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

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

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

© ISO/IEC 2012

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

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

© ISO/IEC 2012 – All rights reserved

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms, definitions and abbreviated terms 1

4 A framework for the analysis of IT security assurance 2

5 Criteria for the analysis SACA paradigms 2
5.1 Availability of recognition agreements and arrangements 2
5.1.1 Discussion 2
5.1.2 Criteria 2
5.2 Geographical and political considerations 3
5.2.1 Discussion 3
5.2.2 Criteria 3

6 Criteria for the analysis of SACA schemes and SACA systems 3
6.1 Independence 3
6.1.1 Discussion 3
6.1.2 Criteria 3
6.2 Scheme competence 4
6.2.1 Discussion 4
6.2.2 Criteria 4
6.3 Assessment conformity 4
6.3.1 Discussion 4
6.3.2 Criteria 5
6.4 Support to security assurance users and providers 5
6.4.1 Discussion 5
6.4.2 Criteria 5
6.5 Provision of interpretations of standards and methods 5
6.5.1 Discussion 5
6.5.2 Criteria 5
6.6 Scheme related policies 6
6.6.1 Discussion 6
6.6.2 Criteria 6
6.7 SACA systems 6
6.7.1 Discussion 6
6.7.2 Criteria 6
6.8 Commercial considerations 6
6.8.1 Discussion 6
6.8.2 Criteria 7
6.9 SACA results 7
6.9.1 Discussion 7
6.9.2 Criteria 7
6.10 SACA Marks and symbols 7
6.10.1 Discussion 7
6.10.2 Criteria 7

7 Criteria for the analysis of SACA bodies 8
7.1 Independence 8
7.1.1 Discussion 8
7.1.2 Criteria 8

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

7.2 Accreditation 9
7.2.1 Discussion 9
7.2.2 Criteria 9
7.3 SACA body competence 9
7.3.1 Discussion 9
7.3.2 Criteria 9
7.4 Commercial considerations 10
7.4.1 Discussion 10
7.4.2 Criteria 10

8 Criteria for the analysis of SACA methods 11
8.1 General criteria for SACA methods 11
8.1.1 Discussion 11
8.1.2 Criteria 11
8.2 Confidence in the assurance method 11
8.2.1 Discussion 11
8.2.2 Criteria 11
8.3 Independent Confirmation 12
8.3.1 Discussion 12
8.3.2 Criteria 12
8.4 Trust Policies 12
8.4.1 Discussion 12
8.4.2 Criteria 13
8.5 Maturity of the assurance method 13
8.5.1 Discussion 13
8.5.2 Criteria 13

9 Criteria for the analysis of standards, specifications and SACA documents 13
9.1 The standards development organization 13
9.1.1 Discussion 13
9.1.2 Criteria 13
9.2 The standard or specification 14
9.2.1 Discussion 14
9.2.2 Criteria 14

10 Criteria for the analysis of the SACA results 14
10.1 Documentation produced 14
10.1.1 Discussion 14
10.1.2 Criteria 14
10.2 Identification of the components of the deliverable 15
10.2.1 Discussion 15
10.2.2 Criteria 16
10.3 Scopes and boundaries of the target of the assessment 16
10.3.1 Discussion 16
10.3.2 Criteria 16
10.4 Functionality of the deliverable assessed 16
10.4.1 Discussion 16
10.4.2 Criteria 16
10.5 Supply chain criteria 17
10.5.1 Discussion 17
10.5.2 Criteria 17
10.6 Analysis of the security problem 17
10.6.1 Discussion 17
10.6.2 Criteria 17
10.7 Lifecycle 17
10.7.1 Discussion 17
10.7.2 Criteria 18
10.8 Operational considerations 18
10.8.1 Discussion 18
10.8.2 Criteria 18

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

 © ISO/IEC 2012 – 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.

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*

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

Information technology — Security techniques — Security assurance framework

Part 2:
Analysis

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

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.

© ISO/IEC 2012 – All rights reserved

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

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

 © ISO/IEC 2012 – All rights reserved

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.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

6.6 Scheme related policies

6.6.1 Discussion

In addition to any policies specified by or applicable to the organization acquiring the deliverable a SACA scheme may implement policies that are applicable to the scheme users.

