No. 3, August 1984,
pp.\198D222.

OSI Information Processing Systems - Open Systems Interconnection -
Basic Reference Model - Part 2: Security Architecture
International Standard ISO 7498-2
International Organization for Standardization, 1988.

RSL RAISE Specification Language Reference Manual,
RAISE/CRI/DOC/2/V1
Computer Resources International A/S
Birkermd, Denmark, 1990.

SADT An Introduction to SADT
Structured Analysis and Design Technique
Report 9022-78R
SofTech Inc, 460 Totten Pond Road
Waltham, MA 02154, USA, November 1976.

SCSSI Catalogue de Criteres Destines a evaluer le Degre de Confiance
des Systemes d'Information, 692/SGDN/DISSI/SCSSI
Service Central de la Securite des Systemes d'Information,

Juillet 1989.

SSADM The SSADM Manual, ISBN 085-012-527-X
National Computing Centre Limited
Manchester, United Kingdom, 1989.

SSVDM Systematic Software Development Using VDM
C.B. Jones
Prentice Hall International, 1990.

TCSEC Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD,
Department of Defense, United States of America, December 1985.

YSM A Note on the Yourdon Structured Method
A.J. Bowles
Yourdon Inc
ACM SIGSOFT Software Engineering Notes
Vol. 15 No. 2 April 1990, p. 27.

ZRM The Z Notation: A Reference Manual, ISBN-0-13-983768-X
J.M. Spivey
Prentice Hall International, 1988.

ZSIEC Criteria for the Evaluation of Trustworthiness of Information
Technology (IT) Systems, ISBN 3-88784-200-6
German Information Security Agency (Bundesamt fur Sicherheit in
der Informationstechnik), Federal Republic of Germany, January
1989.

Annex A - EXAMPLE FUNCTIONALITY CLASSES

Introduction

A.1 This annex sets out example predefined functionality classes, as evaluations. It is hoped that they will stimulate debate on actual security functionality requirements. Indeed, the need to create definitive predefined functionality classes attracted widespread agreement during the consultative process preceding the publication of this version of the criteria.

A.2 Work is already underway in standardisation bodies and other industry organisations to develop standards for security functionality in specific contexts. It is anticipated that such work will produce authoritative definitions of security functionality that can be adapted for use with these criteria and included in or referenced by the next definitive version of this document.

A.3 The present examples provide a basic point of reference and show how predefined functionality classes can be evolved from existing criteria: indeed, these classes have been adapted with minimal alteration from [ZSIEC].

A.4 Each class consists of a statement of objectives, followed by the requirements presented under appropriate generic headings. Absence of a generic heading within the description of a class means that no requirements exist for that heading. The classes F-B2 and F-B3 also contain other information necessary for inclusion as part of a security target; this specifies the mandatory mechanisms required for compatibility with the TCSEC.

A.5 The five example functionality classes F-C1, F-C2, F-B1, F-B2, and F-B form a hierarchy, since they have been derived from the functionality requirements of the hierarchical TCSEC classes. In the description of these classes, those parts of each class which are new or have changed from the preceding class are printed in bold.

A.6 Other hierarchy-based functionality classes may be created in the future, by standardisation bodies and industry organisations, to address other types of security objectives (e.g. for integrity and availability). In the interim, the example classes F-IN, F-AV, F-DI, F-DC, and F-DX have been

ncluded to illustrate the broad range of security requirements that can be
xpressed in the form of a predefined functionality class.

xample Functionality Class F-C1

bjective

.7 Example class F-C1 is derived from the functionality requirements of
he US TCSEC class C1. It provides discretionary (need-to-know) access
ontrol.

dentification and Authentication

.8 The TOE shall identify and authenticate users. This identification ar
uthentication shall take place prior to all other interactions between the TO
nd the user. Other interactions shall only be possible after successful
dentification and authentication. The authentication information shall be
tored in such a way that it can only be accessed by authorised users.

ccess Control

.9 The TOE shall be able to distinguish and administer access rights
etween each user and the objects which are subject to the administration of
ights, on the basis of an individual user, or on the basis of membership of a
roup of users, or both. It shall be possible to completely deny users or use
roups access to an object. It shall not be possible for anyone who is not ar
uthorised user to grant or revoke access rights to an object.

.10 With each attempt by users or user groups to access objects which are
ubject to the administration of rights, the TOE shall verify the validity of
he request. Unauthorised access attempts shall be rejected.

xample Functionality Class F-C2

bjective

.11 **Example class F-C2 is derived from the functionality requirements of
he US TCSEC class C2. It provides a more finely grained discretionary access**

control than class C1, making users individually accountable for their actions through identification procedures, auditing of security relevant events, and resource isolation.

Identification and Authentication

A.12 The TOE shall **uniquely** identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed by authorised users. **For every interaction the TOE shall be able to establish the identity of the user.**

Access Control

A.13 The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of rights, on the basis of an individual user, or on the basis of membership of a group of users, or both. It shall be possible to completely deny users or user groups access to an object. **It shall also be possible to restrict a user's access to an object to those operations which do not modify it. It shall be possible to grant the access rights to an object down to the granularity of an individual user.** It shall not be possible for anyone who is not an authorised user to grant or revoke access rights to an object. **The administration of rights shall provide controls to limit propagation of access rights. In the same way, only authorised users shall be able to introduce new users or delete or suspend existing users.**

A.14 With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected.

Accountability

A.15 **The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:**

a) Use of the identification and authentication mechanism:

Required data: Date; time; user identity supplied; identification of the equipment on which the identification and authentication mechanism was used (e.g. terminal-id); success or failure of the attempt.

b) Actions that attempt to exercise access rights to an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt.

c) Creation or deletion of an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of action.

d) Actions by authorised users affecting the security of the TOE:

Required data: Date; time; user identity; type of action; name of the object to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE).

