PUBLISHED DOCUMENT

PD ISO/IEC TR 19791:2010

Information technology — Security techniques — Security assesment of operational systems

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards
Document Sharing Hub

Full document details: PD ISO/IEC TR 19791:2010

National foreword

This Published Document is the UK implementation of ISO/IEC TR 19791:2010. It supersedes PD ISO/IEC TR 19791:2006 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 April 2010

© BSI 2010

ISBN 978 0 580 68087 8

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 19791:2010

TECHNICAL REPORT

ISO/IEC TR 19791

Second edition
2010-04-01

Information technology — Security techniques — Security assessment of operational systems

Technologies de l'information — Techniques de sécurité — Évaluation de la sécurité des systèmes opérationnels

Reference number
ISO/IEC TR 19791:2010(E)

Documents
Document Sharing Hub

© ISO/IEC 2010

Full document details: PD ISO/IEC TR 19791:2010

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.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

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 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 19791:2010

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 1

3 Terms and definitions 2

4 Abbreviated terms 4

5 Structure of this Technical Report 4

6 Technical approach 5
6.1 The nature of operational systems 5
6.2 Establishing operational system security 5
6.3 Security in the operational system life cycle 7
6.4 Relationship to other systems 10

7 Extending ISO/IEC 15408 evaluation concepts to operational systems 10
7.1 Overview 10
7.2 General philosophy 10
7.3 Operational system assurance 12
7.4 Composite operational systems 14
7.5 Domain Assurance 16
7.6 Types of security controls 18
7.7 System security functionality 20
7.8 Timing of evaluation 21
7.9 Use of evaluated products 22
7.10 Documentation requirements 23
7.11 Testing activities 24
7.12 Configuration management 25

8 Relationship to existing security standards 25
8.1 Overview 25
8.2 Relationship to ISO/IEC 15408 27
8.3 Relationship to non-evaluation standards 27
8.4 Relationship to Common Criteria development 28

9 Evaluation of operational systems 28
9.1 Introduction 28
9.2 Evaluation roles and responsibilities 28
9.3 Risk assessment and determination of unacceptable risks 30
9.4 Security problem definition 30
9.5 Security objectives 31
9.6 Security requirements 31
9.7 The System Security Target (SST) 33
9.8 Periodic reassessment 35

Annex A (normative) **Operational system Protection Profiles and Security Targets** 36
A.1 Specification of System Security Targets 36
A.2 Specification of System Protection Profiles 42

Annex B (normative) **Operational system functional control requirements** 49
B.1 Introduction 49
B.2 Class FOD: Administration 51
B.3 Class FOS: IT systems 59

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: PD ISO/IEC TR 19791:2010

B.4 Class FOA: User Assets 69
B.5 Class FOB: Business 71
B.6 Class FOP: Facility and Equipment 73
B.7 Class FOT: Third parties 78
B.8 Class FOM: Management 80

Annex C (normative) **Operational system assurance requirements** 84
C.1 Introduction 84
C.2 Class ASP: System Protection Profile evaluation 89
C.3 Class ASS: System Security Target evaluation 101
C.4 Class AOD: Operational system guidance document 115
C.5 Class ASD: Operational System architecture, design and configuration documentation 120
C.6 Class AOC: Operational System configuration management 131
C.7 Class AOT: Operational System test 136
C.8 Class AOV: Operational System vulnerability assessment 146
C.9 Class APR: Preparation for live operation 154
C.10 Class ASO: Records on operational system 157

Annex D (normative) **Operational System evaluation methodology** 162
D.1 Technical approach 162
D.2 Class ASP: System Protection Profile evaluation 163
D.3 Class ASS: System Security Target evaluation 178
D.4 Class AOD: Operational system guidance document 195
D.5 Class ASD: Operational system architecture, design and configuration documentation 199
D.6 Class AOC: Operational system configuration management 207
D.7 Class AOT: Operational system test 210
D.8 Class AOV: Operational system vulnerability assessment 217
D.9 Class APR: Preparation for live operation 228
D.10 Class ASO: Records on operational system 231

Bibliography 235

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

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, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, 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).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

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 19791, which is a Technical Report of type 2, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC TR 19791:2006), which has been technically revised.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Introduction

This Technical Report is a support document that defines extensions to ISO/IEC 15408 to enable the security assessment (evaluation) of operational systems. ISO/IEC 15408, as currently defined, provides support for specifying the IT security functionality that exists in products and systems. However, it does not capture certain critical aspects of an operational system that must be precisely specified in order to effectively evaluate such a system.

This Technical Report provides extended evaluation criteria and guidance for assessing both the information technology and the operational aspects of such systems. It is primarily aimed at those who are involved in the development, integration, deployment and security management of operational systems, as well as evaluators seeking to apply ISO/IEC 15408 to such systems. It will be relevant to evaluation authorities responsible for approving and confirming evaluator actions. Evaluation sponsors, and other parties interested in operational system security, will be a secondary audience, for their background information.

Considering the complexity of this project and the need for additional work, the target has been defined to be a Technical Report Type 2. In the future, once additional experience has been gained in this area, it is hoped that it may be possible to convert this Technical Report into an International Standard to support evaluations of operational systems. Until some formalisation of an approach is performed, it is considered unlikely that many operational system evaluations of this nature will be undertaken due to the lack of specific guidance available, a gap that this Technical Report is designed to fill.

There are fundamental issues in regards to the definition and use of the term *system*. ISO/IEC 15408, with its focus on product evaluation, uses the term system to include only the information technology (IT) aspects of the system. The term *operational system*, as used within this Technical Report, covers the combination of personnel, procedures and processes integrated with technology-based functions and mechanisms, applied together to establish an acceptable level of residual risk in a defined operational environment.

This is a revised edition, updated for compatibility with the third edition of ISO/IEC 15408.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Information technology — Security techniques — Security assessment of operational systems

1 Scope

This Technical Report provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation. The principal extensions that are required address evaluation of the operational environment surrounding the target of evaluation, and the decomposition of complex operational systems into security domains that can be separately evaluated.

This Technical Report provides

a) a definition and model for operational systems,

b) a description of the extensions to ISO/IEC 15408 evaluation concepts needed to evaluate such operational systems,

c) a methodology and process for performing the security evaluation of operational systems,

d) additional security evaluation criteria to address those aspects of operational systems not covered by the ISO/IEC 15408 evaluation criteria.

This Technical Report permits the incorporation of security products evaluated against ISO/IEC 15408 into operational systems evaluated as a whole using this Technical Report.

This Technical Report is limited to the security evaluation of operational systems and does not consider other forms of system assessment. It does not define techniques for the identification, assessment and acceptance of operational risk.

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*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub

Full document details: PD ISO/IEC TR 19791:2010

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC 18045 and the following apply.

3.1
component
identifiable and distinct portion of an operational system that implements part of that system's functionality

3.2
external operational system
separate operational system which interfaces to the operational system that is the subject of evaluation

3.3
management controls
security controls (i.e., safeguards and countermeasures) for an information system that focus on the management of risk and the management of information system security

[NIST SP 800-53]

3.4
operational controls
security controls (i.e., safeguards and countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems)

[NIST SP 800-53]

3.5
operational system
information system, including its non-IT aspects, considered in the context of its operating environment

3.6
residual risk
risk remaining after risk treatment

[ISO/IEC Guide 73:2002]

3.7
risk
potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

NOTE This definition is identical to that of 'information security risk' in ISO/IEC 27005:2008.

3.8
risk analysis
systematic use of information to identify sources and to estimate the risk

[ISO/IEC Guide 73:2002]

3.9
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002]

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

3.10
risk management
coordinated activities to direct and control an organization with regard to risk

[ISO/IEC Guide 73:2002]

3.11
risk treatment
process of selection and implementation of options to modify risk

[ISO/IEC Guide 73:2002]

3.12
security controls
management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information

[NIST SP 800-53]

NOTE This definition is intended to include controls that provide accountability, authenticity, non-repudiation, privacy and reliability, which are sometimes considered as distinct from confidentiality, integrity and availability.

3.13
security domain
portion of an operational system that implements the same set of security policies

3.14
subsystem
one or more operational system components that are capable of execution separately from the rest of the system

3.15
system target of evaluation
operational system that is being operated in accordance with its operational guidance, including both technical and operational controls

NOTE Operational controls form part of the operational environment. They are not evaluated in ISO/IEC 15408 evaluation.

3.16
technical controls
security controls (i.e., safeguards and countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system

[NIST SP 800-53]

3.17
verification
assessment processes used to confirm that the security controls for an operational system are implemented correctly and are effective in their application

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 18045 and the following apply.

COTS	Commercial Off The Shelf
OSF	Operational Security Functionality
SP	Special Publication
SPP	System Protection Profile
SSA	System Security Assurance
SSF	System Security Functionality
SST	System Security Target
STOE	System Target of Evaluation

5 Structure of this Technical Report

Clauses 1 to 4 contain introductory and reference material, and are followed by this overview of the contents of the Report (Clause 5).

Clause 6, *Technical approach*, describes the technical approach to operational systems assessment used in this Technical Report.

Clause 7, *Extending ISO/IEC 15408 evaluation concepts to operational systems*, describes how ISO/IEC 15408 evaluation concepts have been extended for use in operational system evaluation.

Clause 8, *Relationship to existing security standards*, describes the relationship between this Technical Report and other security standards which have been used in its development.

Clause 9, *Evaluation of operational systems*, contains requirements for specification of security problems, security objectives, security requirements, SST contents and periodic reassessment which are needed in order to evaluate operational systems.

Annex A, *Operational system Protection Profiles and Security Targets*, defines the security requirement specifications needed for operational systems.

Annex B, *Operational system functional control requirements*, defines the additional security functional requirements needed for operational systems.

Annex C, *Operational system assurance requirements*, defines the additional security assurance requirements needed for operational systems.

Annex D, *Operational system evaluation methodology*, defines additional actions to be performed by an evaluator conducting the evaluation of an operational system.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

6 Technical approach

6.1 The nature of operational systems

For the purposes of this Technical Report, an operational system is defined as an information system, including its non-IT aspects, considered in the context of its operating environment.

Many operational systems are complex in nature, made up of a combination of subsystems that are partially proprietary and unique in nature, and partially constructed using bought-in general products. They interact with and have dependencies upon other systems. An operational system is typically built using components from multiple vendors. These components may be integrated to compose the operational system by an integrator that does not perform any development functions, only configuration and interconnection.

However, operational systems typically:

— are under the control of a single entity, the operational system owner;

— are built against specific needs, for a specific type of operation;

— change frequently; either in technical set-up and/or in operational requirements;

— contain a considerable (or even large) number of components;

— contain bought-in components that possess a large number of possible configuration alternatives;

— enable the operational system owner to balance technical (and specifically IT) and non-technical security measures;

— contain components with different degrees and types of security assurance.

6.2 Establishing operational system security

Secure products offer an important contribution to operational system security and indeed the use of products evaluated against ISO/IEC 15408 may be preferable in construction of a secure operational system. However, security problems in operational systems are caused not only from product problems but also from operational system problems in a real operational environment, such as poor application of bug fixes, poor setting of access control parameters or filtering rules of a firewall, poor linking of files directories, etc. Furthermore, in the case of a network, the security level of an operational system connected to the network might be of concern to other operational systems that have to communicate with it.

