Copy No.

Doc Ref	**7163/T/2**
Client	**Icelandic Data Protection Commission**
Project	**Icelandic Health Database**
Title	**Approval Process Methodology**
Date	**January 2000**

Review & Approval

Issue:	1.3
R&A Number:	7163/RA/6
Originator:	
Clair Groom	
Approval (PM):	
Gary Smith	
Approval (QAR):	
Paul Morrison	

Admiral Management Services Limited
Kings Court
91-93 High Street
Camberley
Surrey GU15 3RN
Tel: (01276) 686678
Fax: (01276) 685205

Contents

1 Introduction

1.1 Background
1.2 Scope
1.3 Structure
1.4 Abbreviations
1.5 References

2 Introduction to Evaluation

2.1 The Icelandic Health Database
2.2 Potential Security Threats to the Health Database
2.3 Making the Health Database Secure
2.4 Gaining Assurance in the Health Database
2.5 IT Security Evaluation Criteria and Evaluation
2.6 The Common Criteria
2.7 Use of Pre-evaluated Systems and Products
2.8 Conclusion

3 Roles and Responsibilities

3.1 Introduction
3.2 Approval Board - Data Protection Commission (DPC)
3.3 Operating License Holder
3.4 Evaluation Facility
3.5 Flow of Deliverables Between Participants
3.6 Impartiality, Integrity and Commercial Confidentiality
3.7 Natural Language for deliverables and Evaluation Reports
3.8 Appeals Procedure

4 Security Evaluation

4.1 Introduction
4.2 Stage 1 - Preparation for Evaluation
4.3 Stage 2 - Perform Evaluation
4.4 Stage 3 - Collate Results into an Evaluation Technical Report
4.5 Stage 4 - Review Evaluation Technical Report /Production of an Approval Report
4.6 Stage 5 - Closedown of Evaluation

5 The Approval Process

5.1 Introduction
5.2 Role of the Approval Board
5.3 Approval Report

Annexes

A Glossary

B Documentation Road-map

1 Introduction

1.1 Background

1.1.1 It has been determined that independent and impartial assessment is required of the security functionality implemented by the planned Health Database in Iceland. This independent and impartial assessment will take the form of one or more security evaluations performed against the Common Criteria in accordance with the [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3].

1.1.2 The methodology by which the evaluation will be performed and the procedures that will be followed, are defined within this document.

1.1.3 Successful completion of evaluation will be a condition for operation of a health centre database, and for the additional permissions required to link the database with external data sources.

1.2 Scope

This methodology is applicable for Common Criteria evaluation assurance levels EAL1 to EAL4.

1.3 Structure

The Approval Process methodology (this document) is structured as follows:

a) Chapter 1 (this chapter) - Introduction

b) Chapter 2 - Introduction to Evaluation

c) Chapter 3 - Roles and Responsibilities

d) Chapter 4 - Description of Security Evaluation

e) Chapter 5 - Description of the Approval Process

f) Annex A - summary of the terminology used within this document, together with a list of abbreviations

g) Annex B - road-map to the [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3].

1.4 Abbreviations

Annex A of [CCEM] and Section 3.1 of [CC Part 1] provides a list of the common abbreviations used within the Common Criteria. However, Table A3.1 below provides a list of the abbreviations used within this document.

Table 2.1 - Abbreviations	
CC	Common Criteria
CLEF	CommerciaL Evaluation Facility
DPC	Data Protection Committee
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IHD	Icelandic Health Database
ISO	International Standards Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
MCHSD	Monitoring Committee on the Health Sector Database
MRA	Mutual Recognition Agreement
OLH	Operating License Holder
UK	United Kingdom

1.5 References

[Act] Act on a Health Sector Database, Icelandic Parliament, No. 139/1998

[CCEM]: Common Methodology for Information Technology Security Evaluation, CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

[CC Part 1]: ISO/IEC 15408-1:1999(E) Information Technology - Security Techniques – Evaluation Criteria for IT Security Part 1: Introduction and general model, dated 18 December 1998

[CC Part 2]: ISO/IEC 15408-2:1999(E) Information Technology - Security Techniques – Evaluation Criteria for IT Security Part 2: Security functional requirements, dated 18 December 1998

[CC Part 3]: ISO/IEC 15408-3:1999(E) Information Technology - Security Techniques – Evaluation Criteria for IT Security Part 3: Security assurance requirements, dated 18 December 1998

[MRA] Arrangement on the Mutual Recognition of Common Criteria Certificates the Field of Information Technology, dated 5 October 1998.

2 Introduction to Evaluation

2.1 The Icelandic Health Database

2.1.1 The IHD is a computer database that stores medical data according to [Act]. If the necessary permissions are obtained from the DPC, the database can be correlated with external data sources on genealogy and genetics. The database will be used for medical and genetic research, into areas such as:

a) the relationship between genetics and disease

b) the effectiveness of treatments

c) cost-efficiency studies.

2.1.2 The Health Database will be used by OLH staff only. They will interrogate the database on behalf of external organisations such as universities and pharmaceutical companies, as well as Icelandic government departments responsible for health care. They will be given access to statistical information only.

2.2 Potential Security Threats to the Health Database

2.2.1 The Health Database stores a large quantity of health information about individuals. Some of this information is highly sensitive and could cause financial damage or embarrassment to the individuals concerned if it were unintentionally or deliberately disclosed.

2.2.2 Potentially, sensitive information is at risk at any of the following stages:

a) during preparation and conversion

b) while stored within the Health Database

c) while being accessed for the purposes of research.

2.2.3 The last risk category includes the possibility of researchers accidentally or deliberately inferring something about a named person on the basis of statistical queries. Such attacks are known to be possible in some cases, and devising countermeasures to them is a complex and difficult process.

2.3 Making the Health Database Secure

2.3.1 In order to gain and keep its role, the OLH must show that the information entrusted to it is kept securely.

2.3.2 How this is implemented will be decided by the OLH, but the security measures employed should include the following:

a) user authentication - ensure users of the Health Database are properly authenticated so that it is not possible to impersonate another user

b) audit - keep records of what each user does so that he/she can be held responsible for his/her actions

c) access control - ensure that each user is only allowed to see what he is authorised to see

d) encryption - scramble data so that it cannot be used without proper authorisation

e) statistical controls - design the user interface so that personal information cannot be inferred from the information returned.

2.3.3 This implies a sizeable development program to put the necessary infrastructure in place, and to manage it afterwards.

2.3.4 The Icelandic Data Protection Committee (DPC) is tasked with ensuring that personal data in the IHD is properly protected. It must be satisfied that appropriate security mechanisms are in place.

2.3.5 Once the license has been granted, another committee, the MCHSD, will monitor the creation and use of the IHD, in so far is this does not fall within the ambit of the DPC. The MCHSD will operate in conjunction with ethics committees set up under [Act].

2.4 Gaining Assurance in the Health Database

2.4.1 The security of the Health Database depends upon a great many factors such as the security of its design, the implementation methods adopted, the off-the-shelf products used and how they will be configured, and the rigour of testing.