\.16 Unauthorised users shall not be permitted to access accountability data. It shall be possible to selectively account for the actions of one or more users. Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

\udit

\.17 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

)bject Reuse

A.18 **All storage objects returned to the TOE shall be treated before reuse by other subjects, in such a way that no conclusions can be drawn regarding th preceding content.**

Example Functionality Class F-B1

Objective

A.19 **Example class F-B1 is derived from the functionality requirements of the US TCSEC class B1. In addition to discretionary access control it introduces functions to maintain sensitivity labels and uses them to enforce a set of mandatory access control rules over all subjects and storage objects under its control. It is possible to accurately label exported information.**

Identification and Authentication

A.20 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed by authorised users. For every interaction the TOE shall be able to establish the identity of the user.

Access Control

A.21 The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of rights, on the basis of an individual user, or on the basis of membership of a group of users, or both. It shall be possible to completely deny users or use groups access to an object. It shall also be possible to restrict a user's access to an object to those operations which do not modify it. It shall be possible to grant the access rights to an object down to the granularity of an individual user. It shall not be possible for anyone who is not an authorised user to grant or revoke access rights to an object. The administration of rights shall provide controls to limit propagation of access rights. The actions for adding and deleting user identities known to the TOE, and the

action to temporarily suspend all of a user's access rights, shall be restricted to authorised users.

A.22 **In addition the TOE shall provide all subjects and storage objects (e.g. processes, files, storage segments, devices) under its control with attributes. The values of these attributes shall serve as a basis for mandatory access rights. Rules shall specify which combinations of attribute values of subject and object are necessary for a subject to be granted access to that object.**

A.23 **When exporting an object its attributes shall be exported in such a wa that the recipient can reconstruct their value unambiguously.**

A.24 **The mandatory access rights shall be designed in such a manner that th following special case can be realised:**

The attribute consists of two parts. Part one has hierarchically ordered values, part two represents a set. (In the official world part one contains classifications e.g. unclassified, confidential, secret, top secret. Part two contains categories.)

An attribute A is said to dominate an attribute B if:

Part one of A is hierarchically greater than, or equal to, part one of B and part two of B is a proper subset of, or equal to, part two of A.

A.25 **The following rules shall be enforced:**

a) Read access by a subject to an object is only permitted if the attribute of the subject dominates that of the object.

b) Write access by a subject to an object is only permitted if the attribute of the object dominates that of the subject.

A.26 **The attributes of a subject created to act on behalf of a user shall b dominated by that user's clearance and authorisation as determined at identification and authentication time. If imported data does not have attributes, an authorised user shall be able to assign attributes to the data.**

A.27 **Each export channel shall be identifiable as either single-level or multi-level. It shall be impossible to transmit or receive data via channels designated as single-level, unless the attributes of that data match a fixed prespecified attribute. Data transmitted to or received from a single-level channel shall be communicated with a corresponding attribute, unless it is possible for an authorised user to specify the attribute of the channel in a**

way that cannot be imitated. In this case, the attribute of the data is implicitly specified by the attribute of the channel.

A.28 **For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes.**

A.29 **Unauthorised users shall not be able to change the security relevant attributes of a channel. It shall not be possible to change these attributes without the change being performed explicitly.**

A.30 **The TOE shall mark human readable output with attribute values. The values of the attributes shall be determined according to the rules laid down in the TOE. Authorised users shall be able to specify the printable name of each attribute value.**

A.31 With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected. **The values of the attributes shall serve as the basis for decisions concerning mandatory access control. The rules shall unambiguously specify when a subject is allowed access to such a protected object. If discretionary access rights are also assigned for an object, access shall only be permitted provided that both the discretionary and the mandatory access rights allow such access.**

Accountability

A.32 The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:

a) Use of the identification and authentication mechanism:

Required data: Date; time; user identity supplied; identification of the equipment on which the identification and authentication mechanism was used (e.g. terminal-id); success or failure of the attempt; **authorisation of the user**.

b) Actions that attempt to exercise access rights to an object

which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt; **attribute of the object**.

c) Creation or deletion of an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of action; **attribute of the object**.

d) Actions by authorised users affecting the security of the TOE:

Required data: Date; time; user identity; type of action; name and **attribute of the object** to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE; **assignation of an attribute; change of attributes, markings or classification of a channel).**

.33 Unauthorised users shall not be permitted to access accountability data. It shall be possible to selectively account for the actions of one or more users. Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

udit

.34 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

bject Reuse

.35 All storage objects returned to the TOE shall be treated before reuse by other subjects, in such a way that no conclusions can be drawn regarding th preceding content.

xample Functionality Class F-B2

Objective

A.36 **Example class F-B2 is derived from the functionality requirements of the US TCSEC class B2. It extends mandatory access control to all subjects and objects and strengthens the authentication requirements of class B1.**

Mandatory Mechanisms

A.37 **This class requires access control to be implemented by a single reference validation mechanism that implements the reference monitor concept, i.e. that the mechanism is tamperproof, always invoked, and small enough (of sufficiently simple organisation and complexity) to be subjected to analysis and tests, the completeness of which can be assured.**

Identification and Authentication

A.38 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed by authorised users. **Identification and authentication shall be handled via a trusted path between user and TOE initialised by the user.** For every interaction the TOE shall be able to establish the identity of the user.

Access Control

A.39 The TOE shall be able to distinguish and administer access rights between each user and the objects which are subject to the administration of rights, on the basis of an individual user, or on the basis of membership of a group of users, or both. **It shall be possible to group access rights to support roles. As a minimum the roles of TOE operator and administrator shall be definable.** It shall be possible to completely deny users or user groups access to an object. It shall also be possible to restrict a user's access to an object to those operations which do not modify it. It shall be possible to grant the access rights to an object down to the granularity of an individual user.

A.40 It shall not be possible for anyone who is not an authorised user to

grant or revoke access rights to an object. The administration of rights shal
provide controls to limit propagation of access rights. The actions for addir
and deleting user identities known to the TOE, and the action to temporarily
suspend all of a user's access rights, shall be restricted to authorised users

A.41 In addition the TOE shall provide all subjects and **objects** (e.g. processes, files, storage segments, devices) **with** attributes. The values of these attributes shall serve as a basis for mandatory access rights. Rules shall specify which combinations of attribute values of subject and object are necessary for a subject to be granted access to that object.

