INTERNATIONAL STANDARD

ISO/IEC 15408-3

First edition
1999-12-01

Information technology — Security techniques — Evaluation criteria for IT security —

Part 3:
Security assurance requirements

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 3: Exigences d'assurance de sécurité

Reference number
ISO/IEC 15408-3:1999(E)

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Contents

List of Figures

List of Tables

Foreword

ISO the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, **Part 3.**

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in collaboration with Common Criteria Project Sponsoring Organisations. The identical text of ISO/IEC 15408-3 is published by the Common Criteria Project Sponsoring Organisations as *Common Criteria for Information Technology Security Evaluation.* Additional information on the Common Criteria Project and contact information on its Sponsoring Organisations is provided in Annex A of ISO-IEC 15408-1.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional requirements*
- *Part 3: Security assurance requirements*

Annexes A and B of this part of ISO/IEC 15408 are for information only.

This LEGAL NOTICE has been placed in all Parts of ISO/IEC 15408 by request:
The seven governmental organisations (collectively called "the Common Criteria Project Sponsoring Organisations") identified in ISO/IEC 15408-1 Annex A, as the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluation, Parts 1 through 3 (called the "CC"), hereby grant non-exclusive license to ISO/IEC to use the CC in the development of the ISO/IEC 15408 international standard. However, the Common Criteria Project Sponsoring Organisations retain the right to use, copy, distribute, or modify the CC as they see fit.

Information technology — Security techniques — Evaluation criteria for IT security —

Part 3:
Security assurance requirements

1 Scope

This part of ISO/IEC 15408 defines the assurance requirements of the standard. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of PPs and STs.

1.1 Organisation of ISO/IEC 15408-3

Clause 1 is the introduction and paradigm for this part of ISO/IEC 15408.

Clause 2 describes the presentation structure of the assurance classes, families, components, and evaluation assurance levels along with their relationships. It also characterises the assurance classes and families found in clauses 8 through 14.

Clauses 3, 4 and 5 provide a brief introduction to the evaluation criteria for PPs and STs, followed by detailed explanations of the families and components that are used for those evaluations.

Clause 6 provides detailed definitions of the EALs.

Clause 7 provides a brief introduction to the assurance classes and is followed by clauses 8 through 14 that provide detailed definitions of those classes.

Clauses 15 and 16 provide a brief introduction to the evaluation criteria for maintenance of assurance, followed by detailed definitions of those families and components.

Annex A provides a summary of the dependencies between the assurance components.

Annex B provides a cross reference between the EALs and the assurance components.

1.2 ISO/IEC 15408 assurance paradigm

The purpose of this subclause is to document the philosophy that underpins the ISO/IEC 15408-3 approach to assurance. An understanding of this subclause will permit the reader to understand the rationale behind the ISO/IEC 15408-3 assurance requirements.

1.2.1 ISO/IEC 15408 philosophy

The ISO/IEC 15408 philosophy is that the threats to security and organisational security policy commitments should be clearly articulated and the proposed security measures be demonstrably sufficient for their intended purpose.

Furthermore, measures should be adopted that reduce the likelihood of vulnerabilities, the ability to exercise (i.e. intentionally exploit or unintentionally trigger) a vulnerability, and the extent of the damage that could occur from a vulnerability being exercised. Additionally, measures should be adopted that facilitate the subsequent identification of vulnerabilities and the elimination, mitigation, and/or notification that a vulnerability has been exploited or triggered.

1.2.2 Assurance approach

The ISO/IEC 15408 philosophy is to provide assurance based upon an evaluation (active investigation) of the IT product or system that is to be trusted. Evaluation has been the traditional means of providing assurance and is the basis for prior evaluation criteria documents. In aligning the existing approaches, ISO/IEC 15408 adopts the same philosophy. ISO/IEC 15408 proposes measuring the validity of the documentation and of the resulting IT product or system by expert evaluators with increasing emphasis on scope, depth, and rigour.

ISO/IEC 15408 does not exclude, nor does it comment upon, the relative merits of other means of gaining assurance. Research continues with respect to alternative ways of gaining assurance. As mature alternative approaches emerge from these research activities, they will be considered for inclusion in the standard, which is so structured as to allow their future introduction.

1.2.2.1 Significance of vulnerabilities

It is assumed that there are threat agents that will actively seek to exploit opportunities to violate security policies both for illicit gains and for well-intentioned, but nonetheless insecure actions. Threat agents may also accidentally trigger security vulnerabilities, causing harm to the organisation. Due to the need to process sensitive information and the lack of availability of sufficiently trusted products or systems, there is significant risk due to failures of IT. It is, therefore, likely that IT security breaches could lead to significant loss.