2.4.2 All these have to meet an appropriate standard, and must provide the functionality required for security. A professional judgement must be made taking all of these dependencies into account.

2.4.3 Unfortunately, it is difficult for an organisation such as the DPC to make this judgement on its own behalf. Analysing the security of a large, complex, innovative system such as the Health Database requires specialist skills that a Government body such as the DPC cannot be expected to have. In addition, developers are generally unwilling to release sufficiently detailed design information, as this would be useful to both attackers and competitors.

2.4.4 On the other hand, many people will be unwilling merely to trust the developer's (i.e. the OLH's) word that their Health Database is secure. Those involved in developing and marketing the system will be seen as having an interest in its success and are therefore unlikely to bring attention to any security defects it may have.

2.4.5 The way round these problems is for an independent third party to evaluate the security of the proposed system and then to report its findings. The report can be:

a) expressed in language that the intelligent layman can understand

b) edited so that it does not contain sensitive information.

2.4.6 Clearly, the third party must have the necessary expertise and has to be trusted to do a thorough evaluation, and not to misuse the information it is given. This will be achieved by having the third party supervised by the DPC.

2.5 IT Security Evaluation Criteria and Evaluation

2.5.1 The methods used by the independent third party need to be standardised so that they can be interpreted, and so that the results of different evaluations can be compared. There is also a need for the required inputs and the work performed during the evaluation to be specified in some way so that the parties involved can estimate the cost, and feasibility, of the evaluation before it starts.

2.5.2 This need is met by defining evaluation criteria. Evaluation criteria define what the developer must produce and what the evaluator must do, to achieve the required degree of assurance. An evaluation criterion has to strike a balance between cost, feasibility and the eventual assurance gained.

2.5.3 A number of evaluation criteria have been defined in the past. Most of these are recognised only by particular countries or regions. The Common Criteria, however, were developed by a world-wide consortium of nations and are now recognised as an

ISO standard (no. 15408). The Common Criteria are also the most modern set of criteria. For this reason, the Common Criteria have been selected as the standard against which the Health Database will be assessed.

2.5.4 The UK Government operates a scheme to provide an independent third party that can perform security evaluations of systems and products under the Common Criteria.

2.5.5 The UK Scheme consists of:

a) Several CommerciaL Evaluation Facilities (CLEFs). These are commercial independent third party organisations which perform analysis and testing of those systems and products undergoing evaluation.

b) A Certification Body. This is a Government department which oversees the evaluation work of the CLEFs.

2.5.6 Each evaluation has a developer who designs and implements a particular product or system and a sponsor, that pays for the evaluation work to be performed.

2.5.7 For the case of the Health Database, it is proposed that the evaluation be performed by an approved CLEF, supervised by the DPC. The DPC will take the place of a certification body.

2.6 The Common Criteria

2.6.1 Introduction

2.6.1.1 The Common Criteria is segmented into four documents the [CCEM], [CC Part 1], [CC Part 2] and the [CC Part 3]. A full road-map showing the structure of each of these documents can be found in Annex B.

2.6.1.2 The [CCEM] defines the evaluation methodology to be adopted during a Common Criteria evaluation and describes the minimum actions which need to be performed by an evaluator.

2.6.1.3 The [CC Part 1] provides an introduction and general model for Common Criteria evaluations, from the Common Criteria approach to performing evaluations through to the specification of Security Targets.

2.6.1.4 A Common Criteria evaluation is performed against a baseline called a ‘Security Target’. The Security Target acts as a baseline for the evaluation and describes the security requirements in the product or system under evaluation. The evaluators verify that the security requirements defined in this baseline are adequate to counter the threats and that the security requirements are correctly implemented and mutually supportive. They also monitor important aspects, such as testing and configuration management of the development environment.

2.6.1.5 Within a Common Criteria evaluation there are two types of security requirements which must be defined within a Security Target, functional requirements and assurance requirements.

2.6.2 Functional Requirements

2.6.2.1 When developing a system, a developer must consider the potential threats to the operating environment in which their system operates. Within the Security Target, a set of functional requirements must be defined to counter these threats that are seen to pose a risk to the system. [CC Part 2] contains a catalogue of functional requirements which developers can use when defining their Security Target.

2.6.3 Assurance Requirements

2.6.3.1 The Common Criteria defines 7 ‘assurance levels’, EAL1 through to EAL7, which define graduated levels of analysis and testing. Table 2.1 summarises each of the Common Criteria Assurance Levels.

Table 2.1 - Common Criteria Assurance Levels	
EAL1 and EAL2	Concentrate on ‘black box’ testing and user guidance documents
EAL3	Adds a requirement for examining the design and the development environment
EAL4	Adds a requirement to examine source code and has additional requirements for testing and for the development environment
EAL5	Adds a requirement for mathematical specification of the security features
EAL6	Requires rigorous structural discipline in the design
EAL7	Requires mathematical proof of the design.

2.6.3.2 For each assurance level, the Common Criteria defines a default set of assurance requirements which must be achieved. The definition of which default assurance requirements are applicable for each of the assurance levels EAL1 through to EAL4 is defined in [CC Part 3].

2.6.3.3 In addition to the default requirements for each assurance level, additional assurance requirements may be specified within a Security Target. If these assurance requirements are defined within [CC Part 3] they are said to “augment” the default assurance level requirements. If however, these additional assurance requirements are not defined within [CC Part 3] they are said to “extend” the default assurance level requirements.

2.7 Use of Pre-evaluated Systems and Products

2.7.1 The predecessor to the Common Criteria was called the Information Technology Security Evaluation Criteria (ITSEC). The ITSEC provided criteria for the evaluation of the products or systems and defined seven assurance levels E0 through to E6 which equate to the Common Criteria assurance levels as summarised in Table 2.2.

Table 2.2 - Relationship Between Common Criteria and the ITSEC	
Common Criteria Assurance Level	**ITSEC Assurance Level**
EAL1	E0
EAL2	E1
EAL3	E2
EAL4	E3
EAL5	E4
EAL6	E5
EAL7	E6

2.7.2 Where a system uses products, it will be unnecessary for the evaluators and developers to perform evaluation activities specific to products satisfying the following conditions:

a) the products used within the system have been previously evaluated and approved against either the Common Criteria or ITSEC

b) the products have been evaluated and approved under a recognised evaluation scheme (where recognised evaluation schemes are those participating in the Mutual Recognition Agreement [MRA])

c) the products have been evaluated to either an equivalent or higher assurance level than the intended assurance level of the system.

2.7.3 For example, suppose the assurance level for the Health Database is selected as EAL3. Then where the Health Database uses products pre-certified to the Common Criteria EAL3, ITSEC E2 or above, by a recognised evaluation scheme, the following need not be performed during the Health Database evaluation:

a) any evaluator actions in respect to the internals of these components

b) any developer testing in respect of these components.

