Part 0 Introduction

Chapter 0.1 Introduction

Background

0.1.1 In May 1990 France, Germany, the Netherlands and the United Kingdom published the *Information Technology Security Evaluation Criteria* [ITSEC] based on existing national work in their respective countries. After widespread international review the ITSEC has been developed in two further versions of which the current version 1.2 is the basis for this document.

0.1.2 An important reason for wishing to produce these international harmonised criteria was that such harmonisation is one of the prerequisites of international mutual recognition of the certificates which summarise the results of Information Technology (IT) security evaluations and confirm that the evaluations have been properly carried out. It is also a prerequisite of mutual recognition that the methods used to apply these harmonised criteria should themselves be harmonised. On completion of the ITSEC therefore, the four countries continued to co-operate, with the aim of agreeing a common approach to the conduct of IT security evaluations, at least to the extent necessary to provide the required confidence to facilitate mutual recognition.

0.1.3 Much work had already been done and some of this published on the development of IT security evaluation methods. In the UK this included CESG Memorandum Number 2 [CESG2], developed for government use, and the "Green Books" series of the Department of Trade and Industry, including V23-Evaluation and Certification Manual [DTI23], for commercial IT security products. In Germany, the German Information Security Agency published their IT Evaluation Manual [GISA1].

0.1.4 The basic approach was to harmonise existing security evaluation methods in each of the four countries to the extent necessary to ensure that national evaluation methods conform to a single philosophy. It was initially felt that the work should be limited to harmonisation of existing methods. However, it has been necessary to extend the existing work and to develop some new ideas in order to achieve these objectives.

General Scope

0.1.5 This IT Security Evaluation Manual (ITSEM) builds on the ITSEC Version 1.2, describing how a Target Of Evaluation (TOE) should be evaluated according to these criteria. The specific objective of the ITSEM is to ensure that there exists a harmonised set of evaluation methods which complements the ITSEC.

0.1.6 The ITSEM is a technical document, aimed predominantly at partners in evaluation (primarily evaluators but also sponsors and certifiers), but it is also of interest to vendors, developers, system accreditors and users. It contains sufficient detail of evaluation methods and procedures to enable technical equivalence of evaluations performed in different environments to be demonstrated. The document will be freely available. The ITSEM will apply to evaluations carried out both in commercial and government sectors.

0.1.7 For the purposes of mutual recognition it is necessary that some parts of the ITSEM be prescriptive on evaluators. However most of the ITSEM is descriptive or intended to provide guidance.

0.1.8 In order to put the evaluation methods prescribed and described into a context, it is necessary to include in the ITSEM some outline information on certification and how it may be organised.

0.1.9 This document stresses the importance of independence of evaluation from any commercial pressures from a sponsor or developer of a TOE. However first party evaluation, in the sense of evaluation performed by another part of the sponsoring or developing organisation, is not precluded provided that the requirements of the national scheme are fulfilled.

0.1.10 The ITSEM has been written from the perspective that certification follows the evaluation. The case that an evaluation is followed by a supplier's declaration is outside the scope of this document although, even in this case, use of the ITSEM may still be helpful. **Structure and Content**

0.1.11 The rest of this document consists of six parts, one of which has annexes. Each part has been written from the perspective of the targeted audience for that part. Some subjects are handled in more than one part, but with a different level of detail.

0.1.12 Part 1 of the ITSEM describes an IT security framework providing background and rationale for IT security, evaluation, certification and system accreditation. This part is of a general nature. It is intended for a management audience.

0.1.13 Part 2 of the ITSEM gives basic information on the establishment and running of an evaluation and certification scheme, describing the general features of the certification process and the organisation of it. It is of interest to those wishing to understand the certification process.

0.1.14 Part 3 of the ITSEM explains the evaluation philosophy which underlies the ITSEC. It contains the principles which must be followed by the evaluators when evaluations are performed. It gives further explanation and clarification of the ITSEC concepts to provide a better basis for understanding the technical issues underlying evaluation.

0.1.15 Part 4 of the ITSEM is the key part for those closely involved in evaluation. All mandatory text is in this part. It gives an overview of how evaluation is performed and describes evaluation in terms of input, process, output. However it does not provide guidance for all details of evaluation.

0.1.16 Part 5 of the ITSEM provides examples of the application of ITSEC, demonstrating how the ITSEC can be applied to the evaluation of systems and products.

0.1.17 Part 6 of the ITSEM gives guidance on evaluation to sponsors, vendors, developers, system accreditors and users. It is particularly concerned with preparing the inputs, and using the outputs, from evaluation. **Numbering and Text Conventions**

0.1.18 Each paragraph within a part is uniquely identified by the combination of part number, chapter number and paragraph number within the chapter. The first use of an ITSEM glossary term within a part is shown in bold type. Italics are used to signify emphasis or quotation. In part 4 of the ITSEM prescriptive text has been highlighted by shading and bolding complete sentences or paragraphs.

Further Developments

0.1.19 The ITSEC version 1.2 is currently being used for a trial period. During this period it is expected that improvements to the ITSEC will be proposed in the light of practical experience. The ITSEM also draws upon other documents ([CESG2], [DTI23], [GISA1]) that have already been extensively discussed and used in practice in national schemes; it is considered that the ideas and concepts have been carefully balanced and that the structure chosen for the document is the right one for maximum consistency and usability.

0.1.20 The current version of the ITSEM benefits from significant revisions arising from widespread international review. The review process has been assisted by the Commission of the European Communities who organised an international workshop in September 1992, at which version 0.2 was discussed. This event was supplemented by written comments and contributions from reviewers, which the authors have sought to take into account in preparing version 1.0. It is recognised by the authors of the ITSEM that in some areas of the ITSEM detailed guidance is still lacking, but that where appropriate, additional information in those areas will appear in later versions, as both this document and the ITSEC evolve in line with experience.