A.42 When exporting an object its attributes shall be exported in such a wa that the recipient can reconstruct their value unambiguously.

A.43 The mandatory access rights shall be designed in such a manner that th following special case can be realised:

> The attribute consists of two parts. Part one has hierarchically ordered values, part two represents a set. (In the official world part one contains classifications e.g. unclassified, confidential, secret, top secret. Part two contains categories.)
>
> An attribute A is said to dominate an attribute B if:
>
> Part one of A is hierarchically greater than, or equal to, part one of and part two of B is a proper subset of, or equal to, part two of A.

A.44 The following rules shall be enforced:

> a) Read access by a subject to an object is only permitted if the attribute of the subject dominates that of the object.
>
> b) Write access by a subject to an object is only permitted if the attribute of the object dominates that of the subject.

A.45 The attributes of a subject created to act on behalf of a user shall b dominated by that user's clearance and authorisation as determined at identification and authentication time. If imported data does not have attributes, an authorised user shall be able to assign attributes to the data.

A.46 Each export channel shall be identifiable as either single-level or multi-level. It shall be impossible to transmit or receive data via channels designated as single-level, unless the attributes of that data match a fixed prespecified attribute. Data transmitted to or received from a single-level channel shall be communicated with a corresponding attribute, unless it is

possible for an authorised user to specify the attribute of the channel in a way that cannot be imitated. In this case, the attribute of the data is implicitly specified by the attribute of the channel.

A.47 For multi-level channels it shall be ensured by the communication protocol that the recipient can completely and unambiguously reconstruct and pair the received data and attributes. **For multi-level channels it shall be possible to state the maximum and minimum attributes. No data shall be transmitted to a multi-level channel unless the attribute of the data dominate the minimum attribute of the channel and is dominated by the maximum attribute of the channel.**

A.48 Unauthorised users shall not be able to change the security relevant attributes of a channel. It shall not be possible to change these attributes without the change being performed explicitly.

A.49 The TOE shall mark human readable output with attribute values. The values of the attributes shall be determined according to the rules laid down in the TOE. Authorised users shall be able to specify the printable name of each attribute value.

A.50 **A user shall be notified immediately of any change in the security level associated with that user during an interactive session. The user shall be able at all times to review all the subject's attributes.**

A.51 With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected. The values of the attributes shall serve as the basis for decisions concerning mandatory access control. The rules shall unambiguously specify when a subject is allowed access to such a protected object. If discretionary access rights are also assigned for an object, access shall only be permitted provided that both the discretionary and the mandatory access rights allow such access.

A.52 **There shall be no known storage channels that can transfer information between processes without verification of access rights (i.e. covertly) that have a maximum bandwidth (determined by actual measurement or engineering estimation) that is unacceptably high. (See the Covert Channel Guideline section of the TCSEC [TCSEC] for guidance on acceptability.)**

Accountability

A.53 The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:

a) Use of the identification and authentication mechanism:

Required data: Date; time; user identity supplied; identification of the equipment on which the identification and authentication mechanism was used (e.g. terminal-id); success or failure of the attempt; authorisation of the user.

b) Actions that attempt to exercise access rights to an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt; attribute of the object.

c) Creation or deletion of an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of action; attribute of the object.

d) Actions by authorised users affecting the security of the TOE:

Required data: Date; time; user identity; type of action; name and attribute of the object to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE; assignation of an attribute; change of attributes, markings or classification of a channel).

A.54 Unauthorised users shall not be permitted to access accountability data. It shall be possible to selectively account for the actions of one or more users. Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

Audit

A.55 Tools to examine the accountability files for the purpose of audit

shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively. **In addition the TOE shall be able to audit known events which could be misused to allow an unauthorised flow of information by exploiting covert channels.**

Object Reuse

A.56 All storage objects returned to the TOE shall be treated before reuse by other subjects, in such a way that no conclusions can be drawn regarding the preceding content.

Example Functionality Class F-B3

Objective

A.57 **Example class F-B3 is derived from the functionality requirements of the US TCSEC classes B3 and A1. In addition to the functions of class B2, it provides functions to support distinct security administration roles, and audit is expanded to signal security relevant events.**

Mandatory Mechanisms

A.58 This class requires access control to be implemented by a single reference validation mechanism that implements the reference monitor concept, i.e. that the mechanism is tamperproof, always invoked, and small enough (of sufficiently simple organisation and complexity) to be subjected to analysis and tests, the completeness of which can be assured.

Identification and Authentication

A.59 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed by authorised users. Identification and authentication shall be handled via a trusted path between user and TOE initialised by the user **or by**

he TOE. For every interaction the TOE shall be able to establish the identit
f the user.

ccess Control

.60 The TOE shall be able to distinguish and administer access rights
etween each user and the objects which are subject to the administration of
ights, on the basis of an individual user, or on the basis of membership of a
roup of users, or both. It shall be possible to group access rights to
upport roles. As a minimum the roles of TOE operator and administrator shall
e definable. **The roles of the TOE operator, TOE administrator and TOE
ecurity officer shall be separated**. It shall be possible to completely deny
sers or user groups access to an object. It shall also be possible to
estrict a user's access to an object to those operations which do not modify
t. It shall be possible to grant the access rights to an object down to the
ranularity of an individual user. It shall not be possible for anyone who is
ot an authorised user to grant or revoke access rights to an object.

.61 **For each object which is subject to the administration of rights, it
hall be possible to supply a list of users and a list of user groups with
heir associated rights to this object. In addition, for each such object it
hall also be possible to supply a list of users and a list of user groups who
re denied access to this object**. The administration of rights shall provide
ontrols to limit propagation of access rights. The actions for adding and
eleting user identities known to the TOE, and the action to temporarily
uspend all of a user's access rights, shall be restricted to authorised users

.62 In addition the TOE shall provide all subjects and objects (e.g.
rocesses, files, storage segments, devices) with attributes. The values of
hese attributes shall serve as a basis for mandatory access rights. Rules
hall specify which combinations of attribute values of subject and object are
ecessary for a subject to be granted access to that object.