2.7.4 Many security related products, such as operating systems and firewalls, have been evaluated using the Common Criteria or the ITSEC. Most evaluations are performed to the Common Criteria assurance levels EAL3 and EAL4 or to the ITSEC assurance level E3.

2.7.5 Documentation deliverables for pre-certified components will, however, still be required.

2.8 Conclusion

2.8.1 As a condition of being granted an operating license for its Health Database, the potential OLH must submit its system for evaluation by an independent third party.

2.8.2 The evaluation will be performed under the Common Criteria, an ISO standard. A ‘Security Target’ will be produced, describing the claimed security requirements, the threats the system is subject to and the environment within which the Health Database will operate.

2.8.3 The rest of this document describes the methodology by which the formal evaluation will be performed (the Approval Process) and the procedures that will be followed, including the responsibilities of the parties involved, the stages of the evaluation, and the outputs produced.

3 Roles and Responsibilities

3.1 Introduction

3.1.1 This Chapter introduces the principal participants in the Approval Process for security evaluation and describes their roles and responsibilities.

3.1.2 The principal participants in an evaluation are the:

a) Approval Board

b) OLH

c) the Evaluation Facility chosen by the DPC.

3.1.3 The following paragraphs describe the responsibilities undertaken by each participant.

3.2 Approval Board - Data Protection Commission (DPC)

3.2.1 The DPC is charged by law with various duties concerning the protection of public and private interests in relation to the systematic registration and other handling of personal data, by computer or otherwise. It ensures requisite control over the compilation, use and dissemination of such data. Its basic role is to monitor the execution of the Act of 121/1989.

3.2.2 These duties include several tasks assigned to the DPC by [Act], which permits the creation of a centralised IHD containing health data, pursuant to an operating license to be granted by the Minister of Health and subject to various stringent requirements. Such tasks relate to both the conditions for initial licensing and development of the IHD and the monitoring of its operation and use.

3.2.3 The assignment below relates to the implementation of Article 5 of [Act], by which the DPC is charged with the task of establishing the technical, security and organisational standards and parameters applicable to the IHD, with particular view to the protection of personal data, and specifying the requirements to be met by the OLH as a condition of granting an operational license.

3.2.4 As part of this responsibility, the DPC shall act as the Approval Board during the security evaluation of the Health Database.

3.2.5 The responsibilities of the Approval Board with respect to evaluation are as follows:

a) to oversee the work of the Evaluation Facility and monitor their compliance with the conditions of the Approval Process

b) to produce (or approve) a Security Target for the IHD which defines the:

   i) security requirements for the IHD
   ii) threats the system may be subject to
   iii) environment within which the IHD will operate
   iv) sampling strategy to be adopted by the Evaluation Facility during the evaluation

c) to register and approve the results of evaluations conducted under the Approval Process

d) to approve press releases and similar statements relating to the Approval Process and the security of the IHD

e) to produce an Approval Report if satisfied that the IHD has met the requirements of the Common Criteria at the selected assurance level.

3.3 OLH

3.3.1 The OLH is responsible for developing, testing and operating the Health Database. With respect to the Common Criteria as defined within [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3] the OLH performs the role of both the Developer and Sponsor.

3.3.2 The responsibilities of the OLH are as follows:

a) to produce a Health Database which is compliant with the Security Target produced/approved by the Approval Board

b) to meet all requests from the Approval Board and Evaluation Facility for information and support during evaluation and the Approval Process

c) to seek approval from the Approval Board for any press releases regarding the status of the evaluation and security status of the Health Database

d) during the course of the evaluation to:
   i) inform the Evaluation Facility when any document delivered to it becomes obsolete
   ii) provide answers to questions posed by the Evaluation Facility or Approval Board
   iii) provide timely resolutions to any Observation Reports raised

e) to provide the Evaluation Facility with a timetable of when deliverables required in support of the evaluation will be supplied to the Evaluation Facility and to provide deliverables in accordance with this agreed timetable

f) to provide the Evaluation Facility access to their development site

g) to provide the Evaluation Facility with an operational version of the Health Database

h) to provide technical support to the Evaluation Facility during the evaluation

i) not to distribute Observation Reports and the Evaluation Technical Report to other parties without the permission of the Approval Board

j) to review the conclusions and recommendations in the Evaluation Technical Report.

3.4 Evaluation Facility

3.4.1 The objective of the evaluation process is to enable an independent third party to prepare an impartial report stating whether or not the Health Database satisfies its Security Target at the level of assurance required.

3.4.2 The Evaluation Facility acts as this “independent third party” during the Approval Process. The Evaluation Facility will appoint a number of personnel called evaluators who will be responsible for performing the evaluation against the agreed Common Criteria assurance level. During the course of the evaluation, the role of the evaluators is to perform the actions defined in the Chapter 4 and to report the results of the work performed to the Approval Board.

3.4.3 The evaluators shall preserve their independence at all times during the evaluation.

3.4.4 To ensure suitable operating procedures are adhered to, the Evaluation Facility chosen is required to be licensed to operate as a CommerciaL Evaluation Facility (CLEF).

3.4.5 The responsibilities of the Evaluation Facility include the following:

a) to perform the actions defined in the Common Criteria for the required assurance level and to report the results within an Evaluation Technical Report

b) to issue the Evaluation Technical Report to both the Approval Board and OLH

c) to assign suitable personnel from within their organisation to act as evaluators during the course of the evaluation

d) during the course of the evaluation:
   i) to perform day to day management of the evaluation
   ii) to remain independent from the development of the Health Database

e) to produce Observation Reports to report to the OLH and the Approval Board where either the documentation supplied in support of the evaluation or the implementation of the Health Database does not meet the requirements of the Common Criteria at the required assurance level.

3.5 Flow of Deliverables Between Participants

Figure 3.1 illustrates the flow of deliverables between the participants during the evaluation. More information on each of these deliverables can be found in Chapter 4.