This Technical Report is based upon a three step approach to establishing the necessary level of security for an operational system:

a) risk assessment, to determine the security risks applicable to a system;

b) risk reduction, to counter or eliminate security risks by the selection, application and assessment of security controls;

c) accreditation, to confirm that the residual risks remaining within the system after the controls are applied are appropriate for the system to be used in live operation.

Conceptually, this three step process is shown in Figure 1 following.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

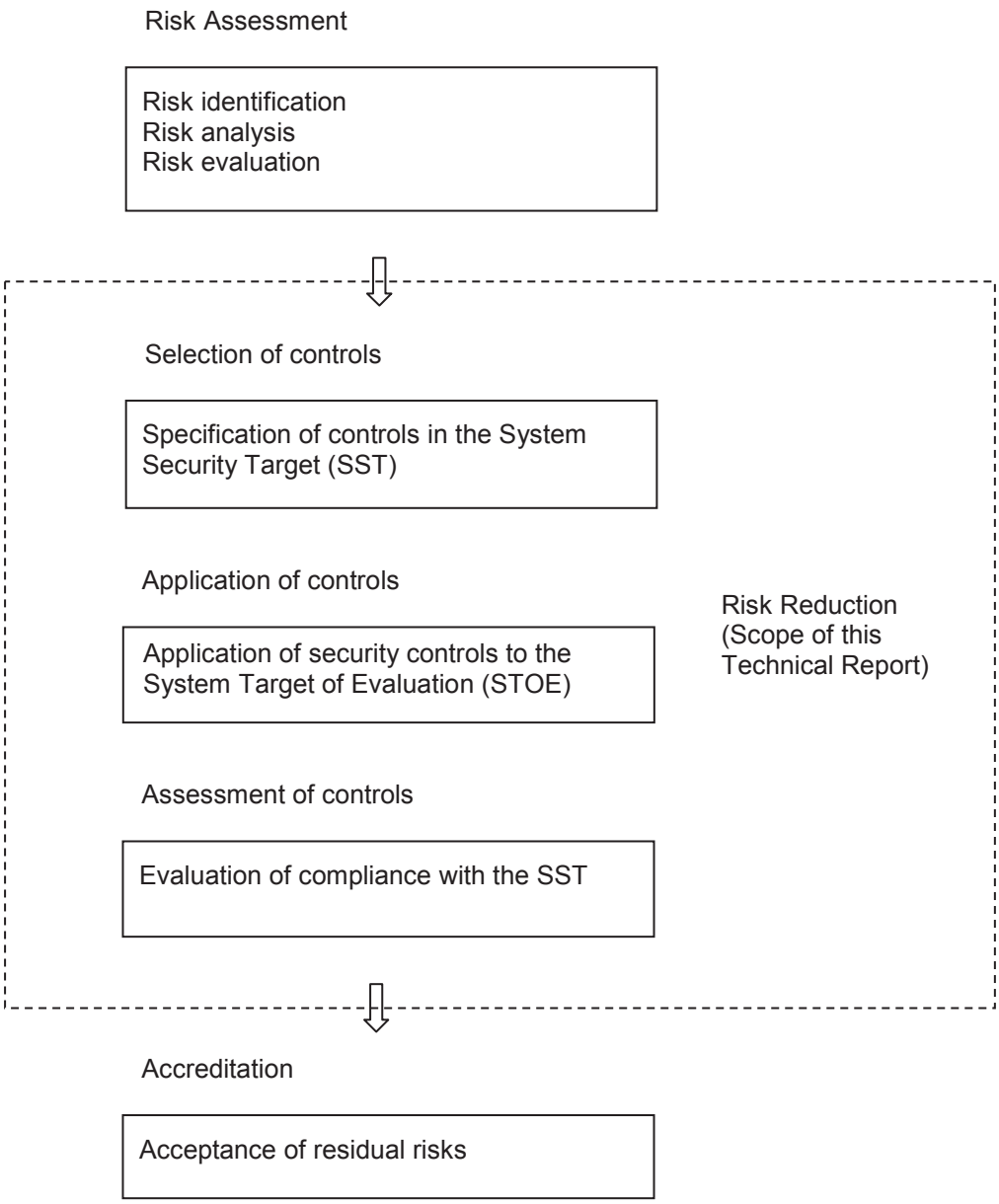

Figure 1 — Process for establishing operational system security

This Technical Report addresses only the middle step of the three step process, namely risk reduction through the selection, application and assessment of security controls. To do this, it uses a security evaluation approach, based upon the security evaluation model for IT security controls defined in ISO/IEC 15408, but extended to deal with all types of security controls.

Techniques and methods for risk assessment are beyond the scope of this report. For more information on risk assessment, see ISO/IEC 27005 [1]. Techniques and models for accreditation are a management responsibility, also beyond the scope of this report. For more information on one possible approach, see NIST SP 800-37 [2].

The security evaluation model of ISO/IEC 15408 excludes consideration of the operational environment surrounding the IT portion of the information system. The operational environment is treated as assumptions in ISO/IEC 15408 evaluation, but cannot be discounted for operational systems. Typically, operational systems are reliant on non-IT security measures, e.g. measures of an administrative or physical nature. There is therefore a need to define ways to express and evaluate such requirements and controls, as an extension

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

to the ISO/IEC 15408 specification criteria. This Technical Report extends ISO/IEC 15408 to do this. The extensions include, but are not limited to:

a) Positioning security evaluation within an overall methodology for the security assessment of operational systems including their operational environment.

b) A methodology for specifying the internal structure of operational systems, including details of internal and external interfaces, to the extent necessary to understand how the various portions of an operational system interoperate.

c) A catalogue of assurance criteria to express the extensions to the scope of evaluation (see Annex A).

d) A catalogue of functional criteria to express additional operational security controls (see Annex B).

e) A catalogue of assurance criteria to express the additional evaluation tasks needed to assess operational systems (see Annex C).

f) A catalogue of evaluator actions to express the additional activities required to assess operational systems (see Annex D).

Extending the ISO/IEC 15408 approach to the evaluation of complete operational systems has the advantage of using a defined existing metric so that common and mutual understanding of evaluation results is possible. For a specific operational system, advertising the evaluation result in a way that is compatible with ISO/IEC 15408 might bring business advantage to customers, not only for service provider systems such as internet banking systems, but also from the view point of social responsibility.

Operational system evaluation requires that a prior risk assessment has identified the security risks applicable to an operational system, and determined those risks that are unacceptable and must be reduced or eliminated through technical and operational controls. It then consists of the following steps:

a) Setting security objectives for the operational system that will reduce the unacceptable risks to a level which is tolerable.

b) Selecting and specifying technical and operational security controls that satisfy the security objectives for the operational system, taking due account of controls that already exist.

c) Defining concrete, measurable assurance requirements for both the technical and operational controls to gain the requisite level of confidence that the operational system meets its security objectives.

d) Recording the decisions made in a System Security Target (SST).

e) Evaluating the actual operational system to judge compliance with the SST.

f) Periodically reassessing both the security risks to the operational system and the operational system's ability to address those risks.

Although this model is an extension of the ISO/IEC 15408 model, it is consistent with that model so that ISO/IEC 15408 evaluation results can be reused.

6.3 Security in the operational system life cycle

6.3.1 Overview

The life cycle of an operational system is considered to have four phases, namely development/integration, installation, system operation and modification. The security controls of an operational system must be assessed throughout the lifetime of the system. This is illustrated in Figure 2 following.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

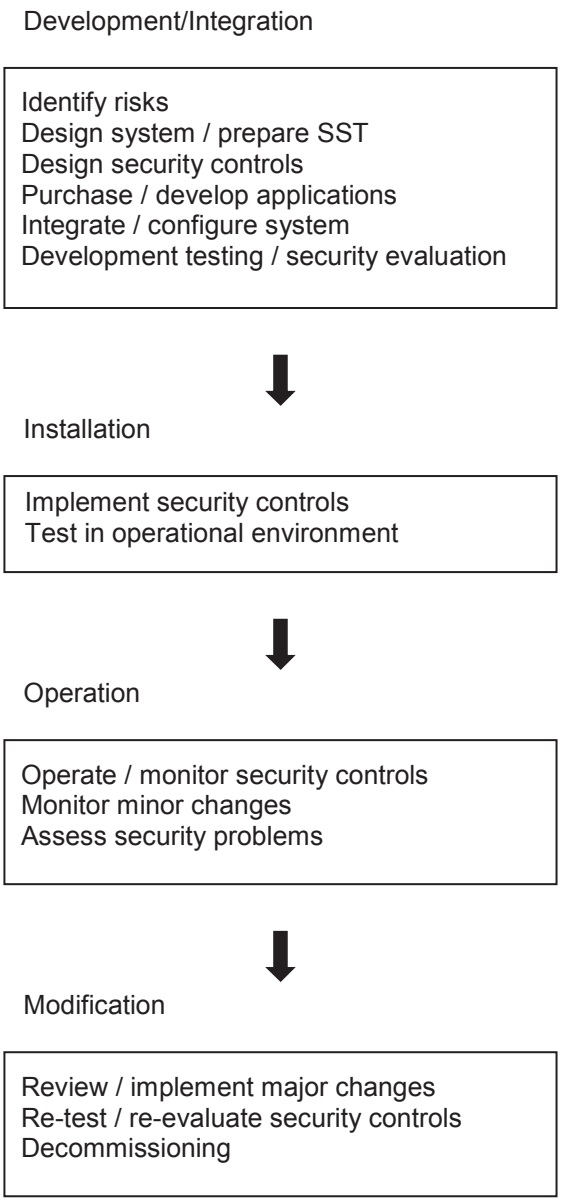

Figure 2 — Security within operational system lifecycle

6.3.2 Development/integration phase

During the development/integration phase, the first security activity is to identify the risks to the operational system. Those risks that are considered unacceptable must be reduced or eliminated by security measures built into the system. Following the risk assessment and identification of risks to be eliminated, an authorized officer of the organization, the Accreditor, must consider the anticipated residual risks, and the sum of the residual risks, and confirm that they will be acceptable.

The operational system will then be designed, including the use of software and hardware products, the physical facilities required, the business application programs needed and the technical security controls required. The design of the operational system must be recorded in the SST. The SST will contain a description of the system security requirements, including the risks to be countered and the security objectives to be achieved by technical and operational controls. The list of technical and operational controls documented in the SST will represent an instantiation of the system security objectives.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

For the purposes of correctness, security objectives should be specified in the SST that address all risks identified as unacceptable. The SST should specify security requirements that completely satisfy the security objectives without any additions or omissions. The design documentation for the operational system should identify precise security countermeasures within the operational system that meet all of the security requirements specified in the SST. The countermeasures might be security functions, facilities, procedures or rules. The countermeasures should be adequately controlled, managed and applied to the system. The security countermeasures should be implemented without any unauthorized addition, elimination or modification. The implementation should be verified with testing of the system or checking of documents. The operation of security countermeasures should be adequately described in the guidance documents.

For effectiveness, the selected security requirements should reduce all security risks identified by risk assessment as unacceptable to a level that can be tolerated as residual risks. Each security countermeasure should work effectively in combination with other countermeasures to satisfy the overall security requirements for the operational system. The strength of the security mechanisms should be sufficient to match the expected attack potential. Vulnerability survey or vulnerability analysis and penetration testing might be required with the expected attack potential.