.63 When exporting an object its attributes shall be exported in such a wa
hat the recipient can reconstruct their value unambiguously.

.64 The mandatory access rights shall be designed in such a manner that th
ollowing special case can be realised:

The attribute consists of two parts. Part one has hierarchically
rdered values, part two represents a set. (In the official world part one
ontains classifications e.g. unclassified, confidential, secret, top secret.
art two contains categories.)

An attribute A is said to dominate an attribute B if:

Part one of A is hierarchically greater than, or equal to, part one of B and part two of B is a proper subset of, or equal to, part two of A.

.65 The following rules shall be enforced:

a) Read access by a subject to an object is only permitted if the attribute of the subject dominates that of the object.

b) Write access by a subject to an object is only permitted if the attribute of the object dominates that of the subject.

.66 The attributes of a subject created to act on behalf of a user shall b dominated by that user's clearance and authorisation as determined at identification and authentication time. If imported data does not have ttributes, an authorised user shall be able to assign attributes to the data.

.67 Each export channel shall be identifiable as either single-level or ulti-level. It shall be impossible to transmit or receive data via channels lesignated as single-level, unless the attributes of that data match a fixed rrespecified attribute. Data transmitted to or received from a single-level channel shall be communicated with a corresponding attribute, unless it is ossible for an authorised user to specify the attribute of the channel in a ay that cannot be imitated. In this case, the attribute of the data is mplicitly specified by the attribute of the channel.

.68 For multi-level channels it shall be ensured by the communication rotocol that the recipient can completely and unambiguously reconstruct and air the received data and attributes. For multi-level channels it shall be ossible to state the maximum and minimum attributes. No data shall be ransmitted to a multi-level channel unless the attribute of the data dominate he minimum attribute of the channel and is dominated by the maximum attribute f the channel.

.69 Unauthorised users shall not be able to change the security relevant ttributes of a channel. It shall not be possible to change these attributes ithout the change being performed explicitly.

.70 The TOE shall mark human readable output with attribute values. The alues of the attributes shall be determined according to the rules laid down n the TOE. Authorised users shall be able to specify the printable name of

each attribute value.

A.71 A user shall be notified immediately of any change in the security level associated with that user during an interactive session. The user shall be able at all times to review all the subject's attributes.

A.72 With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of the request. Unauthorised access attempts shall be rejected. The values of the attributes shall serve as the basis for decisions concerning mandatory access control. The rules shall unambiguously specify when a subject is allowed access to such a protected object. If discretionary access rights are also assigned for an object, access shall only be permitted provided that both the discretionary and the mandatory access rights allow such access.

A.73 There shall be no known storage **or timing** channels that can transfer information between processes without verification of access rights (i.e. covertly) that have a maximum bandwidth (determined by actual measurement or engineering estimation) that is unacceptably high. (See the Covert Channel Guideline section of the TCSEC [TCSEC] for guidance on acceptability.)

Accountability

A.74 The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:

a) Use of the identification and authentication mechanism:

Required data: Date; time; user identity supplied; identification of the equipment on which the identification and authentication mechanism was used (e.g. terminal-id); success or failure of the attempt; authorisation of the user.

b) Actions that attempt to exercise access rights to an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt; attribute of the object.

c) Creation or deletion of an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of action; attribute of the object.

d) Actions by authorised users affecting the security of the TOE:

Required data: Date; time; user identity; type of action; name and attribute of the object to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE; assignation of an attribute; change of attributes, markings or classification of a channel).

.75 Unauthorised users shall not be permitted to access accountability data. It shall be possible to selectively account for the actions of one or more users. Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

udit

.76 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively. In addition the TOE shall be able to audit known events which could be misused to allow an unauthorised flow of information by exploiting covert channels.

.77 **Additionally, there shall be a mechanism to monitor the occurrence of events which are either particularly security relevant or which, due to the frequency of their occurrence, can become a critical threat to the security of the TOE. This mechanism shall be able without delay to notify a special user, or a user with a special role, of the occurrence of such events. The mechanis shall take the least disruptive action to terminate such events.**

bject Reuse

.78 All storage objects returned to the TOE shall be treated before reuse by other subjects, in such a way that no conclusions can be drawn regarding th preceding content.

Example Functionality Class F-IN

Objective

A.79 Example functionality class F-IN is for TOEs with high integrity requirements for data and programs. Such requirements may be necessary in database TOEs, for example.

Identification and Authentication

A.80 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed for review or modification by authorised users. For every interactio the TOE shall be able to establish the identity of the user.

Access Control

A.81 The TOE shall be able to distinguish and administer access rights of users, roles and processes to explicitly designated objects. (Roles denote users with special attributes). It shall be possible to restrict access by users to these objects in such a manner that this access is only possible via specially established processes. In addition, it shall be possible to allocat objects to a predefined type. It shall be possible to specify for each type o object which users, roles or processes can possess certain access types to these objects. This should make it possible to restrict user access to object of a certain type in such a manner that this access is only possible via fixed established processes. It should only be possible for authorised users to define new types or to grant or revoke access rights to types. These actions shall be initiated explicitly by this user. For these actions all communication between the TOE and the user shall be via a trusted path.

A.82 The following minimum access rights shall exist: read, write, add, delete, rename (for all objects), execute, delete, rename (for executable objects), creation of objects of a certain type, deletion of objects of a certain type.

A.83 With each attempt by users or user groups to access objects which are subject to the administration of rights, the TOE shall verify the validity of

:his access attempt. Unauthorised access attempts shall be rejected.