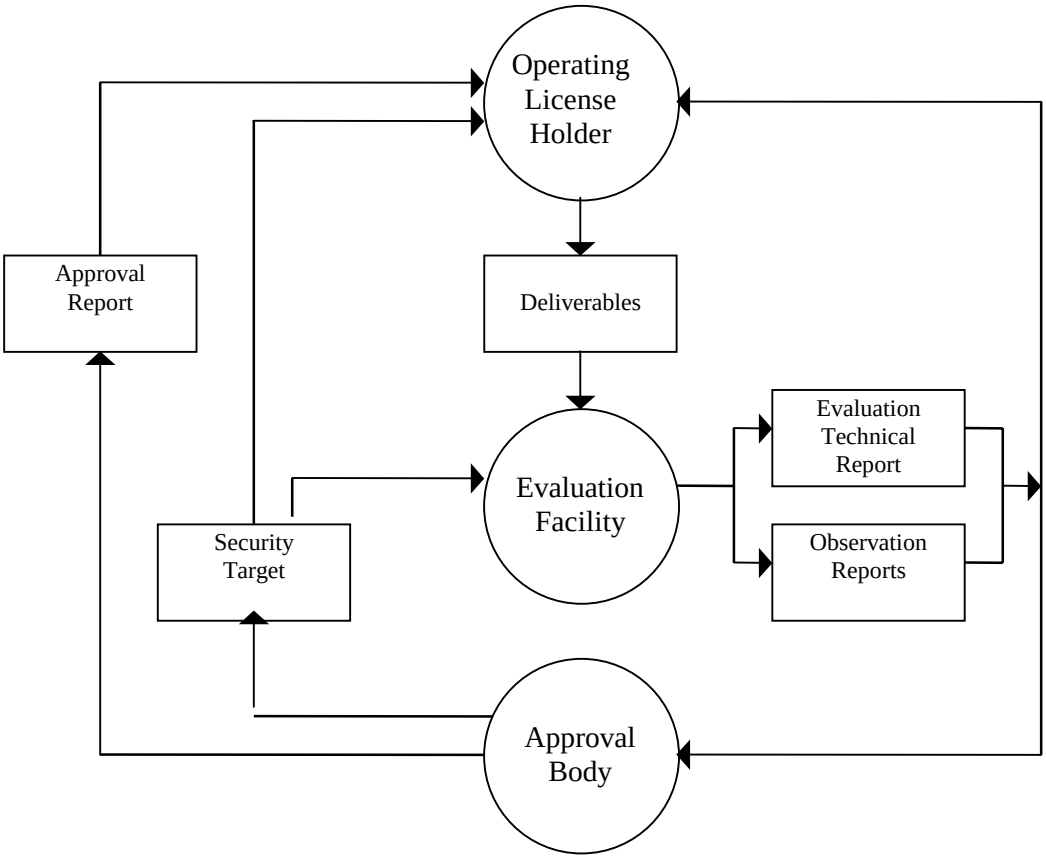


Figure 3.1 - Flow of Information Between Involved Parties

3.6 Impartiality, Integrity and Commercial Confidentiality

3.6.1 The Evaluation Facility must observe the highest standards of impartiality, integrity and commercial confidentiality. Therefore, neither the Evaluation Facility, nor

individual Evaluation Facility staff concerned with the evaluation of the Health Database must have a vested interest in the outcome of the evaluation. No Evaluation Facility staff member shall be involved in:

a) development of the Health Database, or

b) the provision of consultancy advice to the OLH which would in any way compromise the independence of the evaluation.

3.6.2 In order to ensure that these conditions are met, the impartiality of the Evaluation Facility in relation to the OLH shall be open to scrutiny by the Approval Board.

3.6.3 The OLH and Evaluation Facility must obtain written agreement from the Approval Board for all press releases and similar statements that refer to the evaluation or approval of the Health Database.

3.6.4 The Evaluation Facility shall maintain under configuration control all material supplied to them during the course of the evaluation relating to the Health Database. In addition, any material supplied to the Evaluation Facility shall be held securely in such a manner that individuals who are not working on the evaluation do not have access to it.

3.7 Natural Language for Deliverables and Evaluation Reports

The natural language for the deliverables supplied by the OLH to the Evaluation Facility and the evaluation reports produced by the Evaluation Facility shall be English.

3.8 Appeals Procedure

Any dispute concerning the operation of the Approval Process may be referred to the Approval Board by any party, including the OLH or Evaluation Facility.

4 Security Evaluation

4.1 Introduction

The evaluation of the Health Database will be performed against the Common Criteria as defined in the [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3]. Irrespective of the required assurance level, the evaluation will be performed in the following stages:

a) Stage 1 - Preparation for Evaluation

b) Stage 2 - Perform Evaluation

c) Stage 3 - Collate Results into an Evaluation Technical Report

d) Stage 4 - Review Evaluation Technical Report/Production of an Approval Report

e) Stage 5 - Closedown of Evaluation.

4.2 Stage 1 - Preparation for Evaluation

4.2.1 Introduction

4.2.1.1 The Preparation for Evaluation stage ensures that all parties involved in the evaluation have a common and clear understanding of each of their roles and responsibilities in terms of ensuring that the evaluation can be performed in an effective and timely manner.

4.2.1.2 A number of activities are performed during the Preparation for Evaluation stage, namely:

a) submission of the Security Target as the baseline of the evaluation

b) discussion between the Evaluation Facility and the OLH regarding the deliverables which the OLH will need to supply and produce in support of the evaluation, together with agreement on the timescales for the supply of these deliverables

c) production of a Deliverables List by the Evaluation Facility which summarises the above discussion

d) a Start-up Meeting.

4.2.1.3 Each of these activities is described in more detail in the following paragraphs.

4.2.2 Security Target

4.2.2.1 The baseline for a formal evaluation is a Security Target which defines the security functionality against which the Health Database is to be evaluated. Therefore the Security Target for the Health Database shall define the baseline against which it will be evaluated and the required assurance level requirements. In addition the Security Target shall define the environment in which the Database will be operated, and against which the evaluation will be performed.

4.2.2.2 The evaluation of the Health Database will be performed against a Security Target and not a Protection Profile. Therefore, the Security Target shall provide the necessary information as identified in Annex C of [CC Part 1], and illustrated in Table 4.1.

Table 4.1 - Security Target
• Security Target introduction
• Description of the system under evaluation i.e. the Health Database
• The security environment under which the Health Database will operate, including the assumed threats to the security of the Health Database
• The security objectives of the Health Database
• The IT security requirements claimed for the Health Database, i.e. the security functional requirements and the security assurance requirements
• The Health Database summary specification
• Any optional protection profile claims for the Health Database
• A rationale for the security objectives, security requirements and any optional protection profile claims.

4.2.2.3 The Approval Board defines the security requirements which the Health Database must meet. They may produce the Security Target themselves, or alternatively subcontract the production of the Security Target to a security consultant.

4.2.2.4 To ensure that it is acceptable to the Approval Board, the Security Target shall also define any sampling strategy which may be adopted by the Evaluation Facility during the course of the evaluation.

4.2.2.5 At the start of the evaluation the Approval Board shall submit the Security Target to the Evaluation Facility in order that it may be assessed for its suitability as an evaluation baseline. Any problems identified during this initial review will be passed to the Approval Board for action.

4.2.3 Deliverables

4.2.3.1 Hardware, firmware, software or technical documentation generated during the development and operation of the Health Database (including the Health Database itself) can all be grouped under the term “deliverables”. These deliverables are likely to include information on:

a) how configuration management is maintained and controlled

b) the high and low level design of the Health Database

c) the testing the OLH has performed in order to establish that the Health Database operates in the required secure manner.

4.2.3.2 The OLH must supply deliverables that will meet the requirements defined within the Common Criteria, for the required assurance level, to the Evaluation Facility.

4.2.3.3 During the Preparation for Evaluation stage, the Evaluation Facility will discuss with the OLH a suitable timetable for the supply of these deliverables. The Evaluation Facility will then produce a “Deliverables List” which shall annotate the deliverables required, together with their agreed delivery date. The Deliverables List will be distributed to both the OLH and the Approval Board.