6.6.2 Criteria

a) Scheme policies regulating entry as an assessment candidate;

b) Scheme policies that affect the results of the security assurance conformity assessment;

EXAMPLE In the CCRA participating schemes national policies regarding the evaluation of cryptography often apply.

c) The scheme has defined policies for handling any vulnerabilities or weaknesses that are found during the course of the assessment, or that remain in the subject of the assessment after the assessment has completed.

6.7 SACA systems

6.7.1 Discussion

A SACA scheme may employ one or more SACA systems although as a general rule only one is defined. SACA systems may be conformant with CASCO or other standards providing further confidence in the definition and operation of the system.

6.7.2 Criteria

a) Is the SACA system certified to appropriate standards;

EXAMPLE ISO/PAS 17005 Conformity assessment -- Use of management systems -- Principles and requirements ; ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements; and ISO 9001 Quality management systems – Requirements are examples of standards that may be employed.

b) The modification to any SACA method(s) specified by the scheme are published;

NOTE In many cases an open SACA method is adopted by a scheme but modified through the application of policies or interpretations. Such modifications may affect the conformity of assessments when considered with the use of the same SACA method by a different scheme.

c) Management of any detailed SACA evidence reviewed by the scheme;

NOTE Items that may be considered in regard to management of evidence include confidentiality of detailed evidence and retention periods.

d) A system manual is provided ensuring that the relevant processes are effective and repeatable.

6.8 Commercial considerations

6.8.1 Discussion

Commercial criteria are often an important consideration to stakeholders. For suppliers providing solutions to end-users the resources expended in providing security assurance are a consideration. These commercial aspects can affect the time to market for a product or affect the timeliness of the provision of security functionality critical to addressing the mitigation of weaknesses and vulnerabilities.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

NOTE Also see subclause 7.4.

6.8.2 Criteria

a) The length of time taken for validation activities of SACA results;

b) The length of time taken for the production of SACA Marks;

c) The direct cost to an assurance authority to obtain SACA results;

d) The ongoing direct costs for maintaining SACA Marks;

e) The SACA method specifies the provision of pre-requisite SACA Marks either from the same or a different SACA scheme.

6.9 SACA results

6.9.1 Discussion

Depending on the SACA model deployed the SACA scheme may have access to SACA results, and is often responsible for maintaining them.

6.9.2 Criteria

a) SACA results are handled so that confidentiality and integrity are maintained.

NOTE Key results such as documents describing boundaries, assumptions, and configurations need to be supplied appropriately to the relevant stakeholders. The integrity of the results in regard to ensuring that such documents have not been modified since the SACA was performed, and have been appropriately updated and maintained in accordance with any SACA maintenance activities is important.

EXAMPLE Maintaining and appropriately providing documents describing SACA boundaries such as Security Target documents, Security Policy documents, statements of compliance, and assessment reports.

b) maintenance of assurance is handled appropriately.

NOTE Some systems call for a periodical re-assessment of the result, others a review of product updates with emphasis on determining if the changes are security relevant or not.

6.10 SACA Marks and symbols

6.10.1 Discussion

Marks and symbols related to security assurance need to be managed and used appropriately. In most some SACA paradigms it is policy that the Marks awarded are public, but in some cases the award of a Mark may be confidential.

If it can be shown that a SACA system is in conformance with relevant CASCO standards, for example ISO Guide 27 Guidelines for corrective action to be taken by a certification body in the event of misuse of its Mark of conformity, then confidence may be drawn that many of the criteria addressed by these standards are satisfied.

6.10.2 Criteria

a) The list of Marks awarded by the SACA scheme is made public or available to those with a need to know;

EXAMPLE Approved Product Lists (APL), certificates, Marks

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

b) The scheme actively pursue misuse of the SACA Marks and symbols for which they are responsible;

c) The Marks awarded may be updated appropriately for technical changes;

NOTE A minor revision of an IT product that does not affect the results of the assessment.

d) The Marks awarded may be updated for administrative reasons;

EXAMPLE If an organization's name and address changes then the Mark may need to be updated with current information.

7 Criteria for the analysis of SACA bodies

Conformity assessment bodies are variously named within the security assurance conformity assessment domain. For example, in a Common Criteria scheme they may be named "laboratories" or "IT Security evaluation facilities" (ITSEF) or Common Criteria test laboratories (CCTL); In the ISO/IEC 27001 domain they may be named "Certifying bodies" or "Registrars", for the payment card industry they are named "Qualified Security Assessment Companies."