Evaluators should be involved in the development/integration phase, early in the system life cycle, to facilitate their understanding of the system and its intended environment, as well as to provide input from review of design documentation, and to provide guidance on evaluation and guidance documentation to be used as part of assurance evidence. Ideally the full SST should be evaluated in a preliminary evaluation to confirm that there are no inconsistencies or omissions in the security requirements and proposed controls.

The business applications and systems software, including the technical security controls, are then produced or purchased, and the system is integrated, configured, and tested by the developer. At the same time, the operational security organization is created and security policies, rules and procedures produced and integrated into the system. The proper security configuration settings should be identified and implemented.

Following integration testing, the operational system should be security tested as part of the developer's requirements verification testing. Typically, system specific security controls such as access controls can be verified by the developer prior to deployment at the operational site. Testing of site specific security controls (both technical and operational) is deferred until the system is installed in its intended operational environment. Verification testing will confirm the strength of security mechanisms, as well as the correct operation of the security controls.

The operational system will then be evaluated. The evaluation should confirm that all risks, as detailed in the SST, that have to be countered by security controls are addressed by the system at an acceptable level. The result of the evaluation is an independent confirmation to the system owner that this is the case.

The Certification Report will list any confirmed vulnerabilities found in evaluation, and identify any recommended corrective actions, as required. The system owner will then prepare a corrective action plan to reduce or eliminate the identified vulnerabilities, as deemed appropriate. The result of the certification of the system will be presented to the Accreditor for determination that the actual residual risk to operations and system assets is acceptable. The output of this phase will be an authorization for the system to operate.

6.3.3 Installation phase

During the installation phase, the technical and operational controls will be implemented and prepared for use in the operational environment. Site specific controls will be tested, and other controls retested to confirm that they perform correctly in the actual operational environment.

For the purposes of correctness, the controls should be compliant with the security requirements documented in the SST and authorized for use by a competent person. To be effective, all persons should be trained in use of the security controls and procedures.

6.3.4 System operation phase

In the system operation phase, records of the operation of technical controls and operational controls should be collected and assessed. Audit trails and monitoring records for all access to assets should be logged.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Security countermeasures should be confirmed as operating as intended. It should be verified that unauthorized operations and unacceptable risks have not occurred. Secure states should be recovered from insecure states within the required time. Changes due to routine maintenance should be monitored and assessed for security problems. Records of actual access and utilization of assets should be inspected. Security problems should be reported, reviewed and analyzed.

The purpose of these activities is to provide feedback to the Accreditor when changes occur that may have an impact on operational system security. Typically, in systems operation, a critical subset of the operational system security controls should be identified for regular monitoring to determine their continued effectiveness. Additionally, the system owner should have in place a configuration management, control, and reporting system that documents the current operational system assets, its configuration, and presents that information to the responsible parties.

6.3.5 Modification phase

During the system modification phase, any proposed or actual operational system changes beyond the scope of routine maintenance should be reviewed, analysed and, if necessary, tested to determine their impact on operational system security before being implemented in live operation. This includes changes to procedures and policies. Penetration testing of modified controls should be performed to verify their effective operation.

The results of impact analysis and testing should be presented to the Accreditor to determine the need for security re-evaluation. Where modifications are deemed not to have significantly increased the residual risks, perhaps because they have already been assessed as part of a product assurance maintenance process, re-authorization may be given without re-evaluation. However, if the evaluation results have been invalidated, re-evaluation may be required.

The final act of system modification is decommissioning, where a system is closed down and its data archived, destroyed or transferred to other systems. The Accreditor will be required to confirm that the system has been successfully terminated.

6.4 Relationship to other systems

An operational system may interact with other related systems and may form part of a larger whole. The STOE of the evaluated operational system is defined to be that portion of the group of systems that is evaluated, including both IT systems and their operational environment. The remainder is considered to be external operational systems. An operational system may have security objectives that are met by the external operational systems, but these are not analysed or evaluated.

7 Extending ISO/IEC 15408 evaluation concepts to operational systems

7.1 Overview

The purpose of this clause is to document the philosophy that underpins the ISO/IEC 15408 approach to security evaluation and then to extend it to operational systems. ISO/IEC 15408 addresses only technical controls and their related management controls; in operational systems, technical controls and operational controls combine to protect the information and other assets of the organization.

7.2 General philosophy

For many organizations, information is the primary asset and requires protection against the threats of unauthorised release, modification, or destruction. Those assets are protected using a combination of technical controls and supporting operational control infrastructures of personnel, policy, procedures and physical protection measures. The overall ISO/IEC 15408 philosophy is that threats to organizational assets should be clearly articulated and countered using a combination of technical control and operational control infrastructures. The technical control requirements for addressing threats are included in ISO/IEC 15408-2. Under ISO/IEC 15408, the requirements for the operational controls were considered separately as part of an external accreditation process and therefore were not directly addressed by the security evaluation. This

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

document seeks to formalise those requirements so that they may be assessed as part of the operational system evaluation.

ISO/IEC 15408 conceptually divides security measures into security-related services that must be provided and measures taken to have confidence that those measures are implemented correctly and effectively. In a product evaluation, the security-related services are those functions in the IT implemented to meet the objectives for that piece of technology. In an operational systems context, the procedural and physical contributions to the security can also be assessed. They are similar to IT functionality because they are security capabilities of the operational system that together meet the security objectives. However, they are not normally technology-based and are more suited to assessment during the operational control portion of the operational system life cycle than the development portion. Therefore, they are considered to be separate from functional requirements.

The measures taken to ensure that the security capabilities perform as expected are termed “assurance” in ISO/IEC 15408 and consist of evidence being generated and independent assessment of the suitability of those capabilities. This can be extended to cover the operational controls portion of the operational system through documentation describing the operational controls as implemented.

The process used to develop, implement and maintain both the operational system itself and more specifically the security related services has a considerable influence on the correctness and effectiveness of the security related service and its overall contribution to the total security of the operational system. This influence also contributes to the confidence in the performance of the security related service. Thus the process contributes to the overall assurance of the complex operational system. More specifically the greater the level of capability of the process, the greater the confidence that can be had in the correctness and effectiveness of the security related service and thus the overall assurance provided.

In summary, operational security functional requirements are those non-technical security controls implemented in the operational system contributing to the overall security objectives, while operational security assurance requirements reflect the evidence that those requirements are satisfied.

Evaluation of security in an operational system can therefore be decomposed into a series of steps:

a) The security problem is articulated as a set of risks to be reduced or mitigated, and a set of organizational security policies to be enforced. This requires prior analysis to determine the purpose of the operational system, and risk assessment to determine those risks that must be countered by technical and operational controls. The results of the analysis are recorded in the SST.

b) The security problem is partitioned into a high-level security solution, represented by a set of security objectives. These objectives are recorded in the SST.

c) The security objectives are further refined into security requirements that can be assessed by an independent evaluator. Some security objectives will be allocated to the technical controls and others to operational controls. Some may require both technical and operational controls. For example, controlling unauthorized access to an information asset will often be accomplished both by providing physical security to the facility holding the asset (e.g. locks, guards) and by IT functionality (e.g. user authentication and access control mechanisms). The security requirements are recorded in the SST.

d) A set of activities for the evaluator to follow during the assessment is defined, based on the overall objectives and the overall assurance in the protection measures required. These assurance requirements are recorded in the SST.

e) An independent evaluator assessment determines that the operational system meets its security requirements, based on the requirements documented in the SST.

f) Continuing assessments can also take place to gain confidence that the operational system meets its requirements during operation. These will focus mostly on the operational control portion of the operational system because these controls depend on human behaviour, which is less controllable and consistent than IT behaviour.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

g) Periodic re-evaluation of the operational system can assess that the operational system continues to meet its requirements despite changes to the operational system or its environment. This consists of determining what changes have taken place, assessing the security impact of those changes, updating the SST as required, and determining that security has been maintained during this process.

This process is very similar to the ISO/IEC 15408 evaluation process. The typical difference between an operational system evaluation and a ISO/IEC 15408 product evaluation is that in an operational system evaluation the actual operational environment is fully considered, whereas in a product evaluation the operational environment is not defined in detail, it is described purely as assumptions which are not verified during the evaluation.

The primary goal of an operational system evaluation is to gain assurance that the security objectives for the operational system are implemented correctly and effectively. However, evaluation of security controls, whether technical or operational, can never provide absolute assurance that those controls will always function as intended, at all times and in all circumstances. Evaluation produces a pass or fail verdict. Even if evaluation identifies no unacceptable vulnerabilities, there will always be a residual risk that the controls do not perform as intended. This risk can be reduced by adding additional assurance controls or using different assurance measures that give greater confidence. The residual risk of incorrect or ineffective performance of controls can only be identified through continuous monitoring and assessment.

This residual risk must be taken into account when deciding if an operational system can be accredited for live operation.

Environmental factors may result in differing criticality/threat environments for different operational system components. It is possible that some portions of the operational system may require greater assurance while other portions require less assurance. Because risk assessment can establish different levels of acceptability of risk for different portions of the operational system, an operational system can be divided into security domains with different assurance requirements. The risk assessment will determine acceptability of risk for different parts of the operational system and will aid in determining appropriate assurance measures for each part of the operational system.

7.3 Operational system assurance

The ISO/IEC 15408 paradigm for assurance centres on the provision of evidence that the security functions exist and are implemented correctly and effectively. Higher levels of assurance place more detailed requirements on the content and presentation style of the evidence. In addition, higher assurance sometimes requires increasing rigour of analysis of the evidence by both the developer and the evaluator.

A ISO/IEC 15408 product evaluation is conducted in a manner that assumes a generic operational environment in which the product might be employed. The product evaluation focuses on verifying the security capabilities implemented by the product, independent of any specific operational context. The product evaluation utilises various specification, design and test documentation to substantiate the verdict of correctness. In product evaluation, the assurance requirements are not normally derived from the security problem. Instead, they are selected axiomatically or by policy decision.

The primary goal of a product evaluation is to gain assurance that the security capabilities of the product are implemented correctly. The basis for correctness is established by the security requirements that are contained in the product's Security Target (ST). The ST includes some traceability on the security problem being solved by the resulting set of security requirements. The security problem stated in the ST is assumed to be based on a threat assessment for the types of environments suitable for deployment of the product. The scope of the product evaluation is limited to the IT security requirements allocated to the product by this threat assessment. In addition, the product evaluation sets bounds for "secure values" for configurable aspects of the product: termed the "evaluated configuration". However, these configurations do not take into account any specific environment as this in unknown at the time of evaluation. Upon completion of the product evaluation, it remains necessary to properly integrate the evaluated product with other products to compose an operational system, and finally, to verify that the operational system provides the desired security properties and behaviour in its operational environment and operational configuration.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Product evaluations generally have the same assurance measures applied across all the security functionality defined. Although it is technically possible to have different security domains in products, this is not usually applied for generic product evaluations.

The evaluation evidence and evaluation reports generated from a product evaluation may be used to support the operational system integration and verification effort.