\ccountability

\.84 The TOE shall contain an accountability component which is able, for :ach of the following events, to log that event together with the required lata:

ı) Use of the identification and authentication mechanism:

Required data: Date; time; user identity supplied; identification of the equipment on which the identification and authentication mechanism was used (e.g. terminal-id); success or failure of the attempt.

ı) Actions that attempt to exercise access rights to an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of access attempt; success or failure of the attempt.

:) Creation or deletion of an object which is subject to the administration of rights:

Required data: Date; time; user identity; name of the object; type of action.

l) Actions by authorised users affecting the security of the TOE:

Required data: Date; time; user identity; type of action; name and attribute of the object to which the action relates (such actions are introduction or deletion (suspension) of users; introduction or removal of storage media; start up or shut down of the TOE).

:) Definition or deletion of types:

Required data: Date; time; user identity; type of action; name of the type.

:) Assignation of a type to an object:

Required data: Date; time; user identity; name of the object; name

of the type.

l) Granting or revocation of access rights for an object or an object type:

Required data: Date; time; user identity; type of action; type of access right; name of the subject; name of the object or name of the object type.

.85 Unauthorised users shall not be permitted to access accountability lata. It shall be possible to selectively account for the actions of one or ore users. Tools to examine and to maintain the accountability files shall xist and be documented. These tools shall allow the actions of one or more sers to be identified selectively. The structure of the accountability ecords shall be described completely.

udit

.86 Tools to examine the accountability files for the purpose of audit hall exist and be documented. These tools shall allow the actions of one or ore users to be identified selectively.

xample Functionality Class F-AV

bjective

.87 Functionality class F-AV sets high requirements for the availability c complete TOE or special functions of a TOE. Such requirements are ignificant for TOEs that control manufacturing processes, for example.

eliability of Service

.88 The TOE shall be able to recover from a failure of certain individual ardware components (e.g. a board of an individual processor in a ultiprocessor TOE) in such a manner that all constantly required functions emain continuously available in the remaining TOE. After the failed componer as been repaired, it shall be possible to reintegrate it into the TOE in such way that the continuous operation of constantly required functions is ssured. Following the integration the TOE shall achieve its original degree

of tolerance against TOE failures. Maximum times shall be stated for the duration of such a reintegration process.

A.89 Irrespective of its load at any time, the TOE shall be able to guarantee a maximum response time for certain specified actions. In addition, for certain specified actions, it shall be guaranteed that the TOE will not be subject to deadlock.

Example Functionality Class F-DI

Objective

A.90 Example functionality class F-DI sets high requirements with regard to the safeguarding of data integrity during data exchange.

Identification and Authentication

A.91 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The authentication information shall be stored in such a way that it can only be accessed for review or modification by authorised users. For every interactio the TOE shall be able to establish the identity of the user.

A.92 Prior to the establishment of a connection the peer entity (computer, process or user) shall be uniquely identified and authenticated. User data shall only be exchanged after identification and authentication have been successfully completed. On receipt of data it shall be possible to uniquely identify and authenticate the sender of the data. All authentication information shall be protected against unauthorised access and forgery.

Accountability

A.93 The TOE shall contain an accountability component which is able, for each of the following events, to log that event together with the required data:

a) Use of the identification and authentication mechanism:

Required data: Date; time; initiator of the identification and authentication; name of the subject to be identified; success or failure of the action.

b) Identified errors in the data exchange:

Required data: Date; time; peer entity in the data exchange; nature of the error; success or failure of the attempted correction.

c) Data Exchange:

Required data: Date; time; user identity of the initiator; name of the peer entity (computer, process or user); parameters of the establishment of the connection (if these vary).

.94 Unauthorised users shall not be permitted to access accountability data. It shall be possible to selectively account for the actions of one or more users. Tools to examine and to maintain the accountability files shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively. The structure of the accountability records shall be described completely.

udit

.95 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

ata Exchange

ata Integrity

.96 Methods for error detection and error correction shall be applied in the case of data exchange. These mechanisms shall be designed in such a way that intentional manipulations of the address fields and user data can be identified. Knowledge only of the algorithms applied in the mechanisms without any special additional knowledge shall not enable unrecognised manipulations of the aforementioned data. The additional knowledge required for this shall be protected in such a manner that it can only be accessed by a few authorised users.

A.97 Moreover, mechanisms shall be used which reliably uniquely identify as an error the unauthorised replay of data.

Example Functionality Class F-DC

Objective

A.98 Example functionality Class F-DC is intended for TOEs with high demand on the confidentiality of data during data exchange. An example candidate for this class is a cryptographic device.

Data Exchange

Data Confidentiality

A.99 The TOE shall have a facility to encrypt user information prior to exchange and (at the receiving end) to decrypt it automatically. An algorithm officially approved by a certification authority shall be applied. It shall be assured that the parameter values (e.g. keys) required for decrypting are protected in such a manner that no unauthorised person can access this data.

Example Functionality Class F-DX

Objective

A.100 Example functionality class F-DX is intended for networks with high demands on the confidentiality and integrity of the information to be exchanged. For example, this can be the case when sensitive information has to be exchanged via insecure (for example: public) networks.

Identification and Authentication

A.101 The TOE shall uniquely identify and authenticate users. This identification and authentication shall take place prior to all other interactions between the TOE and the user. Other interactions shall only be possible after successful identification and authentication. The

uthentication information shall be stored in such a way that it can only be ccessed for review or modification by authorised users. For every interactic he TOE shall be able to establish the identity of the user.

.102 Prior to the exchange of user data the peer entity (computer, process r user) shall be uniquely identified and authenticated. User data shall only e exchanged after identification and authentication have been successfully ompleted. On receipt of data it shall be possible to uniquely identify and uthenticate the sender of the data. All authentication information shall be rotected against unauthorised access and forgery.

ccountability

.103 The TOE shall contain an accountability component which is able, for ach of the following events, to log that event together with the required lata:

a) Use of the identification and authentication mechanism:

Required data: Date; time; initiator of the identification and authentication; name of the subject to be identified; success or failure of the action.

b) Identified errors in the data exchange:

Required data: Date; time; peers in the data exchange; type of the error; success or failure of the attempted correction.

c) Connection establishment:

Required data: Date; time; user identity of the initiator; name of the peer entity (computer, process or user); establishment parameters (if these vary).

d) Special data exchange transactions:

Required data: Date; time; user identity of the transmitter; user identity of the recipient; user information communicated; date and time of the receipt of the data.