7.1 Independence

7.1.1 Discussion

A SACA body represents an organization that is providing the SACA activities on deliverables that need to provide security assurance conformity assessment.

7.1.2 Criteria

a) The type of assessment body;

NOTE I.e. Is the SACA body operating as type A, B or C assessor? As discussed in part 1 of this Technical Report there are several considerations related to the independence of a SACA body based on their interest in the deliverable, First, second and third party assessments offer different considerations of independence.

b) The degree of independence of the SACA body from other stakeholders in the SACA paradigm;

EXAMPLE Accreditation authorities, SACA schemes and acquirers.

NOTE Some relationships exist. For example many SACA schemes have members or participants that may be involved in the governance of the scheme, or involved in the SACA paradigms technical development. However, it is only intended that this topic should be investigated and any activities understood and assessed for how they affect the independence of the SACA body.

c) The efficacy of the governance of the SACA body;

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

d) Policies for handling potential conflicts of interest.

NOTE Potential conflicts of interest may occur at the organization level. Many SACA schemes offer policy on a SACA body performing consulting activities as well as independent assessment activities. Additionally SACA body policies regarding conflicts of interest affecting individual assessors should be developed. These potential conflicts of interest may derive from working on assessments for similar deliverables; if an assessor has a relationship with the sponsor of the assessment or the producer of the deliverable; and if the assessment body has interests in providing other services and products as well as their assessment services.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

 © ISO/IEC 2012 – All rights reserved

7.2 Accreditation

7.2.1 Discussion

In many paradigms, accreditation of SACA bodies is mandatory. For others accreditation is not an obligation and the fact that a SACA body is not accredited does not, by itself, mean that it is not a reputable organization.

That said, many SACA bodies choose to seek accreditation, even when it is not compulsory, in order to be able to demonstrate an independent confirmation of their competence.

7.2.2 Criteria

a) Accreditation by the SACA body through meeting the requirements of the relevant scheme;

NOTE Requirements often include being in compliance with standards such as ISO/IEC 17025, ISO/IEC 17021, ISO 9001; completing mandatory training requirements; demonstrating competency.

b) The accreditation status: mandatory, voluntary or in remediation.

NOTE Where accreditation is employed it may be possible to investigate if a SACA body has maintained the accreditation effectively or has been subject to sanctions through non conformance with the accreditation requirements. Some accreditation bodies offer public lists of SACA bodies with a remediative accreditation status.

7.3 SACA body competence

7.3.1 Discussion

It is important to consider the competence of the SACA body in performing the assessment work. The competences of the SACA body organisation as well as the individuals assigned to assessments are both relevant since both are contributory factors to a successful assessment.

7.3.2 Criteria

a) The competence of the SACA body;

NOTE One contributing factor is the accreditation process already discussed above. Additionally an organization may make additional efforts to demonstrate competence.

EXAMPLE Examples include voluntary certifications such as conformance with management systems standards such as ISO 9001 or ISO/IEC 27001; provision of public reports, research, industry presentations and involvement in industry forums, and standards development.

a) The competence of assessment staff. Do they have experience in the security assurance methods to be used?

c) The competence of assessment staff. Do they have experience in the subject of the assessment such as the IT products and technology to be assessed?

b) Does independent validation of the competence of assessment personnel occur?

NOTE Most accredited SACA bodies are required to demonstrate the competence of their assessment personnel. The rigour of such training and whether an independent validation of the competence of such personnel, for example through a recognised professional certification, should be considered. The means by how a SACA body assesses the effectiveness of such training is also a factor to be considered.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

7.4 Commercial considerations

7.4.1 Discussion

Commercial criteria are often an important consideration in the real world. For purveyors of COTS products, developers and integrators the resources expended in providing security assurance are a consideration. These criteria can affect the time to market for a product or affect the timeliness of the provision of security functionality critical to addressing the mitigation of weaknesses and vulnerabilities. Commercial considerations can be categorised by whether they are incurred by the sponsor of the assessment, or as a direct cost from the SACA body.

NOTE Also see subclause 6.8.