In principle, there is little difference between the properties of an IT product and an operational system for the purposes of security evaluation. However, operational system evaluation may be significantly more complex than ISO/IEC 15408 product evaluation for a number of reasons:

a) An operational system may comprise many bought-in products and custom IT developments grouped into security domains. The composition of each system security domain may be based upon several factors, such as the technology employed, the functionality provided and the criticality of the assets protected.

b) An operational system may contain multiple instances of the same product (e.g., multiple copies of an operating system provided by the same vendor) or multiple different product instances of the same product type (e.g., multiple firewalls provided by several different vendors).

c) An operational system may have security policies that apply to some security domains while not applying to others.

d) Different residual risks may be acceptable within different domains of an operational system, whereas a product counters specific threats to specific types of asset without consideration of risk.

All these factors impact on the assurance requirements for an operational system. In particular, different forms of assurance controls may be required for different security domains, depending upon the available development information, or upon the different types of functional controls selected. This means that assurance objectives have to be defined and explained as part of the solution to the security problem.

Furthermore, an operational system evaluation must cover all security controls, including those implemented in the operational environment, which are treated as assumptions in a product evaluation. In general, the type of assurance requirements for technical controls documented in ISO/IEC 15408-3 can be extended to apply to operational controls. For example, the concept of assessment of design documentation for technical controls becomes assessment of the description of operating procedures for operational controls. The actions of people implementing operational controls can be tested in a similar way to the way that the actions of programs implementing technical controls are tested.

Some ISO/IEC 15408-3 assurance requirements relating to system development may not be directly applicable to operational systems, or their assessment must be delayed until the system installation life cycle phase. Similarly, assurance in operational controls can often only be achieved in the actual operational environment, whereas technical controls are often examined and tested in their development environment.

Therefore, in order to assess the security controls of operational systems, it is necessary to generalise and modify the assurance classes for technical functionality found in ISO/IEC 15408-3. This has been done, and Annex C contains the definitions of suitable assurance classes.

A particular issue concerns assurance of the effectiveness of the controls implementing the SSF. Assurance in this aspect of technical controls is achieved by architectural design techniques such as domain separation, non-interference and non-bypassability of controls. For operational controls, analogous but somewhat different techniques are used, such as separation of duties, inspection and monitoring.

Areas where additional assurance components are needed to handle operational systems are:

a) the overall security architecture and placement of components within the architecture;

b) the configuration of the components that comprise the operational system;

c) the management policies, rules and procedures that govern operation of the operational system;

Documents
Document Sharing Hub

© ISO/IEC 2010 – All rights reserved

Full document details: PD ISO/IEC TR 19791:2010

d) the requirements and rules for interaction with other trusted and untrusted operational systems;

e) the monitoring of the non-IT controls during the operational phase of the system life cycle.

Because of its product focus, ISO/IEC 15408 assumes that a TOE will be developed in a single development environment which is distinct from the intended operational environment. This assumption is unlikely to hold true for most operational systems. Even if the operational system is developed in a separate test environment, the final stage of operational system development will be integration into the operational environment, when the operational control measures are added into the operational system. Some parts of the operational system, particularly bought-in products, may have been developed in distinct and different development environments from the main development environment.

Some components of the operational system may have already been evaluated against ISO/IEC 15408, based on assumptions about the intended operational environment. If these assumptions are shown to be true in the context of the operational system, the results of such evaluations will still apply to use of those components as part of the operational system, and can be reused.

In summary, there are five major ways that assurance in operational system controls can be obtained:

a) from analysis of the operational system design (the ASD class of Annex C, which is based on the ADV class of ISO/IEC 15408-3);

b) by testing of the operational system (the AOT class of Annex C, based on the ATE class of ISO/IEC 15408-3);

c) by verification that the operational system has been installed and configured correctly (the APR class of Annex C, which has no ISO/IEC 15408-3 equivalent);

d) by verification that the operational system is performing securely during live operation (the ASO class of Annex C, also with no ISO/IEC 15408-3 equivalent);

e) by reuse of existing evaluation results (members of the AOC class).

In addition, assurance can be obtained from examination of the requirements specification (the ASP and ASS classes, based on the APE and ASE classes of ISO/IEC 15408-3), operational documentation (AOD, based on AGD), and from vulnerability assessment (AOV, based on AVA).

Most operational system evaluations will require the use of all of these techniques.

There may be several different ways in which the required level of assurance can be obtained in an operational system. Unlike product evaluation, there are no predefined Evaluation Assurance Levels. Assurance requirements should be chosen to match assurance objectives set from analysis of the risks to the operational system and the availability of documentation, test results, and development and operational test facilities.

7.4 Composite operational systems

Many operational systems are large and complex, offering multiple functions and with a complicated internal structure. This Technical Report therefore defines a standard methodology for the description of the architecture of operational systems, based on two levels of decomposition – subsystems and components.

A component is an identifiable and distinct portion of an operational system that implements part of that system's functionality (whether security related or not). A component may comprise a single function provided by a single product, a single product with multiple functions, or an integrated set of functions implemented by the combination of customised software and operational procedures. A subsystem is a set of one or more operational system components that are capable of execution independently from the rest of the operational system. For example, a subsystem might comprise a single client or server constructed from multiple products, multiple servers and/or clients and networks, or a set of heterogeneous clients and/or servers. Some components and subsystems may already be security evaluated; others not.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

In simple operational systems, every subsystem might be made up of exactly one component; indeed, there might be only one identifiable subsystem. However, most operational systems are likely to be composed from multiple subsystems, each made up of multiple distinct components.

In ISO/IEC 15408 evaluation, the system design of the Target of Evaluation must be broken down into subsystems and modules. A subsystem in ISO/IEC 15408 is a high-level description of what a portion of the TOE is doing and how; a module is a description of system functionality at the most detailed level of breakdown provided by the system design.

In practice, subsystems as defined in this Technical Report will often correspond directly to subsystems as defined in ISO/IEC 15408. However, a component as defined in this Technical Report has a wider scope than a ISO/IEC 15408 module, for example, it may include functionality provided by non-IT means. For functionality implemented by software, a component may correspond to multiple low-level ISO/IEC 15408 module design documents, each of which will correspond to a module of code.

Typically, composite operational systems:

a) Contain several subsystems, each made up of multiple components, with different degrees and types of assurance.

b) Have a well defined control structure. This may be a single operational system “owner” or a defined set of management relationships on the various portions of the operational system.

c) Are built against specific needs for specific operation.

d) Individual components carry a large number of possible configuration options, some of which are inconsistent with the operational system security policies.

e) Enable the operational system owner to implement a different balance of technical controls and operational controls in different parts of the operational system.

The security policy may be different for the different combinations above, except for the rare case in which the operational system has a single function. Logically, all the portions of the operational system under the same set of security policies can be termed a *security domain*. This operational system decomposition of subsystems and components that are governed by the same security policy(s) is then characterized in the security policy in accordance with the appropriate risks to that domain. Functional and assurance security requirements may be identified for each security domain. As such, each security domain will have its own security policy, security problem definition, security objectives, security requirements and security documentation. However, each of these security domains operates within the larger operational system-level set of policies, security problems, objectives, requirements, and documentation. Each security domain may have its own assurance requirements based on the degree of confidence needed in that security domain and its overall contribution to the operational system. The operational System Security Target will specify the operational system security requirements, which will be a representative compilation of the security domains that comprise the operational system from an operational system context. The security domain concept is illustrated in Figure 3.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

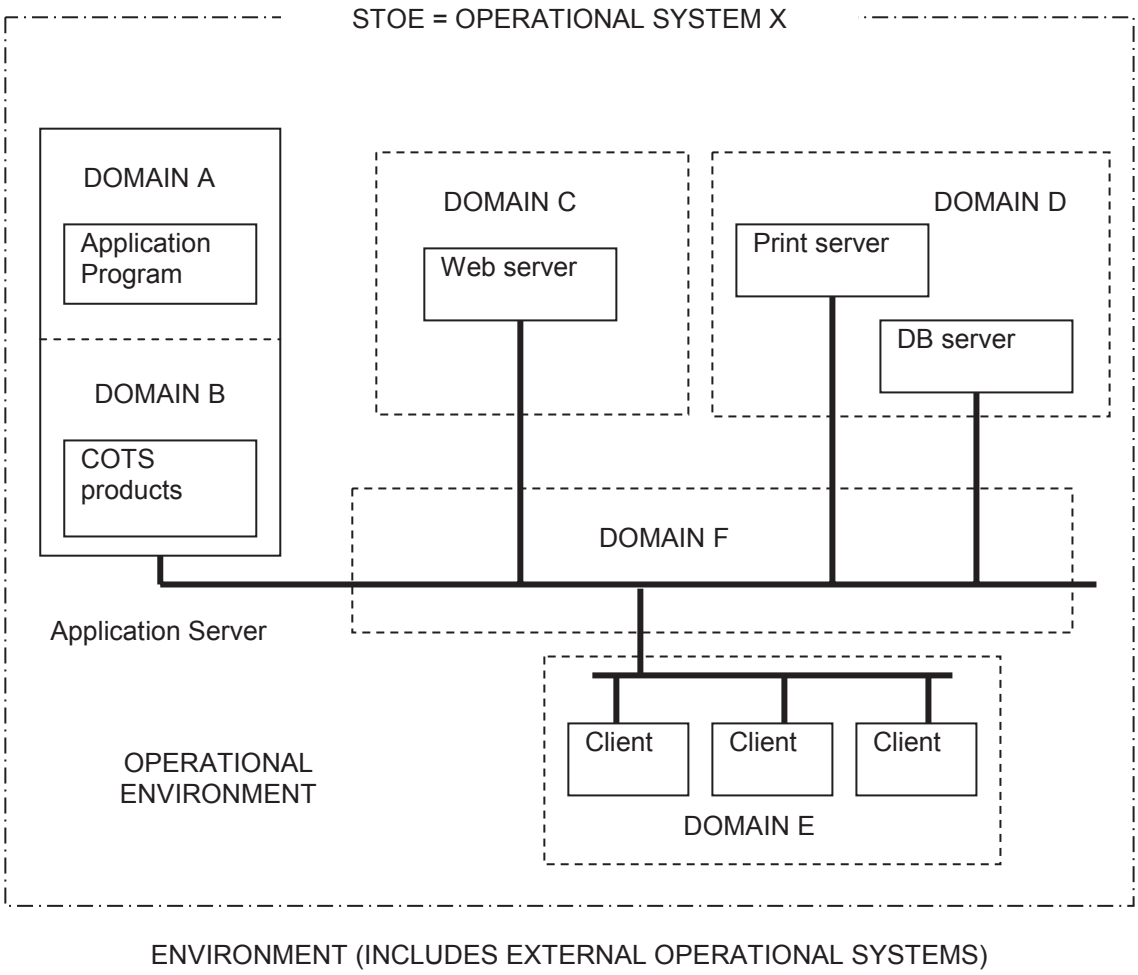

Figure 3 — Example of domains

It is important to realise that the security domain structure of a composite operational system need not be the same as its architectural structure. A subsystem may span several security domains (for example, a single client-server subsystem may have different security policies for the clients and servers). Likewise, several products from different vendors may need to be treated as separate components for build purposes but implement identical security policies and thus fall within a single security domain.

When defining a composite operational system there is a need to describe the architectural structure of the system, in particular to identify and describe the boundaries of the system, to describe the interfaces and dependencies between components of the system, and to describe the interfaces and dependencies between components of the system and its environment (e.g. users, external operational systems). All interfaces between components, and between the operational system and its surrounding environment need to be defined. The interface specifications need to cover any security requirements for the interface or for the communication links implementing the interface. In addition, the specifications must identify any trust relations or invariant security properties for the interface.