4.2.3.4 A detailed description of the requirements which the deliverables must address for each assurance level within the Common Criteria are defined within the [CCEM] and [CC Part 3]. In addition to deliverables, during the course of the evaluation, the Evaluation Facility will require access to the OLH's development and operational site, as well as access to the operational Health Database itself.

4.2.3.5 Should access to the deliverables required be denied to the Evaluation Facility, then it may not be possible to complete the evaluation.

4.2.4 Start-up Meeting

4.2.4.1 At the start of the evaluation a Start-up Meeting shall be held which shall be attended by representatives from the Approval Board, OLH and Evaluation Facility.

4.2.4.2 The agenda for the meeting is flexible but should include as a minimum the items identified in Table 4.2.

Table 4.2 - Start-up Meeting Agenda
• Introductions
• Discussion of the Security Target and its suitability as a baseline for the evaluation
• Confirmation of the Common Criteria assurance level for the evaluation
• Discussion of the Deliverables List
• Timetable for the evaluation
• Support required by the Evaluation Facility from the OLH
• Requirements for the handling of proprietary information
• Any foreseen problems which could hinder progress of the evaluation.

4.2.4.3 The meeting shall be chaired by the Approval Board and minuted by the Evaluation Facility. Minutes of the meeting shall be distributed to all attendees.

4.3 Stage 2 - Perform Evaluation

4.3.1 Introduction

4.3.1.1 During the Perform Evaluation stage the following activities shall be performed:

a) the Evaluation Facility shall perform the activities specified in the assurance requirements section of the ST. These will be interpreted within the context of the Common Criteria as defined in the [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3]

b) the Evaluation Facility shall perform independent testing of the Health Database

c) the Evaluation Facility shall raise Observation Reports where deliverables supplied by the OLH do not meet the requirements in the ST

d) Progress Meetings shall be held to ensure that the Approval Board, OLH and Evaluation Facility are all fully informed of the progress of the evaluation.

4.3.1.2 Each of these activities is described in more detail in the following paragraphs.

4.3.2 Evaluation Work

4.3.2.1 During the evaluation the Evaluation Facility shall perform the evaluator activities as defined in the [CCEM] for the required assurance level. These activities are summarised in Table 4.3.

Table 4.3 - Evaluation Activities	
ASE	Security Target evaluation activity
ACM	Configuration management activity
ADO	Delivery and operation activity
ADV	Development activity
AGD	Guidance documents activity
ALC	Life-cycle support activity (not applicable for EAL1 or EAL2)
ATE	Tests activity
AVA	Vulnerability assessment activity (not applicable for EAL1).

4.3.2.2 The evaluators shall only be able to perform each evaluation activity once the appropriate deliverables have been provided to them by the OLH.

4.3.2.3 For each activity, the evaluators will produce an Activity Report which will describe the:

a) work performed by the evaluators

b) the evaluators recommendations and conclusions of whether the supplied deliverables meet the individual requirements for each activity.

4.3.2.4 Where the individual requirements have been met, the evaluators will assign a “pass” verdict to the evaluation activity. Where problems have been encountered by the evaluators (for example where the deliverables supplied by the OLH do not meet the individual requirements of the activity), the evaluators shall assign a “fail” verdict to the activity and an Observation Report shall be raised (refer to Section 4.3.6).

4.3.2.5 The Activity Reports will be collated at the end of the evaluation and incorporated into an Evaluation Technical Report (Please refer to Section 4.4: Stage 3 - Collate Results into an Evaluation Technical Report).

4.3.2.6 Chapter 5 to Chapter 8 of the [CCEM] define the activities which need to be performed by the Evaluation Facility for Common Criteria assurance levels EAL1 to EAL4.

4.3.3 Sampling

4.3.3.1 Whilst performing the evaluation work, the evaluators may decide to “sample” the information supplied in the deliverables provided by the OLH. The objective of sampling is to gain confidence in the deliverables provided by the OLH without having to analyse all parts of the deliverables in detail.

4.3.3.2 For example, for the Health Database evaluation, it may be acceptable for the evaluators to sample the test evidence supplied to them by the OLH. The Approval Board is responsible for deciding upon the sampling strategy for the Health Database evaluation and this sampling strategy shall be defined within the Security Target. General guidance on sampling can be found in Annex B of the [CCEM].

4.3.4 Cryptography

4.3.4.1 The Evaluation Facility shall take into account the strength of any cryptographic functions used in the Health Database, during the strength of function assessment.

4.3.4.2 The effort required to attack a cryptographic function shall be calculated based on the best publicly known attack method.

4.3.5 Perform Independent Testing

4.3.5.1 During the ATE: Tests activity the evaluators will perform independent testing of the Health Database in order to gain confidence and assurance that the:

a) Health Database behaves as specified by the OLH

b) testing performed by the OLH is adequate

c) test results from the tests performed by the OLH are accurate.

4.3.5.2 In order to perform independent testing, the evaluators will require access to the operational version of the Health Database.

4.3.6 Observation Reports

4.3.6.1 Should the evaluators identify potential or exploitable vulnerabilities or deficiencies in the deliverables supplied by the OLH or in the Health Database itself, then an Observation Report shall be raised. The Observation Report is raised by the Evaluation Facility and issued to both the OLH and the Approval Board. The required content of an Observation Report is defined in Section 2.3.3 [CCEM] and shall include those items as defined in Table 4.4.

Table 4.4 - Content of an Observation Report
• The name of the system under evaluation, i.e. the Health Database
• The evaluation activity being performed when the observation was identified

• Description of the observation, together with the following information:
  • whether the observation is an exploitable vulnerability
  • whether the observation is a potential vulnerability

• Assessment of the severity of the observation, together with the following information:
  • whether the observation is severe enough for the activity to be assigned a “fail” verdict”
  • whether resolution of the observation needs to be performed prior to the remainder of the evaluation proceeding
  • whether resolution of the Observation is required prior to the completion of the evaluation, but in the meantime the evaluation can proceed.

• Organisation who is responsible for addressing the observation, e.g. the OLH
• Required timetable for resolution of the observation
• Assessment of the impact on the evaluation should the observation not be resolved.

4.3.6.2 If it is not possible to resolve the issues raised in an Observation Report, the OLH may either abandon the evaluation, or discuss with the Approval Board and Evaluation Facility the problem and the implications for Approval.

4.3.6.3 The Evaluation Facility shall maintain a report which summarises the Observation Reports raised during the course of the evaluation and whether they still need to be, or have been, addressed by the OLH.

4.3.7 Progress Meetings

4.3.7.1 To ensure regular communication between all parties, formal Progress Meetings shall be held between the OLH, Approval Board and Evaluation Facility in which progress and timescales shall be reviewed for both the project and the evaluation. The Progress Meetings provide a forum for problems to be identified and discussed, and actions to be placed as appropriate.