7.4.2 Criteria

a) Resource availability;

NOTE As well as the assessors, resources needed may include equipment, money and support personnel, that are needed to support the assessment process. These may include a project manager, supporting consultants, specialist suppliers and technical writers.

b) Remediation costs;

NOTE If any vulnerabilities, non-conformities or recommendations are identified during the assessment then these may have to be remediated by the developer or discussed with the scheme.

c) Subject complexity;

NOTE if the subject of the assessment is unusually complex, involves new or unusual technology, or it is difficult to apply the method then the resources required including time and cost may be affected.

d) SACA body costs;

NOTE The SACA body costs and expenses may be paid by the sponsor of the project, For many SACA paradigms these are paid by the developer, but may also be paid by another stakeholder.

e) Time needed to provide assurance;

NOTE For assessments where the time taken to make the assessment is important then the length of the process should be considered, elements of this measure include the time taken for scheme processes, assessment activities and remediation.

f) The SACA body may assume some liabilities for the assessment results, This could result in activities to mitigate this risk including insurance costs or the addition of contractual language;

NOTE This aspect varies within the paradigm being considered.

g) Confidentiality & asset protection requirements;

NOTE If the assessment includes analysis of confidential information such as manufacturing processes, design documents, and source code, then the SACA body's method of protecting this information should be assessed. Depending on the SACA scheme requirements or applicable legislation the SACA body may be required to retain these assets even after the assessment has completed.

h) Geographical considerations

NOTE For some assessments geographical criteria are an issue. For example, consideration may be related to travel expenses for the assessment, proximity to the development locations, the location of the SACA body, or geographical restrictions by the SACA scheme. Such considerations also extend to considering the requirements of export control legislation.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

8 Criteria for the analysis of SACA methods

8.1 General criteria for SACA methods

8.1.1 Discussion

Different SACA methods may be defined, targeting different assurance objectives, different technology types and/or different assurance “levels”. All those methods need to have the following in common:

8.1.2 Criteria

a) The method clearly identifies the assurance objectives;

b) The method clearly identifies the subject matter to which they are to be applied;

c) The method clearly identifies the input required to perform the assessment;

d) The method, including interpretations and the assessment activity steps to be performed as part of the assessment, are clearly defined;

e) The method clearly identify the results of the assessment and how those results can and should be used by users of the subject of the assessment;

EXAMPLE 1 Integrators of an assessed component may use the SACA results as input to assurance assessment of products or systems, using the SACA results in a compositional way.

EXAMPLE 2 Vendors of products including an assessed component should clearly identify to which parts of the product the results apply.

f) The method clearly identify the limits of the assessment method, stating what can not be assessed using the method as well as limitations on the use of the assessment results.

g) The method clearly identifies if results or Marks obtained from using other methods can be reused.

8.2 Confidence in the assurance method

8.2.1 Discussion

Stakeholders must have confidence in the SACA method used that allows stakeholders, in turn, to have confidence in the SACA results. If the SACA results are not able to be understood properly by assurance authorities, for example boundaries are not clearly defined or are defined in a way that does not support the security objectives.

An additional factor is the stakeholder's understanding and perception of the SACA method. Lack of knowledge, misconceptions about requirements of the method, or the assurance paradigm can influence the confidence that the stakeholder has in the results.

EXAMPLE The Cambridge University Technical Report Number 711, "Thinking inside the box: system-level failures of tamper proofing", section 5.2 [2)] illustrates some considerations of this topic.

8.2.2 Criteria

a) The method ensures that the security boundaries are clearly defined and available to assurance authorities;

2) A full citation for this reference is given in the bibliography of part 1 of this TR.

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

b) The method ensures that any excluded components are clearly described or enumerated;

c) The method ensures that any assumptions or environmental requirements are clearly described or enumerated;

d) The method includes communicating the threat model employed in the SACA assessment;

e) The documentation required for supporting the assessment is sized appropriate;

NOTE Too much detailed documentation aimed at the assurance authority can have the effect of hiding the critical information needed to describe the security problem, assumptions and threats.

f) The risks and limitations of the SACA method are highlighted to assurance authorities and other stakeholders;

EXAMPLE A SACA method that includes a vulnerability assessment has the risk that critical vulnerabilities are missed during the assessment activities.

8.3 Independent Confirmation

8.3.1 Discussion

A type A, or first-party assessment, is trusted most by the organization performing it's own assessment. However the SACA results may miss items that the organization does not feel are critical. The SACA results are usually not equally trusted by other organizations,

A type B, or second-party assessment, can help vested stakeholders build confidence in the SACA results since they are able to make assessments focussed on their own needs. However the SACA results may not be equally trusted by other organizations,

A type C, or third party assessment provides independent confidence in the SACA results and engenders trust from a wider range of stakeholders.

