TECHNICAL REPORT

ISO/IEC TR 15443-2

Second edition
2012-11-15

Information technology — Security techniques — Security assurance framework

Part 2: Analysis

Technologies de l'information — Techniques de sécurité — Assurance de la sécurité cadre
Partie 2: Analyses

Reference number
ISO/IEC TR 15443-2:2012(E)

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

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.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

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 TR 15443-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition of ISO/IEC TR 15443-2 cancels and replaces the first edition (ISO/IEC TR 15443-2:2005) and ISO/IEC TR 15443-3:2007, which have been technically revised.

ISO/IEC TR 15443 consists of the following parts, under the general title *Information technology — Security techniques — Security assurance framework*:

— *Part 1: Introduction and concepts*

— *Part 2: Analysis*

Introduction

This part of ISO/IEC TR 15443 is intended to be used together with ISO/IEC TR 15443-1. ISO/IEC TR 15443-1 introduced and discussed the concepts of assurance describing a model whereby the security assurance requirements for a deliverable can be satisfied through the presentation of a security case supported by security evidence that was obtained through making security assurance arguments in the development of a security assurance claim, IT security assurance arguments are verified by the application of security assurance conformity assessment methods and a Mark or symbol awarded appropriately.

ISO/IEC TR 15443-1 introduced the notion of methods for obtaining confidence in the security assurance claims made for a deliverable. This includes methods based on national or international agreed standards, specifications and methods as well as de-facto standards, specifications and methodologies which have as a characteristic a specified and systematic repeatable method for obtaining security assurance. These may be supplemented by a governing conformity assessment scheme that has responsibility for the oversight of the conformity of the application of the standard or specification and the testing method and often undertakes other duties such as awarding security assurance Marks.

By defining such a framework, this part of ISO/IEC TR 15443 guides the IT professional in the selection, and possible combination, of the assurance method(s) suitable for a given IT security product, system, or service and its specific environment.

Intended users of this part of ISO/IEC TR 15443 include those specifying security assurance cases including:

— acquirers (an individual or organization that acquires or procures a system, software product or software service from a supplier);

— developer (an individual or organization that performs development activities, including requirements analysis, design, testing and possibly integration during the software life cycle process)

— maintainer (an individual or organization that performs maintenance activities);

— supplier (an individual or organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract);

— user (an individual or organization that uses the deliverable to perform a specific function);

— evaluator, tester or assessor (an individual or organization that performs an evaluation; an evaluator may, for example, be a testing laboratory, the quality department of a software development organization, a government organization or a user);

The objective of this part of ISO/IEC TR 15443 is to describe criteria that may be used in an analysis to support obtaining confidence in a variety of IT security assurance conformity assessment (SACA) paradigms, and to relate the described criteria to the security assurance model of ISO/IEC TR 15443-1. The emphasis is to identify criteria, often qualitative, and where possible quantitative, that can be used to support the degree of confidence that can be placed in the claims, results and Marks obtained from the associated SACA paradigms.

To provide such a framework it is necessary to characterize the criteria that can be used to assess the quality of the subject paradigm. Many of the criteria proposed in this framework rely on subjective analysis, with elements of assessment that may rely upon individual, organizational, and national norms, cultures and beliefs.

Information technology — Security techniques — Security assurance framework

Part 2:
Analysis

1 Scope

This part of ISO/IEC TR 15443 builds on the concepts presented in ISO/IEC TR 15443-1. It provides a discussion of the attributes of security assurance conformity assessment methods that contribute towards making assurance claims and providing assurance evidence to fulfil meeting the assurance requirements for a deliverable.

This part of ISO/IEC TR 15443 proposes criteria for comparing and analysing different SACA methods. The reader is cautioned that the methods used as examples in this part of ISO/IEC TR 15443 are considered to represent popularly used methods at the time of its writing. New methods may appear, and modification or withdrawal of the methods cited may occur. It is intended that the criteria can be used to describe and compare any SACA method whatever its provenance.

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 TR 15443-1:—[1)], *Information technology — Security techniques — Security assurance framework — Part 1: Introduction and concepts*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviated terms given in ISO/IEC TR 15443-1 and the following apply.

CAP Certificate Authorising Participants

CCP Certificate Consuming Participants

CCRA Common Criteria Recognition Arrangement

CCMC Common Criteria Management Committee

PCI Payment Card Industry

[1)] To be published.