4.3.7.2 The scheduling of Progress Meetings is flexible. Meetings should be timed to ensure that all parties are aware of any project issues or risks which may affect the timescales for Approval of the Health Database.

4.3.7.3 The agenda for the meeting is flexible but should include, as a minimum those items identified in Table 4.5.

Table 4.5 - Progress Meeting Agenda
• Review of any outstanding actions
• Progress made since previous Progress Meeting
• Technical issues including any Observation Reports outstanding
• Contractual issues
• Any other business
• Date of next meeting.

4.3.7.4 Formal meeting minutes of the Progress Meetings will be produced by the Evaluation Facility and distributed to the meeting attendees.

4.4 Stage 3 - Collate Results into an Evaluation Technical Report

4.4.1 At the end of a formal evaluation, the Evaluation Facility shall prepare an Evaluation Technical Report (ETR) which describes the evaluators' findings together with their conclusions on whether:

a) the Health Database meets its Security Target

b) all of the Common Criteria's requirements have been met for the required assurance level.

4.4.2 In addition, the Evaluation Technical Report describes the work performed during the course of the evaluation by incorporating and summarising the individual Activity Reports produced during Stage 2 - Perform Evaluation.

4.4.3 The required content of an Evaluation Technical Report is defined in Section 2.3.4.3 of the [CCEM] and shall include as a minimum those items identified in Table 4.6.

Table 4.6 - Contents of the Evaluation Technical Report
• Introduction

• Architectural description of the Health Database
• Evaluation, including the evaluation methods, techniques, tools and standards used
• Results of the evaluation - summary of the results of performing each activity defined within the [CCEM] for the required assurance level
• Conclusions and recommendations
• List of deliverables supplied by the OLH
• List of acronyms used together with a glossary of terms
• Copies of all Observation Reports raised during the course of the evaluation
• Copies of all Activity Reports produced during the course of the evaluation.

4.4.4 The Evaluation Technical Report is released by the Evaluation Facility to both the Approval Board and OLH.

4.4.5 Should the OLH disagree with the findings described within the Evaluation Technical Report, then they can call a Progress Meeting in order to discuss them with both the Approval Board and the Evaluation Facility.

4.5 Stage 4 - Review Evaluation Technical Report/Production of an Approval Report

4.5.1 The Approval Process and evaluation shall conclude with the Approval Board reviewing the Evaluation Technical Report and determining whether the Health Database has met the specified requirements for the selected assurance level. If the Approval Board concludes that the assurance criteria has been achieved then they will write a short Approval Report confirming that they agree with the results of an evaluation as described within the ETR and that the evaluation criteria used were correctly applied.

4.5.2 More information regarding the Approval Process can be found in Chapter 5.

4.6 Stage 5 - Closedown of Evaluation

4.6.1 During this stage the evaluation will be closed down and the material supplied to the Evaluation Facility by the OLH during the evaluation will be returned to them.

4.6.2 The Evaluation Facility will archive all reports including the Activity Reports, Observation Reports and Evaluation Technical Reports produced by them during the evaluation in a secure manner for a minimum period of three years.

5 The Approval Process

5.1 Introduction

This Chapter summarises the role that the Approval Board plays in the Approval Process.

5.2 Role of the Approval Board

5.2.1 During the preparation for evaluation stage, the Approval Board confirms the suitability of the Security Target as part of the formal acceptance of the proposed Evaluation into the Approval Process.

5.2.2 During the evaluation stage, the Approval Board monitors the conduct of the evaluation, including the attendance at the Start-up and Progress Meetings. The Approval Board reviews all Observation Reports and the Evaluation Technical Report to ensure conformance to the Approval Process. The Approval Board reserves the right to witness the evaluation procedures at the premises of the parties involved.

5.2.3 On completion of the evaluation, the Approval Board reviews the Evaluation Technical Report to determine the extent to which the Security Target is met by the Health Database, and to assess the implications of the results for security. In doing so the Approval Board shall assess all evaluation results, assigning an assurance level, taking into account factors explicitly excluded from the evaluation.

5.2.4 The Approval Board may contact the Evaluation Facility to make requests for access to specific technical evidence and results to support any conclusions presented in the ETR.

5.3 Approval Report

5.3.1 At the end of the evaluation, the Approval Board shall formally document the findings of the evaluation in an Approval Report.

5.3.2 The Approval Report shall reference the ETR where appropriate and shall include as a minimum those items defined in Table 5.1:

Table 5.1 - Contents of the Approval Report
• A summary of the evaluation results as defined in the Evaluation Technical Report

• The Approval Board's conclusions on whether:
  • the Health Database meets its Security Target
  • all of the Common Criteria's requirements have been met for the required assurance level

5.3.3 Approval provides confirmation that the evaluation has been conducted in accordance with the provisions of the Approval Process and that the conclusions drawn from the evaluation are consistent with the facts presented. However, the issue of an Approval Report does not imply that the Health Database is guaranteed to be completely free of exploitable vulnerabilities. There remains a small probability (smaller with higher assurance levels) that some exploitable vulnerabilities within the Health Database will remain undiscovered.

A Glossary

A1 Glossary

Section 2.3 of [CC Part 1] provides a glossary of the terms used within the Common Criteria. However, Table A2.1 below provides a list of the terms and their meanings used within this document.

• Activity	actions performed by the Evaluation Facility as defined in the [CCEM] for the required assurance level
• Activity Report	a report produced by the Evaluation Facility for each activity required by the Common Criteria - the report describes the work performed by the evaluators and the evaluators' recommendations and conclusions of whether the supplied deliverables meet the individual requirements for each activity
• Approval Board	the Data Protection Commission, who will oversee the evaluation and monitor its compliance with the Approval Process
• Approval Process	methodology under which the evaluation of the Health Database will be performed
• Approval Report	report produced by the Approval Board which defines their conclusions on whether the Health Database has met its Security Target and whether all of the Common Criteria requirements have been met for the required assurance level
• Assurance level	for each assurance level the Common Criteria defines a set of assurance requirements which must be achieved
• Common Criteria	evaluation criteria developed by a world-wide consortium of nations which is now recognised as an ISO standard
• Deliverables	all hardware, firmware, software or technical documentation generated during the development and operation of the Health Database (including the Health Database itself), supplied by the Operating License Holder to the Evaluation Facility in support of the evaluation
• Deliverables List	a list which defines the deliverables which the Operating License Holder must supply to the Evaluation Facility during the course of the evaluation together with their required delivery date