Where a choice of assessment types is available, does the program make clear any differences in the assurance that can be provided by each?

8.3.2 Criteria

a) Consideration that the program is based on first, second or third party assessments.

b) Any choice of assessment types available;

c) The SACA methods applied are the same for each type of assessment;

d) For different types of assessment using the same method if the training or qualifications requirements for assessors in each type are the same;

e) Another assessor can follow the method and independently produce the same results.

8.4 Trust Policies

8.4.1 Discussion

The consumer may establish trust policies in regard to SACA methods and results. This is a reflection of the confidence that that the paradigm including warranties, methods and oversight have the capability of producing results and Marks that are trusted by the consumer,

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

8.4.2 Criteria

a) Trust policies are established regarding the SACA paradigm or any of its elements;

EXAMPLE In the Common Criteria a proliferation of Protection Profiles that fail to meet the needs of the assurance authority led to a lack of confidence in their use.

b) Trust policies are based on a deep knowledge and understanding of the SACA paradigm.

NOTE Some paradigms are very complex and the establishment of a trust policy may be based on an incomplete understanding of the features of the paradigm.

8.5 Maturity of the assurance method

8.5.1 Discussion

Like any defined process operating under a system allowing for improvements to be made a SACA method will improve through application of any lessons learned during it's repeated application, in response to developing technologies, and through developing tools and techniques in the SACA industry.

8.5.2 Criteria

a) The length of time that the method been established;

NOTE Methods that have been established and tested over a period of time may offer greater confidence in the associated SACA results.

b) The process for evolving and developing the method.

NOTE The introduction of new technologies, evolving threats, and improvements in assessment techniques mean that updates to the method may be necessary.

c) A feedback mechanism allowing the method developers to gain knowledge from practitioners exists.

9 Criteria for the analysis of standards, specifications and SACA documents

9.1 The standards development organization

9.1.1 Discussion

An assessment of the provenance of the standard, specification or assessment method to be used as a basis for conformance testing or evaluation should be made. The assessment includes assessing the attributes of the standards development organization producing the documents that are the basis for an assessment.

9.1.2 Criteria

a) The maturity of the SDO;

NOTE This may include an assessment of the governance of the SDO, how intellectual property is handled

c) The independence of the SDO;

NOTE Consider what interests does the SDO have in the commercial success of the standard, or any associated schemes/programs? Also consider the membership characteristics of the SDO.

d) The quality of the standards produced by the organization;

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved

NOTE This may include an assessment of the SDO's system for producing the standards and specification including acceptance procedures and consensus building policies.

e) The significance of the organization within the proposed sector that the deliverable will be used;

NOTE This may include an assessment of how experts are recruited to contribute to the development of the standards and specifications.

f) The resources required to develop the standards.

NOTE The resources required may include SDO membership costs; development-meeting attendence and the associated costs of providing appropriate experts.

9.2 The standard or specification

9.2.1 Discussion

An assessment of the provenance of the standard, specification or other document to be used including consideration of at least the following factors:

9.2.2 Criteria

a) The maturity of the document, standard or specification;

b) The SDO development process is well defined;

EXAMPLE ISO/IEC 17007, Conformity assessment -- Guidance for drafting normative documents suitable for use for conformity assessment , provides guidance for SDOs during the development of documents relevant to SACA.

c) The relevance in the industry in which the document is to be applied;

d) It's use within the proposed industry by others, and hence it's recognition;

e) The availability and licence costs to use the relevant documents;

f) The security assurance techniques employed by the standard or specification, and their employment in associated assessment methods.

10 Criteria for the analysis of the SACA results

This clause describes criteria for assessing aspects of the results of a SACA method. The SACA results made available to the assurance authority should be sufficient for the assurance authority, and other stakeholders to understand the security assurance claims, the boundaries of the assessment, factors related to the composition of the security assurance claimed.

10.1 Documentation produced

10.1.1 Discussion

Various SACA methods result in the production of supporting evidence, usually in the form of documentation.

10.1.2 Criteria

a) The results are made available to an assurance authority allowing for sufficient information to build a larger assurance case including these and other results;

b) Any assumptions of the assessment are clearly identified;

IECNORM.COM : Click to view the full PDF of ISO/IEC TR 15443-2:2012

© ISO/IEC 2012 – All rights reserved