7.5 Domain Assurance

One benefit of the security domain concept is that it permits different assurance requirements to be applied to different parts of the operational system. Consider a typical server system. It will be constructed from a variety of components, such as application programs, middleware products and base software such as an operating system. The middleware and base software may have been the subject of product evaluations, but may equally well be unevaluated. For unevaluated products, the vendor may cooperate in providing the evidence needed for evaluation, but also may refuse to make the necessary evidence available. For evaluated

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

products, an Evaluation Technical Report (ETR) may be available to assist in reuse of evaluation results, but access to the ETR may be refused.

Consider the system shown in Figure 4 following. For security domain A, which is built from proprietary software, it is likely all evaluation evidence required for ISO/IEC 15408 evaluation can be made available. For security domain B, evidence to satisfy some ISO/IEC 15408 criteria might be obtained (e.g. the ADO and AGD classes and ATE_FUN) but some other criteria (e.g. the ADV and AVA classes and ATE_COV/DPT) are unlikely to be achievable as the necessary evidence will not be obtainable and may never have existed. Alternative assurances must be obtained (such as a product evaluation certificate) or residual risks accepted.

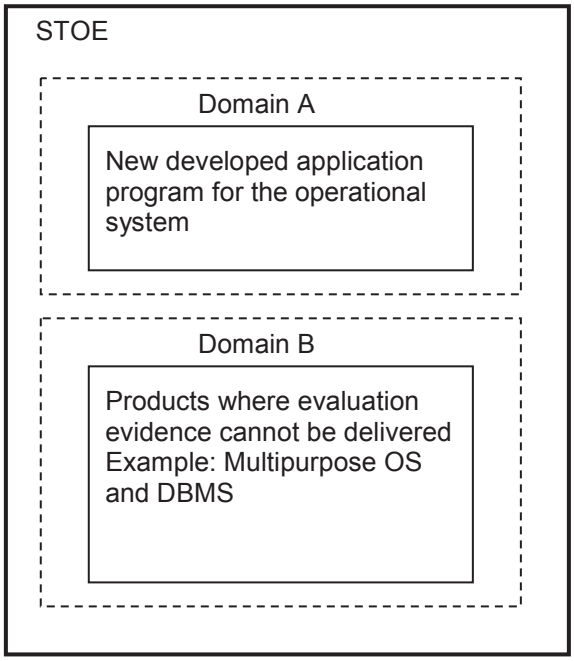

Figure 4 — Heterogeneous system composition

On the other hand, the system shown in Figure 5 following is built entirely from components for which evidence required for ISO/IEC 15408 evaluation can be obtained. This can therefore be treated as a single security domain, domain X, with homogenous assurance requirements.

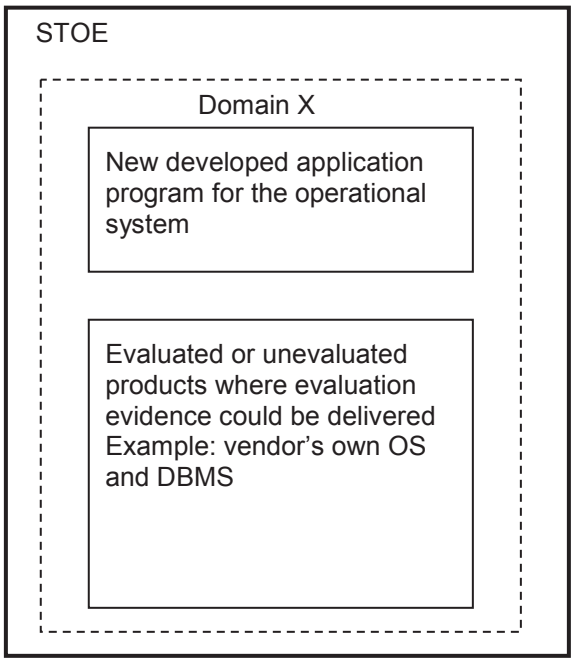

Figure 5 — Homogeneous system composition

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

In order to achieve its security requirements, one domain within a composite operational system may have dependencies on the security properties of other domains. A domain may offer security services that can be used by other domains through communications or application programming interfaces, or it may enforce security properties on other domains. This needs to be reflected within the SST for the operational system.

Security services and properties that are enforced on or made available to other domains must be identified as such with the statement of security objectives for the domain. Similarly, if a security domain has security objectives that are met by other domains, these must be identified as such within its statement of security objectives.

7.6 Types of security controls

ISO/IEC 15408 mainly specifies technical controls, i.e. security controls that are implemented by the IT components of a system. However, it also needs to specify those management controls and activities that are needed to control and monitor the technical controls.

Operational systems also need to specify operational controls. As for technical controls, operational controls have related management controls and activities which are essential to ensure that they are implemented as specified, do not fall into disuse, and are effective in practice.

Because most operational controls depend on human action which is not necessarily predictable or repeatable, management and monitoring is even more important than for technical controls. In addition, there are controls implemented by system and corporate management designed to ensure the secure operation of the system. These controls could be categorised as either operational controls (since they are part of the operation of the system) or as independent management controls (since they purely relate to management).

This Technical Report uses the same approach to management controls as in ISO/IEC 15408, namely management controls are always considered to be part of the technical or operational controls that they support.

An example of this is shown in Figure 6 following. In this example, the access control functions implemented by the server are a technical control. The registration of user attributes is a management control that supports the access control functions. However, the rules for assignment of user roles (e.g. to enforce separation of duties) is an operational control. The procedures for management of these users' roles are a management control, but one which supports this operational control.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

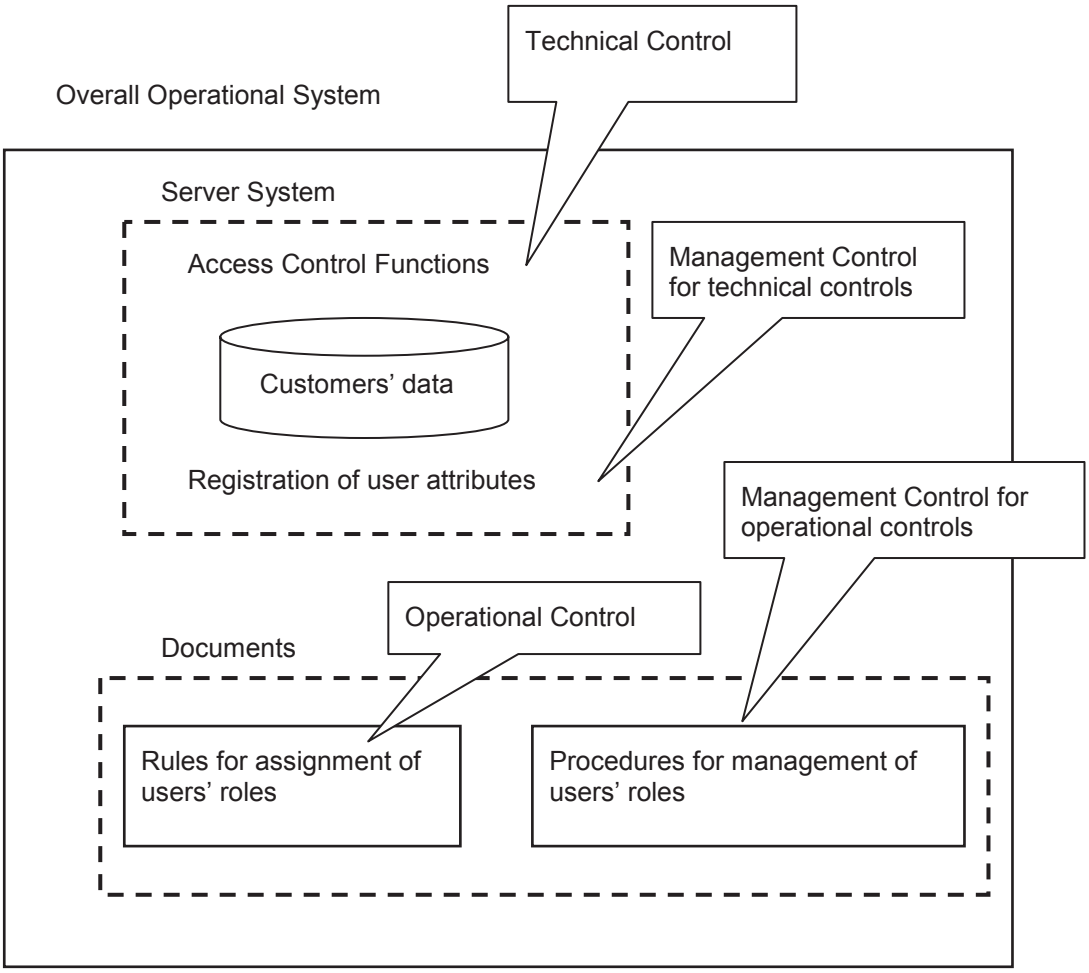

Figure 6 — Example of security controls

Operational controls may include rules and procedures as well as physical protection. An example of an operational control that would involve purely management activities is security incident reporting.

For an operational system to be secure, the technical and operational controls (including related management controls) must integrate and work together to provide coverage of all threats. In practice, the contribution to security of the system's technical controls is influenced by and dependent on the operational controls that provide the operational environment. As an example, the value of the system's "IT-asset" to the organization will determine the type of operational controls such as physical protection it is afforded, what personnel will be granted access to it, and under what conditions it will be backed up to support continuing operation. In addition, there may be integration of technical controls and operational controls such as physical protection. For example, physical access operational controls may rely on technical controls for authentication services and operational controls may provide to technical controls information about the physical presence or absence of personnel from a facility.

Many technical controls for operational systems can be expressed directly using ISO/IEC 15408-2 functional components. However, the complexity of operational systems may require additional refinement of components not normally necessary in ISO/IEC 15408 evaluation. Some examples of this are:

a) The administrator might need the capability to ascertain that the operational system configuration is as expected. The requirement for this capability would be a refinement of TSF self-testing (FPT_TST) to be included in the definition of "correct operation of the TOE".

b) The SST may wish to specifically allocate portions of security functionality to specific components within security domains. This would mean refining "the TSF" to specific portions of the TSF, e.g. "The firewall security domain shall provide a mechanism to…".

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

c) It may be necessary to define technical control functions concerning interoperability with other systems, or concerning interoperability between different components or subsystems of the operational system.

Where an ST already exists for the technical controls of an operational system, for example if the controls are provided by a bought-in and evaluated product, the ST can be used as a template for construction of the operational system security requirements. However, since operational system evaluation is risk-based, the threats and assumptions of the product ST and the associated ST rationales will have to be reassessed and possibly amended.

Most operational controls of an operational system address management and operational processes and procedures that are beyond the scope of ISO/IEC 15408 evaluation, and which therefore cannot readily be expressed using ISO/IEC 15408-2 functional components. Additional functional components are needed to handle these requirements, and suitable components are defined in this Technical Report.

7.7 System security functionality

The ISO/IEC 15408 paradigm for security functionality centres around the provision of a TOE which deals with IT security functions only. In an operational system the TOE is generalised into a STOE that includes both the technical and operational control functions.