• Evaluation	assessment of a system or product (in this case, the Health Database) against a pre-defined criteria, for example the Common Criteria
• Evaluation Facility	independent third party that will perform an evaluation of the Health Database against the Common Criteria following the Approval Process methodology
• Evaluation Technical Report	a report which describes the work performed by the Evaluation Facility during the course of the evaluation
• Evaluators	personnel who are employed by the Evaluation Facility to perform the evaluation against the Common Criteria
• Observation Reports	reports raised by the Evaluation Facility which identify exploitable vulnerabilities within the Health Database or deficiencies in the deliverables supplied by the Operating License Holder in support of the evaluation
• Operating License Holder	deCODE, who are responsible for developing, testing and operating the Health Database and for supplying deliverables to the Evaluation Facility during the course of the evaluation
• Progress Meetings	regular meetings held between the Approval Board, Operating Licence Holder and Evaluation Facility during the course of the evaluation to ensure there is regular communication between all parties
• Recognised Evaluation Scheme	any scheme which participates in the Mutual Recognition Agreement [MRA]
• Security Target	baseline for an evaluation which describes the security requirements for the product or system under evaluation
• Start-up Meeting	a meeting held at the beginning of the evaluation to ensure that all parties, i.e. the Approval Board, Operating License Holder and Evaluation Facility, have a common understanding of their responsibilities during the evaluation

B Documentation Road-map

B1 Introduction

B1.1 This Annex provides an overview of the Common Criteria documentation which is applicable to the Approval Process and which is referred to within this document. An overview can be found in Section 3.4 of [CC Part 1].

[CCEM] The [CCEM] is the technical methodology applicable for all Common Criteria evaluations, up to and including EAL4.

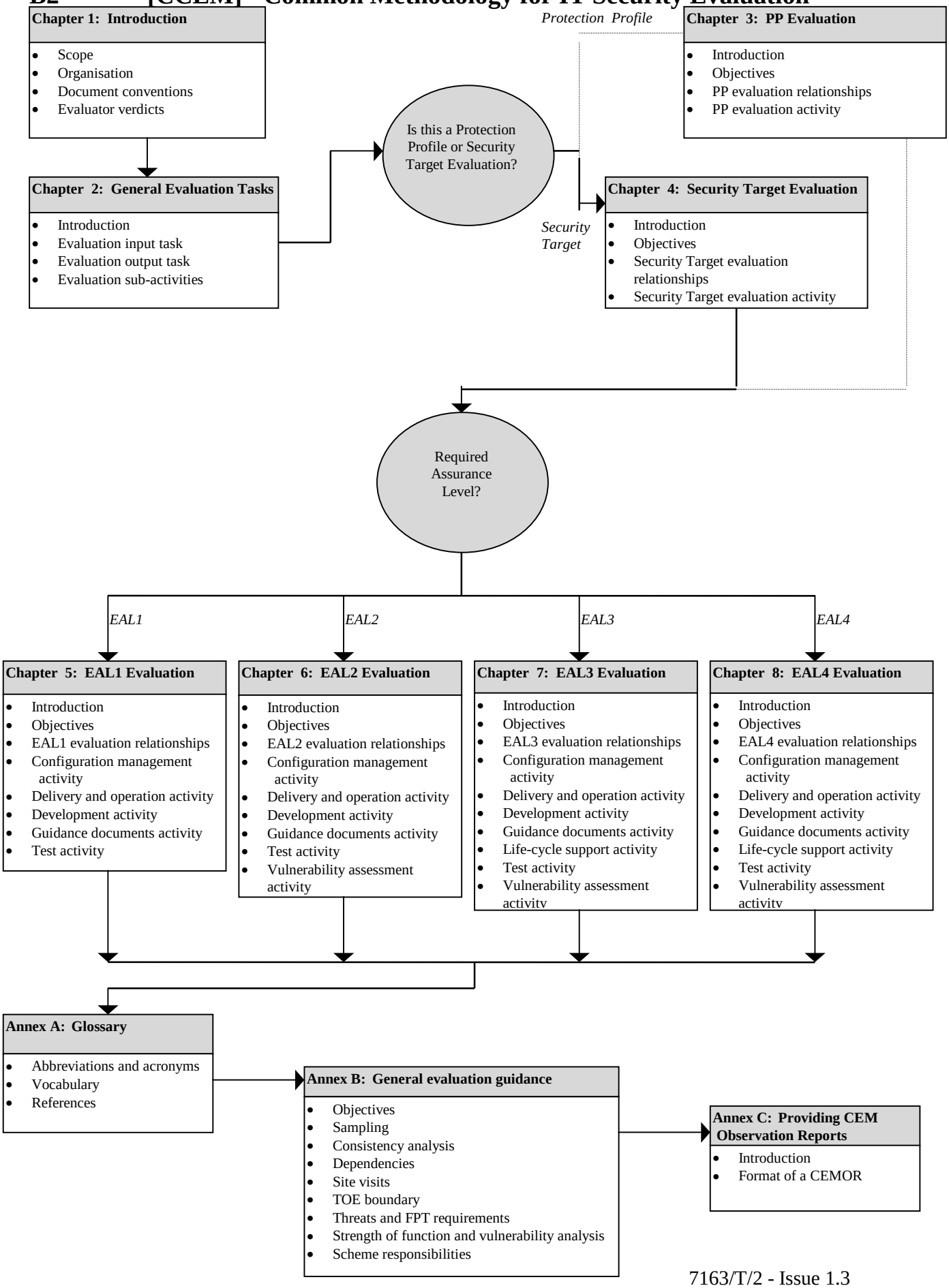
[CC Part 1] The [CC Part 1] provides an introduction and general model for Common Criteria evaluations, from the Common Criteria approach to performing evaluations through to the specification of Security Targets.

[CC Part 2] When developing a system, a developer must consider the potential threats to the operating environment in which their system operates. Within the Security Target, the developer must define a set of functional requirements which are designed to counter these threats. [CC Part 2] contains a catalogue of functional requirements which developers can use when defining their Security Target.