4 A framework for the analysis of IT security assurance

The framework provided in the following clauses presents criteria that will generally be assessed subjectively and that may be used in gaining confidence in various elements of a SACA paradigm. Criteria for the analysis of SACA paradigms, schemes and systems are presented in clause 6, criteria related to assessing SACA bodies are given in clause 7, criteria related to assessing various methods are found in clause 8; criteria for assessing SDOs and standards are found in clause 9 and criteria for assessing the SACA results are offered in clause 10.

The criteria catalogued in this document are intended to be used in support of obtaining confidence in a SACA results. Depending on the objectives of the user of the catalogue some criteria may not be appropriate and still others may need to be defined.

Several CASCO standards exist that should guide stakeholders in a SACA paradigm in the definition and operation of various elements of the paradigm including the SACA schemes, bodies, and systems employed. Those whose objective is to assess these should be familiar with the relevant CASCO documents which have been discussed in clause 9 of part 1 of this Technical Report. Further, obtaining confidence in the SACA results means that criteria for the quality of the results must be considered.

The structure of the following clauses includes a discussion of the topic to be considered, and the identified criteria to be considered with explanatory notes and examples as appropriate.

5 Criteria for the analysis SACA paradigms

There are many examples of SACA schemes. These include the full range of organizations ranging from internal departments within a development or integrating organization, commercially operated schemes, industry-sponsored schemes, as well as those operated by government departments and agencies.

5.1 Availability of recognition agreements and arrangements

5.1.1 Discussion

It is usually the responsibility of a SACA scheme to participate in appropriate recognition agreements and arrangements. Consideration of any such recognition agreements or arrangements may be an important criterion to the producers of deliverables with a wide range of acquirers

5.1.2 Criteria

a) Formal or informal recognition agreements or arrangements are in place;

b) The value to the SACA stakeholders of any recognition agreements or arrangements;

NOTE The stakeholders may consider if such agreements or arrangements are made at international, national, political or industry levels and if such agreements or arrangements facilitate the objectives of the stakeholders.

c) Agreements or arrangements that are made include consideration of development, issuance and operation of arrangements for the recognition and acceptance of results produced by SACA bodies undertaking similar conformity assessment and related activities.

EXAMPLE ISO/IEC Guide 68:2002

5.2 Geographical and political considerations

5.2.1 Discussion

The SACA paradigm may include operations at international, national, regional, political or at an industry level. Consumers of the assurance provided and other stakeholders may specify SACA schemes with jurisdiction in particular areas. This then becomes a consideration for those selecting a SACA paradigm.

5.2.2 Criteria

a) The SACA paradigm operates in appropriate geo-political areas;

b) Cultural differences between the geographies are considered by stakeholders;

c) The existence of Interpretations of standards and specifications in different geo-political areas, or regional policies.

NOTE If interpretations are made differently in different geographical regions then the assessment of the SACA results and the value of the Marks awarded in each region should be reviewed to ensure that commensurate confidence is obtained in each case.

6 Criteria for the analysis of SACA schemes and SACA systems

6.1 Independence

6.1.1 Discussion

A SACA scheme is an organization that is trusted to validate the SACA claims made by others.

Confidence in the claimed assurance can be gained if the scheme specifies a recognised standard or specification for SACA, along with a suitably selected method, particularly if the standards and specifications have been developed by a third party or using an open development process. Further confidence can be provided to interested third parties if the provision of such assurance is validated by a trusted independent third party.

If the SACA scheme is not independent of some stakeholders a conflict of interest may arise, or may be perceived by other stakeholders.

6.1.2 Criteria

a) The degree of independence of the scheme organization from other stakeholders in the SACA paradigm;

EXAMPLE In some cases the scheme has a vested interest in the reduction of its own risk through mandatory SACA. The degree of independence between for example different government agencies may need some consideration.

NOTE It is expected that some relationships exist. For example many SACA schemes have members or participants that may be involved in the governance of the scheme. However, it is intended that this topic should be investigated and any relationship understood and assessed for how they affect independence by those looking for confidence in the scheme

b) The efficacy of the governance of the SACA scheme;

NOTE Use of this criterion may include investigation of the reputation of the SACA scheme an assessment may include obtaining references from others with experience of the operation of the SACA scheme.

c) The accreditation of the SACA scheme itself by another accreditation body.