The system security functionality (SSF) comprises those portions of the STOE (and therefore operational system) relied upon to maintain the security policies for that system. The SSF contains both technical and operational security controls.

When security requirements are defined, the system owner may choose to allocate the requirements to satisfy a functional security objective to either technical security controls, operational security controls or a combination of both.

Three terms are therefore used when defining operational security requirements. When a technical security control is required, the requirement should be expressed in the form “The TSF shall…”. This form is used because ISO/IEC 15408 already uses the term TSF for technical security controls. If an operational security control is required, the requirement should be expressed in the form “The OSF shall…”, indicating the control must be physical, personnel or procedure based. If the implementation could be either technical or operational, or a combination of the two, the requirement should be expressed as “The SSF shall…”.

It is important to note that only the security relevant portions of the STOE would be included in the evaluated SSF, and that the STOE need not represent the entire operational system. Figure 7 following provides a pictorial representation of these concepts.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

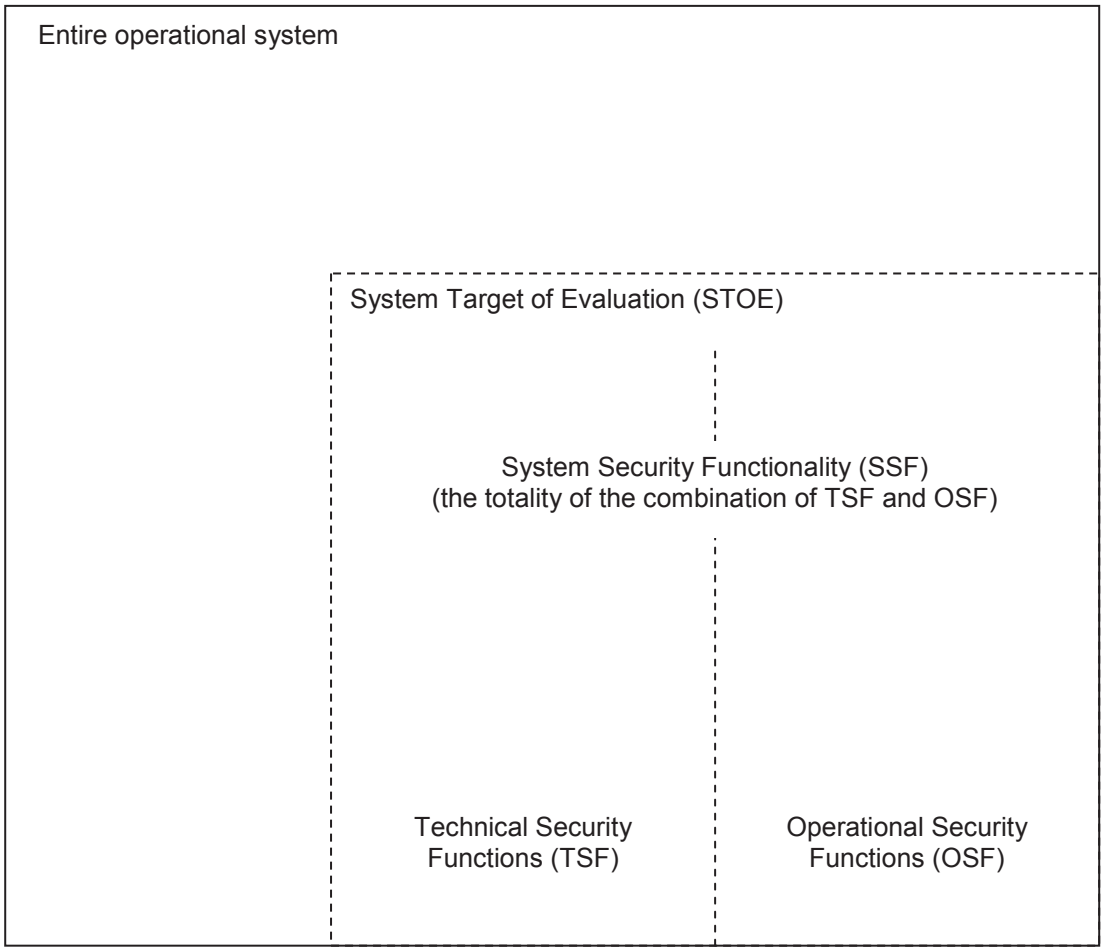

Figure 7 — System security controls

In ISO/IEC 15408 evaluation, technical security functions often have dependencies on aspects of operational security. An example is ISO/IEC 15408-2 access control element FDP_ACC.1.1:

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*].

In ISO/IEC 15408 evaluation, the access control policy and list of subjects, objects and operations would be documented, but otherwise assumed correct. In operational system evaluation, this policy and list would be evaluated as part of the assessment of data protection and personnel roles and responsibilities (see B.4.2.4, FOA_INF.1.8; and B.2.2.4, FOD_PSN.1.18). In general, rules and procedures required by TSF that must be assumed correct and applicable in ISO/IEC 15408 evaluation will be evaluated as part of an operational system evaluation.

It is important in any operational system that a good balance is chosen between TSF and OSF. TSF require the purchase of security products or the design and implementation of specific system security functionality within hardware and software. TSF therefore have an initial system development cost in time and money. On the other hand, OSF are flexible but may become ineffective over time if not policed. They typically have a low initial cost to set up, but a high cost during operation due to extra staff activities performing and checking OSF controls. Explaining the desired balance between TSF and OSF within the SST or SPP may assist in understanding the choice of functionality selected.

7.8 Timing of evaluation

Evaluation makes a determination at a given moment of time whether controls meet the requirements placed upon them. This may take place at any time in a product or system's life cycle, but in the case of a

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

ISO/IEC 15408 product evaluation normally takes place once development is complete, but before the product is put into operation.

It is very likely that a technical control that is successfully tested in a development environment will also work in the operational environment. This is much less certain for operational controls. During regular operation, the people in the operational environment may be less trustworthy, less experienced, less competent and/or less motivated than during testing in the development environment. Thus assurance from the development phase in operational controls is much less transferable to the operational environment than assurance in technical controls. It is therefore more likely that initial evaluation will extend into the operational phase, or will take place on a system that already is in operation.

Ideally, an operational system should be re-evaluated following major changes in system capabilities or risks. However, it is also necessary to re-evaluate an operational system periodically to confirm it is still meeting its objectives effectively and to determine whether adjustments are necessary to remain within the risk tolerance required.

In the first case, as for development evaluation, evaluation will provide good evidence that the operational system is capable of meeting its changed objectives but little evidence that such is the case in actual operation. It is left for management to ensure that the operational system security controls are utilised effectively. In the second case, the evaluator can confirm by examination of records of the operation of controls and of security incidents that the controls are meeting their requirements and thus working effectively.

7.9 Use of evaluated products

Where a product has been evaluated, there may be evidence available from the product evaluation that can be reused in operational system evaluation. However, the detailed evidence may not be publicly available. In some instances, this evidence can be obtained directly through an agreement with the product developer or from the authority controlling the evaluation scheme. In others, the relevant detail necessary to determine its applicability to its role in the operational system may not be possible to obtain, and system owner must then determine whether it is acceptable to accept the results without access to the evidence that contributed to those results.

Similarly, it is not necessarily the case that the results of a product evaluation are applicable to the operational system evaluation. Some reasons might be:

a) the configuration of the product during the product evaluation and the configuration of the product when integrated into the operational system may be different.

b) the assurance at which the product was evaluated is inadequate compared to the assurance to which the product is required when integrated as a component in the operational system. In this case, there may be evidence that can be reused but new evidence that will have to be generated as well.

In these instances, the operational system evaluation needs to determine the degree to which the results available can be used and what additional assurance measures may be needed. In the worst case, these components would need to be treated as unevaluated components.

When a product has not completed evaluation, it is unknown how much information might be available to support the operational system evaluation and it is unknown whether any existing product information will be confirmed by the product evaluation. When a product has not been evaluated, information usually required for product evaluation may not be available to support the operational system evaluation. Such considerations would need to be considered in the operational system evaluation.

It is essential that information is available about the security characteristics of the interfaces between products, i.e. which security functions of one product depend on security functions of a different product. It is necessary to confirm in the system evaluation that all products that depend on security functions within other products use those products in a secure manner. Often the necessary information will be documented in the ETR of the other product, but the information may not be presented in a way that is compatible. In this case, it will be necessary to look at other documents such as interface specifications and architectural design

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

documentation as part of system evaluation, and to confirm that the required security properties are present. The same applies where unevaluated products are used.

The variety and maturity of evaluated COTS products that are available for integration into an operational system limits the maximum assurance that can be achieved purely by using evaluated products. In general, it will be impractical to re-evaluate evaluated products at a higher level of assurance, as the additional evidence and developer support are unlikely to be available. If product assurance is not sufficient, it will be necessary to obtain additional assurance from alternative controls or by architectural means, such as adding firewalls or other security-specific architectural components.

Alternatively, an operational system evaluation has the ability to allocate differing levels of assurance across different operational system domains. Where assurance for a particular domain is constrained by the use of evaluated products, the Accreditor can be asked to accept the consequential increased residual risk for that single domain.

7.10 Documentation requirements

In ISO/IEC 15408 product evaluation most documentation requirements are used by the evaluators to confirm that development activities have been performed correctly, and to ensure that users have the necessary information to configure and operate the TOE in a secure manner.

In an operational system, documentation must also be provided that defines the operational controls, so that:

a) the evaluators can confirm that these controls, if properly implemented, will actually satisfy the security objectives placed upon them;

b) checks can be made during the operational phase of the system life cycle that the relevant procedures are being followed, and that both procedural and physical controls are effective.

Documentation must also be provided concerning the security properties of interfaces between different components of the operational system, and between components of the operational system and other systems within its surrounding environment, so that where a component has dependencies on the security properties of another component or system, it can be confirmed by the evaluators that these properties are valid according to the specification of that component or system.

Documentation requirements for the design of operational systems must be more flexible than permitted in product evaluation. For some subsystems and components, good security documentation, of the standard required for product evaluation at high assurance levels, may be available. However for other subsystems and components, particularly those with no intended security features, there may be little or no security-specific documentation available, and often very little design documentation at all. This means that any documentation mandated for operational system evaluation may have to be specially created for the purposes of evaluation. In some cases, the security properties of a subsystem or component may be well defined, but how they are implemented may be unknown. In such cases, creation of detailed internal design documentation may be impossible.

The basic requirement for the evaluation of the design of an operational system is that an architecture description is provided. This must identify the operational system in terms of its subsystems and interconnects between subsystems, and its external interfaces to other systems. The architecture description need not be a security-specific document. It enables the evaluator to gain an understanding of the overall architecture of the operational system, but not how it achieves its security objectives.

The second level of architectural description is to provide the evaluators with a security concept of operations document. This describes the security properties of the operational system, at a level of detail consistent with the architecture description. It must cover all modes of operation of the operational system, describe how the security functions of the operational system work together to enforce the security properties of the operational system, and how the operational system is protected from bypass or tampering with its security functionality. This document enables the security architecture of the system to be assessed, independently of how the operational system is implemented internally.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

As well as assessment of the security architecture, operational system evaluation may look at how the security features of the system have been implemented. The first level of assessment requires an interface functional specification to be provided that specifies all security functions and properties of the operational system visible at its interfaces, but without any internal details of the implementation. This enables “black box” assessment of the operational system, where claimed properties are known but there are no details of how they are achieved.