IT security breaches arise through the intentional exploitation or the unintentional triggering of vulnerabilities in the application of IT within business concerns.

Steps should be taken to prevent vulnerabilities arising in IT products and systems. To the extent feasible, vulnerabilities should be:

a) eliminated — that is, active steps should be taken to expose, and remove or neutralise, all exercisable vulnerabilities;

b) minimised — that is, active steps should be taken to reduce, to an acceptable residual level, the potential impact of any exercise of a vulnerability;

c) monitored — that is, active steps should be taken to ensure that any attempt to exercise a residual vulnerability will be detected so that steps can be taken to limit the damage.

1.2.2.2 Cause of vulnerabilities

Vulnerabilities can arise through failures in:

a) requirements — that is, an IT product or system may possess all the functions and features required of it and still contain vulnerabilities that render it unsuitable or ineffective with respect to security;

b) construction — that is, an IT product or system does not meet its specifications and/or vulnerabilities have been introduced as a result of poor constructional standards or incorrect design choices;

c) operation — that is, an IT product or system has been constructed correctly to a correct specification but vulnerabilities have been introduced as a result of inadequate controls upon the operation.

1.2.2.3 ISO/IEC 15408 assurance

Assurance is grounds for confidence that an IT product or system meets its security objectives. Assurance can be derived from reference to sources such as unsubstantiated assertions, prior relevant experience, or specific experience. However, the standard provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

1.2.2.4 Assurance through evaluation

Evaluation has been the traditional means of gaining assurance, and is the basis of the ISO/IEC 15408 approach. Evaluation techniques can include, but are not limited to:

a) analysis and checking of process(es) and procedure(s);

b) checking that process(es) and procedure(s) are being applied;

c) analysis of the correspondence between TOE design representations;

d) analysis of the TOE design representation against the requirements;

e) verification of proofs;

f) analysis of guidance documents;

g) analysis of functional tests developed and the results provided;

h) independent functional testing;

i) analysis for vulnerabilities (including flaw hypothesis);

j) penetration testing.

1.2.3 The ISO/IEC 15408 evaluation assurance scale

The ISO/IEC 15408 philosophy asserts that greater assurance results from the application of greater evaluation effort, and that the goal is to apply the minimum effort required to provide the necessary level of assurance. The increasing level of effort is based upon:

a) scope — that is, the effort is greater because a larger portion of the IT product or system is included;

b) depth — that is, the effort is greater because it is deployed to a finer level of design and implementation detail;

c) rigour — that is, the effort is greater because it is applied in a more structured, formal manner.

2 Security assurance requirements

2.1 Structures

The following subclauses describe the constructs used in representing the assurance classes, families, components, and EALs along with the relationships among them.

Figure 2.1 illustrates the assurance requirements defined in this part of ISO/IEC 15408. Note that the most abstract collection of assurance requirements is referred to as a class. Each class contains assurance families, which then contain assurance components, which in turn contain assurance elements. Classes and families are used to provide a taxonomy for classifying assurance requirements, while components are used to specify assurance requirements in a PP/ST.

2.1.1 Class structure

Figure 2.1 illustrates the assurance class structure.

2.1.1.1 Class name

Each assurance class is assigned a unique name. The name indicates the topics covered by the assurance class.

A unique short form of the assurance class name is also provided. This is the primary means for referencing the assurance class. The convention adopted is an “A” followed by two letters related to the class name.

2.1.1.2 Class introduction

Each assurance class has an introductory subclause that describes the composition of the class and contains supportive text covering the intent of the class.

2.1.1.3 Assurance families

Each assurance class contains at least one assurance family. The structure of the assurance families is described in the following subclause.