.104 Unauthorised users shall not be permitted to access accountability lata. It shall be possible to selectively account for the actions of one or ore users. Tools to examine and to maintain the accountability files shall xist and be documented. These tools shall allow the actions of one or more

users to be identified selectively. The structure of the accountability records shall be described completely.

Audit

A.105 Tools to examine the accountability files for the purpose of audit shall exist and be documented. These tools shall allow the actions of one or more users to be identified selectively.

Data Exchange

Access Control

A.106 All information previously transmitted which can be used for unauthorised decryption shall be protected in such a way that only such persons who positively need such access in order to be able to perform their duties can access this data.

Data Confidentiality

A.107 The TOE shall offer the possibility of end-to-end encryption which ensures confidentiality regarding the recipient over large sections of the communication channel. In addition, traffic flow confidentiality shall also be guaranteed on designated data communication links.

Data Integrity

A.108 The TOE shall be designed in such a way that unauthorised manipulation of user data and accountability data and unauthorised replay of data are reliably identified as errors.

ex B - THE CLAIMS LANGUAGE

roduction

Within the context of the IT security evaluation criteria it is helpful have a means of describing the claimed security functions provided by an IT urity product in semiformal style, but still expressed using natural guage. The Claims Language defined in this Annex was developed to meet that uirement.

The benefits of using the Claims Language to specify security ctionality are that:

a) it provides a semiformal style of specification, but because it is based on natural language, it can be read and understood without special knowledge of a notation or set of rules;

b) it indicates the necessary linking and grouping of claims;

c) it reduces the scope for ambiguity in the interpretation of the claims;

d) it enables the claims for a TOE to be expressed in a way that is suited to the process of evaluation.

The Claims Language facilitates controlled extension of the predefined ation to handle concepts for which no suitable elements exist. Within a ims Document, normal natural language can be used to describe mechanisms and umptions if a more formal approach is not necessary. The Claims Language is ficiently flexible to allow any set of claims peculiar to a specialised TOE be defined without any departure from the rules of the language; thus nsors of an evaluation are not in any way constrained to make their claims the language.

rview

Using the Claims Language, security functions are expressed using a set rules for generating Action Phrase Templates, each of which provides the

mework for a particular type of claim. Each Action Phrase Template is then bined with one of a set of Target Phrases to create an outline claim. Nouns phrases specific to the product, the function and/or the vendor are then stituted into the outline claim to create a real claim. An example of the eration of a claim will be found in paragraphs B.30 to B.34 of this Annex.

As part of the statement of a claim it is possible to include a erence to the mechanism that implements the claim.

It is permissible to omit or modify the linking words used in outline ims in order to improve the readability or grammatical accuracy of claims.

Examples of permissible changes are:

a) substituting the plural for the singular, or vice versa;

b) inserting or removing the definite and indefinite articles;

c) changing prepositions.

It is permissible to introduce new action or target phrases where no sting phrases are appropriate, provided that such phrases have been discussed h and approved by the Certification Body.

A standard layout shall be used for Claims Documents containing Claims guage claims, as set out in paragraphs B.38 to B.44 of this Annex. Claims ll be grouped under a standardised headings based on the Generic Headings for ctionality. This aids understanding and facilitates comparison with other s.

nings

0 Care should be taken when formulating claims which are configuration endent. It may be possible to configure a TOE in ways which are insecure e. some of the claims are invalidated). If this is the case, restrictions to lude such insecure options or combinations of options should be stated as ironmental constraints (see paragraph B.41 of this Annex onwards).

1 Care should also be take to formulate claims at an appropriate level of nularity. If a proposed claim seems to encompass several Generic Headings, requires more substitutions than are possible using the appropriate template, n the claim is at too high a level and needs to be broken down into a series

simpler claims.

ion Phrase Templates

2 Action Phrase Templates shall be generated from the framework below, h italics indicating words or phrases in the template to be replaced by cific claim-related substitutions in an actual claim, with [] indicating ional parts, and <> indicating selection of an option from the relevant list options following:

This TOE [<qualifier>] <verb> <action> ... [<time>] [using the mechanism defined in paragraph n].

Where <qualifier> may be:

contains a *function* that
or must be used in an environment that

and <verb> may be:

will
or will not
or can be configured to
or can be configured to not
or cannot be configured to

and <action> may be:

establish
or detect
or control
or permit
or prevent
or ensure
or record in *object*

and <time> may be:

before *security-relevant-event*
or after *security-relevant-event.*

3 The environment option of <qualifier> is only used in defining ironmental constraints where great precision is required.

4 Where details of specific mechanisms form part of the security target, y shall be defined as part of the Claims Document through a linked mechanism ecification paragraph. If no such link is included, details of the mechanism not form part of the security target and will be treated as proprietary ormation. The function option of <qualifier> is optional. It is used to e the particular product mechanism that implements a particular claim. This e is included purely for explanatory purposes.

5 Some example Action Phrase templates are:

This product will ensure ...

This product contains an audit utility that will establish ...

This product can be configured to permit ...

This product must be used in an environment that will prevent ...

This add-in board will record in its audit trail ...