Finally, operational system evaluation may look at internal design documentation for the operational system. This can be done at three levels:

a) where all subsystem interfaces and properties are documented;

b) where interfaces and properties are documented at the level of individual components;

c) where a component level design is supplemented by implementation representations (source code, configuration scripts) for key security components.

Although operational controls will not exist until the operational system enters operation, they can be designed during the development of the operational system and their design assessed at that time.

7.11 Testing activities

The testing activities performed as part of operational system evaluation have requirements that are not usually found in ISO/IEC 15408 product evaluation.

Operational system testing assesses the effectiveness of the technical and operational control functions which counter known unacceptable risks and enforce the defined security policies. The effectiveness is determined partly through testing the security functionality of the operational system and partly through conducting penetration testing. Testing is only meaningful after the operational system has been placed into a verified secure configuration, and in the case of operational controls, can only be simulated in a test environment. There are two types of configuration: the configuration of the products to interoperate as components of the operational system and the configuration of the products to provide the security behaviour required to enable secure day-to-day operations for the business or mission that the operational system supports. The operational system’s technical controls can and should be tested prior to deployment by the system developer/integrator. This testing will provide confidence that the system’s technical control functions are working properly and effectively counter the risk to the level intended by the risk assessment. It should also identify any unintended shortcomings and provide the developer with a window to resolve those shortcomings prior to evaluation. The operational controls will then be integrated with the technical control functions at the operational site(s), where the effectiveness of the operational system integrated security controls can be evaluated.

Because operational testing is not part of product evaluation, and ISO/IEC 15408 product evaluation does not require configuration of the product to enforce a specific set of “real-world” operational policies, all products will need to be specifically tested in their operational system configuration as part of the overall operational system testing.

It may also be the case that products or subsystems within an operational system do not interoperate properly. This means the overall operational system testing must investigate and confirm the secure interaction between different components and subsystems.

The internal testing strategy may also be different for different security domains that comprise the operational system, depending on characteristics such as:

a) level of assurance required in the subsystem;

b) level of assurance already established (or not established) in products that comprise the subsystem;

c) architecture chosen and products that comprise the architecture;

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

d) technology employed;

e) placement of components in the physical environment.

7.12 Configuration management

Operational system evaluation has configuration management requirements that are not usually found in ISO/IEC 15408 product evaluation. ISO/IEC 15408 treats the life cycle of IT products from the perspective of a developer. The life cycle begins with the requirements for the product and then progresses through design, development, evaluation and production. The life cycle only considers operational concerns as it impacts the next version of the product.

Because of this, configuration management is treated primarily as an assurance measure so the evaluator can be sure that the TOE being assessed is the correct version, and can be sure that the developer knows what should be incorporated into the evaluated TOE to be distributed. The configuration management process is not part of the TOE but rather a tool for generating the TOE.

In operational systems it is not only important to know that the correct components are incorporated into the operational system but also that the configuration of the system continues to be known and understood during operation of the operational system. Therefore there may be two different configuration management systems: one for the development environment in which the operational system is produced, and another for the operational environment in which it operates. The first of these is treated as an evaluation assurance and the latter is an operational control capability.

The operational configuration management system exists primarily for the operational system administrators and security managers to be able to establish that the operational system continues to operate in a secure configuration and also to know the impact of updates, removal and insertion of operational system components. Therefore, the operational system needs to have the capability (through either procedural or technological means) to manage the configuration and to report the current configuration. The reporting capability can be used to compare the actual operational system configuration with its intended configuration to facilitate verification that the system security controls are configured correctly, and that security controls have not been changed, due to maintenance action or otherwise and not duly documented. The reporting will also serve to support assurance of any change impact analysis, as a result of continuous monitoring activities. Configuration management therefore becomes a security capability of the operational system. It can be used to provide assurance evidence that the operational controls are correctly and effectively implemented.

A further function of configuration management is to ensure that independent products that are incorporated as components within an operational system are configured securely, in accordance with their guidance documentation and any product evaluation requirements. Operational system configuration management can perform this check, by comparing the actual configuration against any constraints recorded in the product documentation.

8 Relationship to existing security standards

8.1 Overview

This Technical Report provides an extension to ISO/IEC 15408 to permit the evaluation of operational systems. As described in previous clauses, this requires extensions to the model of evaluation found in ISO/IEC 15408 and the definition of additional evaluation criteria.

For the most part, the additional processes, documentation and tasks required for operational system evaluation have been defined by extending analogous concepts within ISO/IEC 15408. The additional evaluation criteria that are required deal primarily with the operational and system integration aspects of information security, and have been derived from existing non-evaluation information security standards. In particular, this Technical Report draws heavily on two specific security best practice standards, ISO/IEC 27002 [3] and NIST SP 800-53 *Recommended Security Controls for Federal Systems* [4]. Given the

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

existence and wide acceptance of these documents, it was considered inappropriate to develop new criteria and criteria structures.

This relationship is shown in Figure 8. The SST, system security policy model, risk assessment, vulnerability assessment, guidance documents, procedures, and development design documents will all form part of the documentation provided for the system evaluation and have been generalised from ISO/IEC 15408. The criteria for assessing the operational environment and in particular the operational controls have been drawn from non-evaluation standards and guidelines.

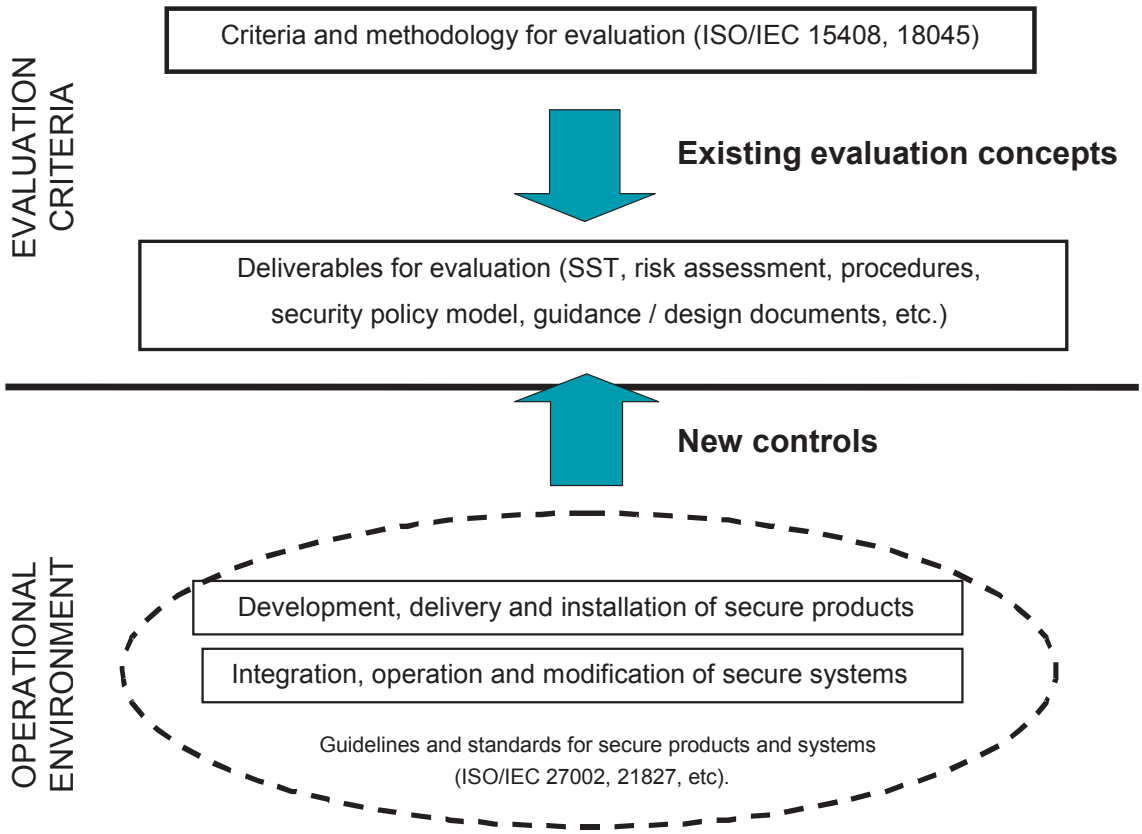

Figure 8 — Relationship between operational environment and evaluation criteria

As well as ISO/IEC 27002 and NIST SP 800-53, there are a number of other SC 27 standards, such as ISO/IEC 21827 [5] that have been used as sources. ISO/IEC TR 15443 [6] offers alternative potential approaches with respect to assurance requirements. ISO/IEC TR 15446 [7] suggests guidelines for protection profiles and security target design.

Other relevant documents include NIST SP 800-53A Guide for Verifying the Effectiveness of Security Controls in Federal Information Systems [8] and the German IT Baseline Protection Manual [9].

Concepts and specific controls have been adapted from all these documents where appropriate. However, evaluation criteria are not intended to define how to design and manage an operational system securely. The purpose of evaluation criteria is to define how to evaluate secure operational systems using evidence provided to evaluators by the system owners, developers, integrators, operators and administrators of the operational system. Evaluation criteria will therefore cover different aspects and have different emphases than the source material from these other standards and guidance documents.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Since the processes, documents and tasks defined within this Technical Report are based on existing ISO/IEC 15408 equivalents, the contributions from other standards and guidelines have been restructured into a format that is an extension of that already used in ISO/IEC 15408.

8.2 Relationship to ISO/IEC 15408

The first edition of ISO/IEC 15408 was used as the baseline for the development of this Technical Report. This revised edition has been updated for compatibility with the third edition of ISO/IEC 15408.

ISO/IEC 15408 has been used as the primary basis and framework for operational system evaluation. It provides the means to specify the requirements for technical controls. For example, it contains criteria for specification of access control policies. ISO/IEC 15408 does not provide the means to specify operational controls, but such controls can be captured within a ISO/IEC 15408-like framework. This then enables the operational system to be assessed using ISO/IEC 15408-like assurance criteria that are verified during the evaluation.

Part 1 of ISO/IEC 15408 defines the concepts of security targets and protection profiles. These requirements specification frameworks serve as the basis for enhanced targets and profiles, System Protection Profiles (SPPs) and System Security Targets (SSTs), that also cover operational controls.

Part 2 of ISO/IEC 15408 defines evaluation criteria for functional requirements. These criteria are directly applicable to the technical controls required for operational systems, and are used as the basis for defining new additional classes, families and components with focus on the operational controls of the operational system within this Technical Report. This Technical Report also captures the “as configured” aspect of the functions and mechanisms within the operational system, and requirements for the policies and procedures that must be implemented in the operational environment by the operational controls.

Part 3 of ISO/IEC 15408 defines criteria for assessing the assurance requirements. These assurance criteria are used as the basis for new assurance classes, families and components with focus on the evaluation activities that must be performed to evaluate the security controls aspects of the operational system as a single integrated unit. This includes the requirements for evidence of the policies and procedures that will be implemented in the operational environment by the operational controls.

8.3 Relationship to non-evaluation standards

ISO/IEC 27002 is a Code of Practice that recommends security controls that should be considered by an organization in order to manage the security of information assets. ISO/IEC 27002 provides recommendations for information security management to initiate, implement and maintain information security within an organization.