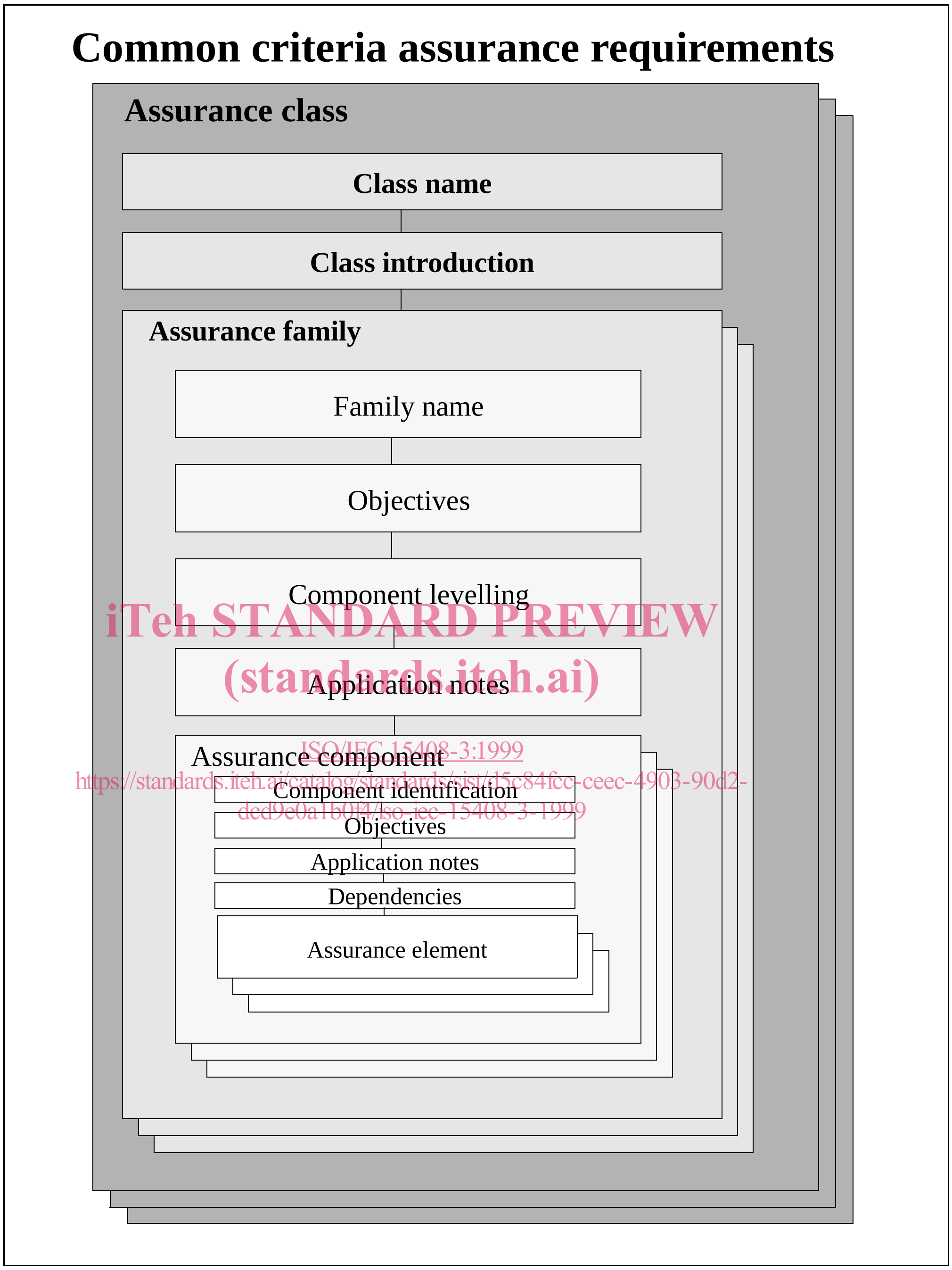

Figure 2.1 - Assurance class/family/component/element hierarchy

2.1.2 Assurance family structure

Figure 2.1 illustrates the assurance family structure.

2.1.2.1 Family name

Every assurance family is assigned a unique name. The name provides descriptive information about the topics covered by the assurance family. Each assurance family is placed within the assurance class that contains other families with the same intent.

A unique short form of the assurance family name is also provided. This is the primary means used to reference the assurance family. The convention adopted is that the short form of the class name is used, followed by an underscore, and then three letters related to the family name.

2.1.2.2 Objectives

The objectives subclause of the assurance family presents the intent of the assurance family.

This subclause describes the objectives, particularly those related to the ISO/IEC 15408 assurance paradigm, that the family is intended to address. The description for the assurance family is kept at a general level. Any specific details required for objectives are incorporated in the particular assurance component.

2.1.2.3 Component levelling

Each assurance family contains one or more assurance components. This subclause of the assurance family describes the components available and explains the distinctions between them. Its main purpose is to differentiate between the assurance components once it has been determined that the assurance family is a necessary or useful part of the assurance requirements for a PP/ST.

Assurance families containing more than one component are levelled and rationale is provided as to how the components are levelled. This rationale is in terms of scope, depth, and/or rigour.

2.1.2.4 Application notes

The application notes subclause of the assurance family, if present, contains additional information for the assurance family. This information should be of particular interest to users of the assurance family (e.g. PP and ST authors, designers of TOEs, evaluators). The presentation is informal and covers, for example, warnings about limitations of use and areas where specific attention may be required.

2.1.2.5 Assurance components

Each assurance family has at least one assurance component. The structure of the assurance components is provided in the following subclause.

2.1.3 Assurance component structure

Figure 2.2 illustrates the assurance component structure.