INTERNATIONAL STANDARD

ISO/IEC 15408-3

Second edition
2005-10-01

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

Reference number
ISO/IEC 15408-3:2005(E)

© ISO/IEC 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/27184084-c6a5-4243-bace-
b3b83bddee/iso-iec-15408-3-2005

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/2711f064-cfa5-4245-bace-b3f885faddee/iso-iec-15408-3-2005

 © ISO/IEC 2005 - All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/27148084-a6e5-4345-bace-15f8851addee/iso-iec-15408-3-2005

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-
b7f85fadddee/iso-iec-15408-3-2005

 © ISO/IEC 2005 - All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/2711f084-cfa5-4245-baee-b31883faddec/iso-iec-15408-3-2005

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

 © ISO/IEC 2005 - All rights reserved

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This second edition cancels and replaces the first edition (ISO/IEC 15408-3:1999), which has been technically revised.

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/27114084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

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*

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 2.3 Parts 1 through 3 (called CC 2.3), they hereby grant non-exclusive license to ISO/IEC to use CC 2.3 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 2.3 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;

© ISO/IEC 2005 - All rights reserved

France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

 © ISO/IEC 2005 - All rights reserved

Introduction

Security assurance components, as defined in this part of ISO/IEC 15408, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogues the set of assurance components, families and classes. This part of ISO/IEC 15408 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT systems and products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE. ISO/IEC 15408-1 Subclause 5.3 provides more detailed information on the relationship between security objectives and security requirements.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part of ISO/IEC 15408 when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this part of ISO/IEC 15408 as mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

© ISO/IEC 2005 - All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

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 ISO/IEC 15408. 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.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the terms, definitions, symbols and abbreviated terms given in ISO/IEC 15408-1 apply.

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

4 Overview

4.1 Organisation of this part of ISO/IEC 15408

Clause 5 describes the paradigm used in the security assurance requirements of this part of ISO/IEC 15408.

Clause 6 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 12 through 18.

Clauses 7, 8 and 9 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 10 provides detailed definitions of the EALs.

Clause 11 provides a brief introduction to the assurance classes and is followed by clauses 12 through 18 that provide detailed definitions of those classes.

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.

© ISO/IEC 2005 - All rights reserved

5 ISO/IEC 15408 assurance paradigm

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

5.1 ISO/IEC 15408 philosophy

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.

5.2 Assurance approach

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 ISO/IEC 15408, which is so structured as to allow their future introduction.

ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-b5f8851addee/iso-iec-15408-3-2005

5.2.1 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.

 © ISO/IEC 2005 - All rights reserved

5.2.2 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.

5.2.3 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, ISO/IEC 15408 provides assurance through active investigation. Active investigation is an evaluation of the IT product or system in order to determine its security properties.

5.2.4 Assurance through evaluation

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-3:2005
https://standards.iteh.ai/catalog/standards/sist/271f4084-efa5-4245-bace-
051885faddec/iso-iec-15408-3-2005

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.

5.3 ISO/IEC 15408 evaluation assurance scale

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.

© ISO/IEC 2005 - All rights reserved