This product will prevent ... before completion of secure startup.

get Phrases

6 The permitted set of Target Phrases is as follows, with [] indicating ional parts of the phrase:

... *audit-information* concerning *security-relevant-events*

... the identity of a *process* requested

... the identity of the {user,process} requesting a *process*

... the identity of the *{user,process}* requesting *access-type* to an *object*

... the identity of a *process* executed

... the rejection of a *process* request

... the identity of an *object* to which *access-type* was requested

... the identity of an *object* to which *access-type* was granted

... the identity of an *object* to which *access-type* was refused

... the *access-set* of a *user*

... the *access-set* of a *process*

... the *access-set* of a *{user,process}*

... the *access-set* of an *object*

... the *access-type* granted to a *{user,process}* in respect of an *object*

... *access-type* by *{user,process}* in respect of an *object*

... the actions performed by a *{user,process}* in respect of an *object*

... the *factors* affecting the *access-set* of a *user*

... the *factors* affecting the *access-set* of a *process*

... the *factors* affecting the *access-set* of a *{user,process}*

... the *factors* affecting the *access-set* of an *object*

... clearing of information from an *object*

... the *security-attributes* of an *object*

... the correctness of the *security-attributes* of an *object*

... the *security-attributes* of an *object* formed by combining a number of *objects*

... the *security-attributes* of a set of *objects* formed by partitioning a single *object*

... the granting of *access-type* to an *object* cannot cause deadlock

through *{user,process}es* using *access-type* to *objects*

... the *{user,process}es* using *access-type* to an *object* which has caused deadlock

... the granting of *access-type* to an *object* cannot cause livelock through *{user,process}es* using *access-type* to *objects*

... the *{user,process}es* using *access-type* to an *object* which has caused livelock

... *security-attribute* of *object* is identical to that of *object*

... *claim* [not] to become time-critical

... *claim* [not] to become accelerated or delayed

... *claim* [not] to become time-dependent

... *claim* [not] to be by-passed

... *claim* [not] to be deactivated

... *claim* [not] to be corrupted

stitutions

7 Substitutions shall be made for the following nouns/phrases *(italicised the Action Phrase Templates and Target Phrases above):-*

access-set; access-type; audit-information; claim; factors; ction; n; object; product; process; security-attribute; security- evant-event; user; {user,process}

8 All substitutions shall be explained using natural language, either in a arate section of the Claims Document (see paragraph B.39 of this Annex), or ediately following the claim where the substitution is used.

9 Some examples of possible substitutions are:-

ess-set	replaced by	read/write access to I/O ports
ess-type	replaced by	read permission
ess-type	replaced by	read/write/delete permission
it-information	replaced by	date and time

```
it-information              replaced by     terminal number
im                          replaced by     (a cross-reference to another
im)
tors                replaced by     number of incorrect responses
ction                       replaced by     password system
                            replaced by     (a paragraph number)
ect                         replaced by     file
ect                         replaced by     resource control block
ject                        replaced by     hard disc storage (i.e. a type
object)
                            replaced by     operating system
                            replaced by     PC security board
cess                replaced by     unprivileged task
urity-attribute             replaced by     integrity of data
urity-attribute             replaced by     actual destination
urity-attribute             replaced by     apparent source
urity-relevant-event        replaced by     attempted privilege violations
urity-relevant-event        replaced by     user logoff
urity-relevant-event        replaced by     change of security level
r                           replaced by     data entry clerk
r                           replaced by     security administrator
er,process}                  replaced by     job (i.e. implying any user)
```

0 There are parts of the Action Phrases and Target Phrases which are in are brackets []; these are optional words or phrases which may be included omitted as appropriate to the vendor's claim.

1 Most noun and phrase substitutions are straightforward. However, some ticular conventions exist and are explained below.

2 The definition of an access-set depends on whether it is related to:-

a) an object; in which case it represents the list of users, processes and {user,process}es, each with an associated access-type, able to use an object.

b) a process or a user or a {user,process}; in which case it represents the list of objects, each with an associated access-type, available to a user, a process or a {user,process}.

3 Thus, access-set is a (notional) list of all the objects a user can ess, together with what he can do to each one and via which processes, or a

tional) list of all the users who can access an object, via which processes what they can do to it.

4 Access-type is the series of ways of using an object and is vendor-ined. Typical examples of these are create, read, write, delete, execute or ombination of these or none.

5 As a specific example the set could be defined as:

a) "Amend" allows a record to be updated but does not allow new records to be added to the file.

b) "Create" allows new records to be added to the file but does not allow existing ones to be changed.

d) "Delete" allows records to be removed from the file.

e) "Execute" allows the file to be loaded into memory and then scheduled for running as a program.

f) "Read" allows data in records to be copied to working storage.

6 Many objects will possess identical security attributes. Thus if a im will apply to all objects of a particular type the substitution will ally be best expressed in terms of the type of object, rather than by listing possible objects of that type.

hanisms

7 As part of a claim it is possible to include a description of the hanism used to implement that claim. This is done through the "using" option the claim's Action Phrase Template, by giving a reference to a paragraph in Claims Document that specifies and/or explains the mechanism employed. luation will then include confirmation that the stated mechanism is the hanism used.

8 Any appropriate method may be used to define or describe the mechanism, vided that the explanation is sufficient for evaluation to determine at the el of confidence corresponding to the targeted Evaluation Level:

a) the claimed mechanism is present in the product;

b) its operation matches the claimed specification;

c) it is the mechanism actually used to implement the claim.

9 In many cases it may be easier and clearer to define a mechanism by erence to a published standard, or give a table of types of inputs and the responding results, rather than providing details of the algorithm employed ng either natural language or a specification or programming language.

mple

0 As an example, the following Action Phrase Template may be generated ng the rules specified:

This *TOE* will establish ...

where the word in italics can be replaced by a specific term.

1 Similarly, a Target Phrase may be selected such as:

... the identity of an *object* to which *access-type* was requested.

2 Putting these together gives:

This *TOE* will establish the identity of an *object* to which *access-type* was requested.

into which some possible substitutions are:

add-in security board for *TOE*
any file for *object*
write or delete permission for *access-type*

3 Thus a complete claim could be:

This add-in security board will establish the identity of any file to ch write or delete permission was requested.