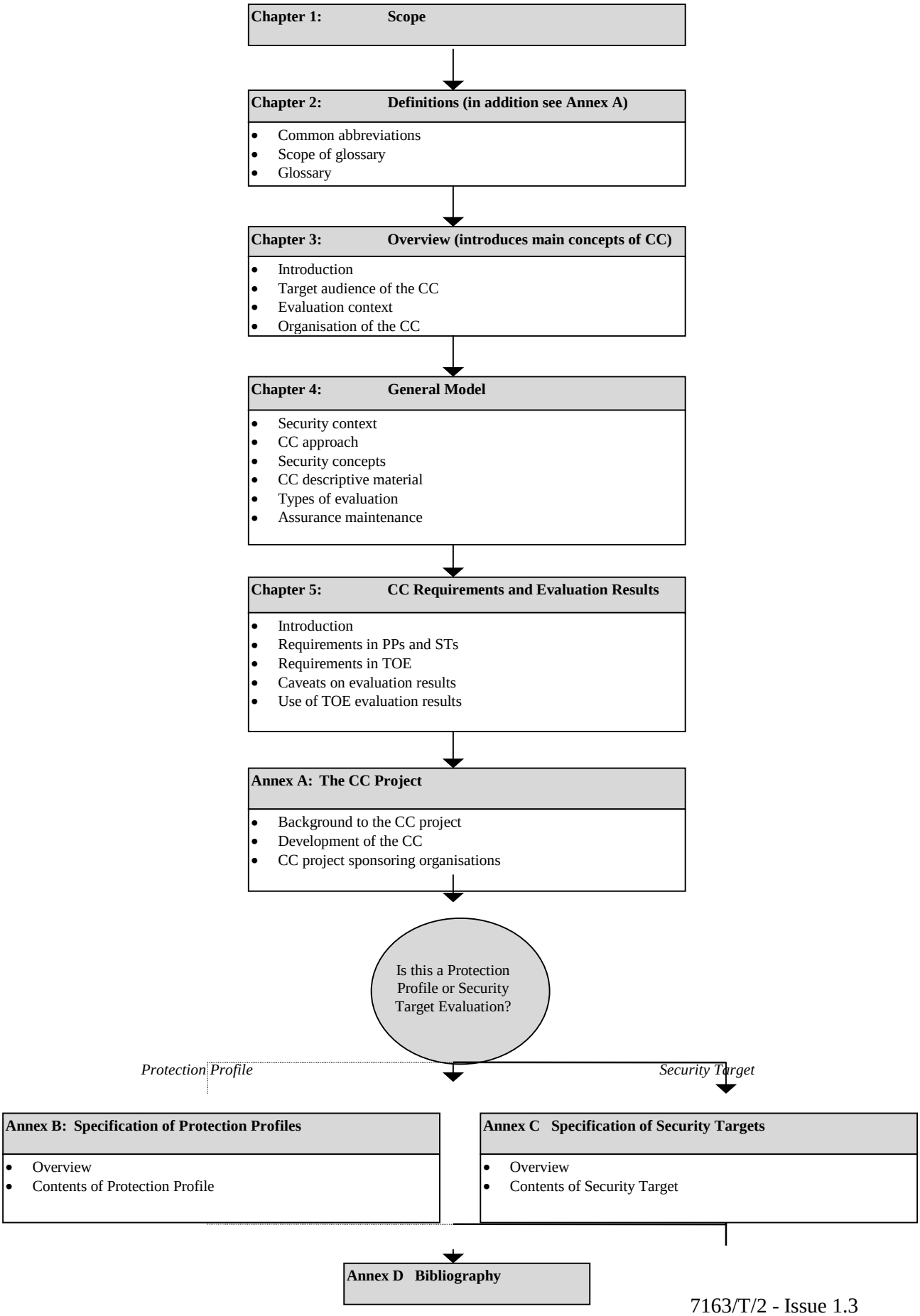
[CC Part 3] For each assurance level, the Common Criteria defines a default set of assurance requirements which must be achieved. The definition of which default assurance requirements are applicable for each of the assurance levels EAL1 through to EAL4 is defined in [CC Part 3].

B1.2 The following pages provide a flow-chart for each of the [CCEM], [CC Part 1], [CC Part 2] and [CC Part 3]. A dotted line (i.e.) is used where a section of these documents does not apply to the Approval Process methodology.

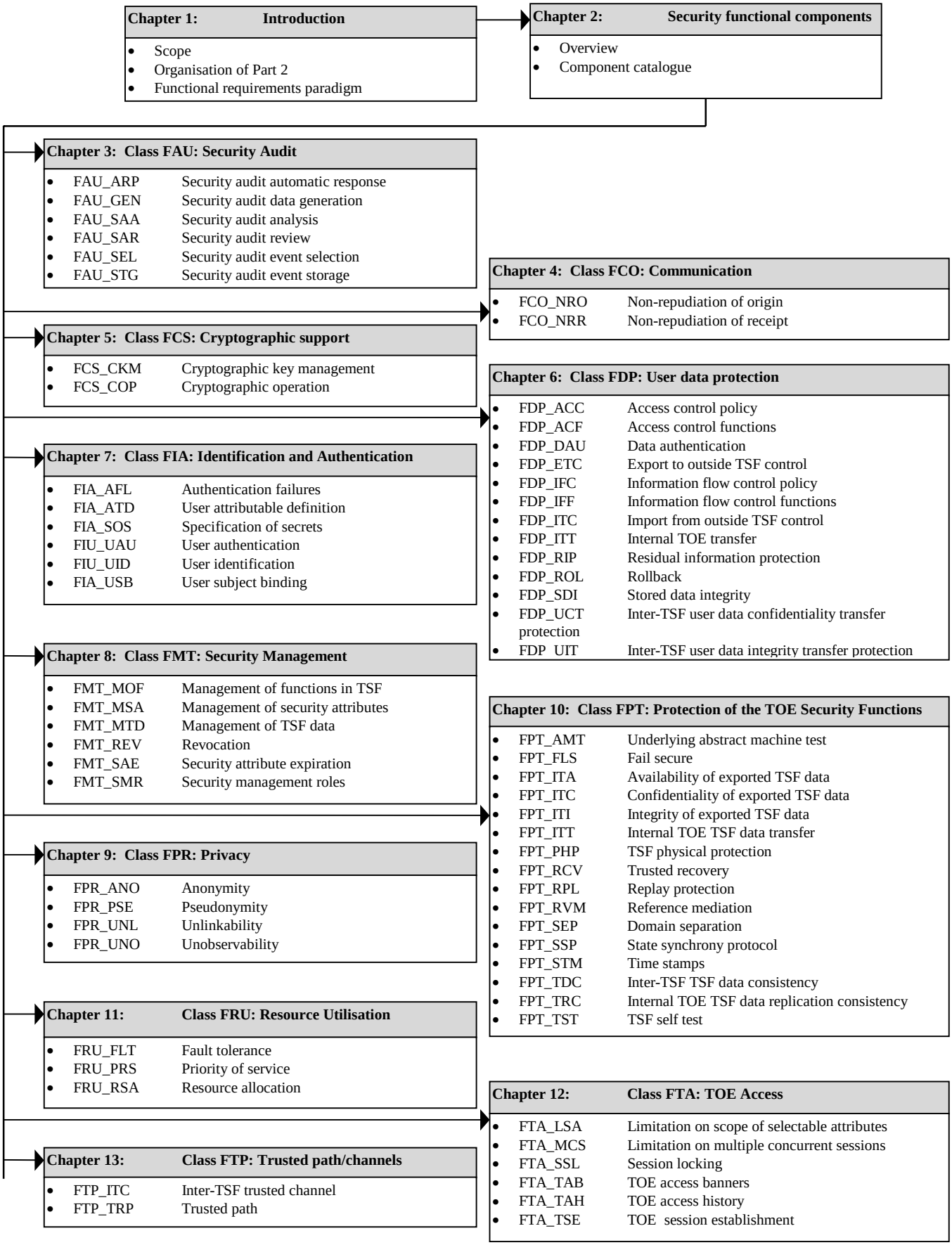
B2 [CCEM] - Common Methodology for IT Security Evaluation



B3 [CC Part 1] - Introduction and General Model



B4 [CC Part 2] - Security Functional Requirements



B5 [CC Part 3] - Security Assurance Requirements