EXAMPLE In the Common Criteria Recognition Arrangement (CCRA), The Common Criteria Management Committee (CCMC) determines which nations can enter into the CCRA as Certificate Consuming Participants (CCP). The CCMC also determines which nations can change status to Certificate Authorizing Participants (CAP) taking a proposal from CCES into consideration.

NOTE In some cases the accreditation body may operate the SACA scheme itself. In others the operator may be accredited by an independent accreditation body and occasionally both situations are true.

In a few SACA paradigms an accreditation process is not available or is a choice. So the fact that a scheme is not accredited does not, by itself, mean that it is not a reputable organization. That said, many schemes choose to seek accreditation, even when it is not compulsory, in order to be able to demonstrate an independent confirmation of their competence.

6.2 Scheme competence

6.2.1 Discussion

The SACA scheme has responsibility for the quality of the SACA results, often overseeing SACA conformity assessment bodies such as laboratories, ITSEF and assessment organizations. There are several criteria that contribute to confidence in the competence of a SACA scheme.

6.2.2 Criteria

a) Conformance to CASCO standards relevant to the SACA scheme;

EXAMPLE ISO/IEC 17020 gives General criteria for the operation of various types of bodies performing inspection.

b) Technical experience & competence of the scheme personnel with the deliverable type and technology;

NOTE The topic of training of personnel is addressed in ISO/IEC 17020, however the consideration in this criterion is to consider if the scheme as a whole can offer competency in particular type of deliverable.

EXAMPLE In the Common Criteria paradigm, some national schemes have developed particular expertise in the assessment of smart card technology, while others focus on operating systems. It may be argued that such schemes will therefore offer a more mature assessment for that technology, even though, through the scheme accreditation process, all participating schemes will offer a minimum competency in each technology type.

c) Experience of the responsible organization in operating SACA schemes;

NOTE Items that may contribute to assessing experience include if the scheme management operated any other schemes either currently or in the past, and the length of time that the scheme has been in operation.

d) The scheme provides interpretations and guidance regarding the scheme's policies, SACA system and SACA method(s) applied by the scheme;

e) The scheme has adequate policies regarding liability and where appropriate, liability insurance;

NOTE The scheme may assume risk through providing assurance to assurance consumers. In some cases its liability is assumed by the State in accordance with national laws or by the organization of which it forms a part.

6.3 Assessment conformity

6.3.1 Discussion

The SACA scheme is very often responsible for ensuring conformity between the SACA bodies working under the auspices of the scheme, and hence between assessments performed by different SACA bodies.

6.3.2 Criteria

a) The provision of scheme policies regarding assessment conformity of SACA bodies providing SACA results;

NOTE Policies may include criteria such as conformance with CASCO standards for SACA bodies performing SACA activities under the auspices of the scheme.

b) The provision by the scheme of tools for use by SACA bodies performing conformity assessment activities;

NOTE Considerations about any tools provided include if such tools been assessed for their quality, and whether it is mandatory that any such tools are used by SACA bodies.

c) The provision or specification by the scheme for training of staff working within the scheme;

NOTE This is very important when scheme processes include validating the work of a SACA body.

d) The provision or specification by the scheme for training of SACA body personnel performing assessments.

NOTE In addition to the training aspects for the competence of scheme personnel some SACA schemes also offer a base training and even personnel certification for assessors working with the schemes accredited SACA bodies.

6.4 Support to security assurance users and providers

6.4.1 Discussion

In some cases the scheme offers additional support to participants. This may take the form of training, provision of templates, guidance documentation and events.

6.4.2 Criteria

a) The scheme provides supportive services to scheme users;

b) The scheme is engaged with the various stakeholders.

6.5 Provision of interpretations of standards and methods

6.5.1 Discussion

In most cases standards or specifications require interpretations or corrigenda to resolve ambiguities that were not foreseen. This may be because of evolving technology, changing requirements or scheme policies, an evolving threat landscape or other reasons. It is important that any such interpretations are available to stakeholders and applied uniformly.

6.5.2 Criteria

a) The scheme provides relevant interpretations of the standards, specifications and methods;

b) Relevant interpretations are available to all stakeholders, are applied uniformly;

NOTE See subclause 5.2.

c) Interpretations are reviewed, updated and maintained regularly.

NOTE This may include co-ordinating interpretations with SDOs, other schemes and users of the standards, specifications and methods.