4 Obviously this example is extremely artificial. In practice for real s highly specific claims are made, often related to a particular real or umed environment.

ims Document Structure

of Generic Headings for Functionality

5 Claims shall be grouped under the Generic Headings set out in Chapter 2 these criteria. Not all TOEs will make claims under all headings; where re are no claims made for a particular heading this shall be stated. Claims ll be included for any events or actions that are to be prevented.

6 Table B.1 identifies Target Phrases which will often appear under ticular Generic Headings. The table is intended for use as a general guide y; the flexibility of the Claims Language means that often other Target ases will also be appropriate.

7 Table B.2 cross-references Target Phrases to the possible substitutions y contain.

out of Claims Documents

8 A security target using the Claims Language shall be set out using the lowing structure:

a) the security objectives of the target including any constraints or assumptions concerning the real or assumed environment of the TOE, set out as a Product Rationale (or in the case of a system, a System Security Policy);

b) an informal specification of the claims in natural language, or a reference to another document containing that informal specification (this may be a reference to a functionality class defined in informal style), and a correlation of these informal claims to the security objectives;

c) global substitutions;

d) claims under each Generic Heading in turn;

e) details of security mechanisms;

f) the claimed rating of the minimum strength of mechanisms;

g) the target evaluation level.

9 Under the Global Substitutions heading any general substitutions used in Action or Target Phrases of more than one claim shall be defined and lained.

0 These substitutions shall be overridden where different (usually more cific) substitutions are given as part of particular claims.

1 If the TOE relies upon properties of its real or assumed environment in er for it to function correctly, these shall be specified in the rationale or icy section of the Claims Document. Evaluation will assume that these straints/assumptions will hold in actual use.

2 Each such constraint/assumption shall be expressed either in natural guage or in the Claims Language (using the Action Phrase environment lifier). Where ambiguity exists (because natural language has been used) the luators will interpret such constraints/assumptions in a way that is sistent with other assumptions or claims.

3 Some claims may remain valid even if a particular assertion is not true. ere this is the case, natural language shall be used to indicate which claims ain true when that assertion fails.

4 An example of an assertion (expressed in natural language) is:

> The RAM backup battery must not be removed from the security board or allowed to discharge below its minimum operating voltage.

mat of Individual Claims

5 Each substitution in the Action or Target phrases used to form a claim ch is not identified and defined in the global substitutions section of the ims Document must be defined and expressed in natural language immediately lowing the claim where it appears.

Table B.1 Claims Target Phrases and Generic Headings

Authentication	Identification and	Access Control	Accountability	Audit	Object Re	Accura

Reliability of Service							
	|	|	|	|	|	|	|
Data Exchange							
	|	|	|	|	|	|	|
1 Audit information	X	X	X	X	X	X	X
2 Identity of process requested	X	X	X	X			X
3 Identity of {u,p} requesting a process	X	X	X	X			X
4 Identity of {u,p} requesting an object	X	X	X	X			X
5 Identity of process executed	X	X	X	X			X
6 Rejection of process request	X	X	X	X			X
7 Identity of object requested	X	X	X	X			X
8 Identity of object granted	X	X	X	X		X	X
9 Identity of object refused	X	X	X	X			X
10 Access-set of user		X					X
11 Access-set of process		X					X
12 Access-set of {u,p}		X					X
13 Access-set of object		X					X
14 Object access granted to {u,p}	X	X	X	X			
	X						
15 Object access by {u,p}	X	X	X	X			
	X						
16 Object actions performed by {u,p}		X	X	X			
	X						
17 Factors affecting user access-set		X					X
18 Factors affecting process access-set		X					X
19 Factors affecting {u,p} access-set		X					X
20 Factors affecting object access-set		X					X
21 Clearing information from object					X		X
22 Security-attributes of object	X	X	X	X	X	X	X
23 Correctness of security-attributes of object						X	

X									
24	Security-attributes of combination object		X				X		
X									
25	Security-attributes of partitioned object		X				X		
X									
26	Granting access causes no deadlock						X		
X									
27	Deadlock can be detected						X		
X									
28	Granting access causes no livelock						X		
X									
29	Livelock can be detected						X		
X									
30	Objects have identical security-attributes		X				X		
X									
31	Time-critical claim								X
32	Accelerated or delayed claim								X
33	Time-dependent claim								X
34	By-pass claim	X	X	X	X	X	X	X	
35	Deactivate claim	X	X	X	X	X	X	X	
36	Corrupt claim	X	X	X	X	X	X	X	

Table B.2 Claims Target Phrases and Permitted Substitutions

	access-set	access-type	audit-information	claim	object	proce	security-attribute	security-relevant-event	user	{user,process}
1 Audit information			X							
2 Identity of process requested						X				
3 Identity of {u,p} requesting a process						X				
4 Identity of {u,p} requesting an object		X		X						
5 Identity of process executed						X				
6 Rejection of process request						X				
7 Identity of object requested		X		X						
8 Identity of object granted		X		X						
9 Identity of object refused		X		X						
10 Access-set of user	X									
11 Access-set of process	X					X				
12 Access-set of {u,p}	X									
13 Access-set of object	X			X						
14 Object access granted to {u,p}		X		X						
15 Object access by {u,p}		X		X						
16 Object actions performed by {u,p}				X						
17 Factors affecting user access-set	X									

				X				
18	Factors affecting process access-set			X			X	
19	Factors affecting {u,p} access-set			X				
					X			
20	Factors affecting object access-set			X		X		
21	Clearing information from object					X		
22	Security-attributes of object					X		X
23	Correctness of security-attributes of object					X		X
24	Security-attributes of combination object					X		X
25	Security-attributes of partitioned object					X		X
26	Granting access causes no deadlock				X	X		
					X			
27	Deadlock can be detected				X	X		
					X			
28	Granting access causes no livelock				X	X		
					X			
29	Livelock can be detected				X	X		
					X			
30	Objects have identical security-attributes					X		X
31	Time-critical claim						X	
32	Accelerated or delayed claim						X	
33	Time-dependent claim						X	
34	By-pass claim						X	
35	Deactivate claim						X	
36	Corrupt claim						X	

This page left blank