ISO/IEC 27002 provides a widely-accepted management framework for the control of operational security. It has been used as the principal source for identifying and specifying aspects of operational security where controls are required, and for formulating specific operational control requirements.

NIST SP 800-53 provides guidelines for selecting and specifying security controls for information systems intended for use in US Government Federal systems. US state, local, and tribal governments as well as private sector organizations comprising the critical infrastructure of the United States are also encouraged to consider the use of its guidelines. Its use is mandated by a formal US Federal Standard, FIPS Publication 200, *Minimum Security Controls for Federal Information Systems* [10]. Where appropriate, NIST SP 800-53 draws on ISO/IEC 27002 in the definition of its security controls, but it also covers other areas not directly related to information security management.

NIST SP 800-53 has therefore been used as a secondary principal source for operational controls, particularly in those areas of operational security that are outside the scope of the International Standard, ISO/IEC 27002.

There are other International Standards that address requirements for security controls. However, in general these deal with controls at too high a level to be used as a source of specific operational control requirements.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

8.4 Relationship to Common Criteria development

The Common Criteria is a technically identical standard to ISO/IEC 15408 published by the Common Criteria Development Board, an association of national schemes for evaluation and certification. Common Criteria Version 3.1 Revision 2 [11] is the equivalent to the third edition of ISO/IEC 15408, which was used as the baseline for this edition of this Technical Report.

The Common Criteria Development Board is currently soliciting ideas for major changes to the Common Criteria. If adopted, these are likely to be reflected in future revisions of ISO/IEC 15408.

9 Evaluation of operational systems

9.1 Introduction

Operational systems shall be evaluated using the general model of evaluation defined in ISO/IEC 15408-1, with extensions as defined in this clause.

9.2 Evaluation roles and responsibilities

There are three types of activity required for operational system evaluation. These are:

— production of evidence for the evaluation (which includes the risk assessment, SST specification, development and integration, operation, modification);

— evaluation (including certification of evaluation results);

— accreditation;

For each of these activities appropriate personnel shall be assigned, their terms of reference agreed and the necessary tasks performed. These activities and associated roles and responsibilities are listed in Table 1. Each of the different actions required by this Technical Report should readily map to the roles and responsibilities identified in Table 1. Each of the different actions should also map to the SST sections identified in the table.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Table 1 — Roles and Responsibilities for Operational System Evaluation

Activity	Role	Responsibility	SST Sections
Production of the evaluation evidence	Senior Management	Overall responsibility for security. Define acceptable risks. Approve actions of authorized officers	N/A
	Authorized officers of the organization	Assess and accept residual risks.	Security problem definition
	Security agency	Sets organization-wide security policies. Defines mandatory controls to be implemented by all organization systems.	Security problem definition
	System owner	Conducts risk assessment. Defines security problems to be addressed by the system (including objectives, requirements). Prepares any SPP (perhaps as part of a consortium of owners of similar systems) Authorises re-evaluation based on changes to system or its environment. Reviews system status from continuous monitoring reports.	Security problem definition Security objectives Security requirements STOE description
	Developer/ Integrator/ System Designer	Production or support of production of SST based on security problem defined by the system owner. Production of development evidence. Assists the system owner to reduce or eliminate vulnerabilities found during evaluation.	STOE description Technical controls Assurance requirements relating to development Architecture and summary specifications
	Operator/ Administrator/ Maintainer	Support of production of SST. Production of operational evidence. Assists the system owner to reduce or eliminate vulnerabilities found during system operation.	Operational controls Assurance requirements related to operation Architecture and summary specifications
Evaluation	Evaluator/ certification agent	Evaluates system based on security requirements articulated in SST, to make determination of system capability to meet its security requirements at that point in time. Provides independent assessment of system security operations throughout system operation Performs re-evaluation, as required, to support changes to the system or its environment. Certifies the evaluation results. Provides evaluation and certification reports to system owner, with recommendations, as required, to support system accreditation/authorization	All
Accreditation	Accreditor	Authorizes system for use or confirms to the authorized officer that anticipated residual risks are acceptable.	Security problem definition

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

9.3 Risk assessment and determination of unacceptable risks

Prior to operational system evaluation, the system owner shall assess the scope of the operational system, determine the assets that need protecting, and, in concert with the authorized officer or designated representative from higher management, determine the level of risk which the organization is willing to accept that each asset of the operational system could be lost, damaged or compromised.

The system owner shall then conduct a risk assessment covering all assets of the operational system. This risk assessment should identify all possible risks to the operational system, including those risks that are countered or eliminated by existing security controls. These existing controls shall be documented as part of the risk assessment, so that they can be included in the SST description of security objectives.

NOTE This Technical Report does not prescribe any particular model or form for risk assessment. Further information about risk assessment of ICT systems can be found in ISO/IEC 27005.

Where risks to assets exist that are above the level of risk that the organization is prepared to tolerate, the system owner shall identify a proposed course of action to reduce the risk to an acceptable level. This may take the form of:

— risk acceptance, accepting the increased risk and acknowledging liability for the consequences should the risk be realised;

— risk transfer, transferring the risk or liability for its consequences, to another party;

— risk avoidance, such as by abandoning the activity which causes the risk;

— risk reduction or elimination, reducing the risk to an tolerable level through the implementation of evaluated countermeasures within the operational system to reduce the likelihood and/or the impact of the risk.

Following this analysis, each risk shall then be categorised as acceptable or unacceptable from the point of view of the operational system. Acceptable risks are those which are to be tolerated, accepted, transferred or avoided. Unacceptable risks are those that are to be reduced or eliminated.

Where risks are unacceptable, the system owner in conjunction with the system developer shall identify and specify technical and operational security controls to be implemented as countermeasures. The system owner in conjunction with the system developer shall also identify and specify assurance controls to confirm that the risk that technical or operational security controls fail to meet their security objectives as countermeasures is reduced to a level that the organization is prepared to tolerate.

As part of the operation phase of the system life cycle, the system owner shall periodically review the risk assessment, to determine whether:

— there are changes to business assets;

— there are new risks, or changes to risks to assets;

— the existing countermeasures are still appropriate.

The owner shall then determine if there is a need for the system to be re-evaluated to confirm the adequacy and continued effectiveness of the operational system security controls against the revised risk assessment.

9.4 Security problem definition

The system owner shall define the security problem to be addressed by the operational system and assessed by evaluation. The description of the security problem shall include:

— the results of the risk assessment;

— any organizational security policies that apply to the system.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

9.5 Security objectives

The system owner shall prepare a statement of security objectives for the operational system. The security objectives shall provide a concise statement of the intended response to the security problems faced by the operational system.

For operational system evaluation, two types of security objective must be distinguished:

a) functional security objectives that will be satisfied by technical and operational controls implemented within by the operational system;

b) assurance security objectives that will be satisfied by assurance controls (e.g. verification activities).

In ISO/IEC 15408 evaluation, functional security objectives are normally implemented exclusively by technical controls, since the operational environment is not evaluated, but defined by assumptions within the security problem definition. Within an operational system evaluation, the operational environment is included within the scope of evaluation, and functional objectives may be implemented as technical controls, operational controls, or a combination of the two. Of course, both technical and operational controls may involve associated management controls or actions.

The statement of security objectives shall cover all security objectives, including both objectives that are already satisfied by existing controls and objectives that must be satisfied by additional controls implemented as part of the operational system.

Different security domains may have different assurance security objectives as well as different security functional objectives. This might be because different levels of residual risk will be accepted in the different domains.

Some security objectives might apply to the whole of the STOE but must be implemented using different functional or assurance security requirements in different domains. This might be because the same types of controls are not possible in all domains, or because equivalent assurance is required in all domains, but must be obtained by different means.

9.6 Security requirements

9.6.1 Introduction

The system owner shall prepare a set of security requirements for the operational system. The security requirements shall define a set of security controls to be implemented within the operational system to satisfy the functional security objectives and shall define the assurance requirements to confirm that those controls satisfy the assurance security objectives.

9.6.2 Security functional requirements

Technical security controls shall be selected from the functional classes defined within ISO/IEC 15408-2. Operational security controls shall be selected from the functional classes defined in Annex B.

Where controls may be implemented by a combination of technical and operational security measures, they shall be selected from the functional classes defined in Annex B. Suitable controls are indicated by the use of the abbreviation SSF to indicate that either technical or operational measures might be used.

Controls which must be implemented as a specific combination of technical and operational measures shall first be subdivided into separate technical and operational requirements, and then specified as defined above.

If no suitable components exist within either ISO/IEC 15408-2 or Annex B of this document to satisfy some specific security functional objective, additional custom components shall be devised and defined in accordance with the procedure defined in ISO/IEC 15408-1, Annex B.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Table 2 shows a comparison between the functional classes defined in ISO/IEC 15408 and this Technical Report, and their applicability to operational system evaluation.

Table 2 — Comparison of functional classes

ISO/IEC 15408	Operational system	Applicability and coverage
Security audit (FAU)	Applicable to operational systems	Same as 15408
Communication (FCO)		
Cryptographic support (FCS)		
User data protection (FDP):		
Identification and authentication (FIA)		
Security management (FMT)		
Privacy (FPR)		
Protection of the TSF (FPT):		
Resource utilisation (FRU)		
TOE access (FTA)		
Trusted path/ channels (FTP)		
	Administration control (FOD)	Policy, Personnel, Risk management, Incident management, Security organization, Service agreement
	IT System control (FOS)	Policy, Configuration, Network security, Monitoring, Personnel control, Operational system assets, Records
	User Assets control (FOA)	Privacy data protection, User assets
	Business control (FOB)	Policy, Continuity
	Facility and Equipment control (FOP)	Mobile, Removable equipment, Remote equipment, System, Facility
	Third Parties control (FOT)	Management
	Management (FOM)	Security parameter, Asset classification, Personnel responsibility, Security organization, Security reporting

9.6.3 Security assurance requirements

Assurance requirements shall be selected from the assurance classes defined within Annex C. The assurance classes of Annex C are based for the most part on assurance classes from ISO/IEC 15408-3, but generalised for applicability to both technical and operational security measures.

If no suitable assurance components exist within Annex C that will meet a particular assurance objective, it may be possible to use assurance components from ISO/IEC 15408-3. If no suitable assurance components exist within either Annex C or ISO/IEC 15408-3, additional custom components shall be devised and defined in accordance with the procedure defined in ISO/IEC 15408-1, Annex B.

Table 3 shows a comparison between the assurance classes defined in ISO/IEC 15408 and this Technical Report, and their applicability to operational system evaluation.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Table 3 — Comparison of assurance classes

ISO/IEC 15408	Operational system	Applicability
APE: Protection Profile evaluation	System Protection Profile evaluation (ASP)	Specification of SPP
ASE: Security Target evaluation	System Security Target evaluation (ASS)	Specification of SST
ADV: Development	Operational system architecture, design and configuration document (ASD)	Interfaces and configuration of components External interfaces Architecture, information flow, access to STOE Mode of operation / transition condition
AGD: Guidance documents	Operational system guidance document (AOD)	Rules and procedures for User and Administrator guidance Confirmation and verification (operation time)
ALC: Life cycle support	Operational system configuration management (AOC)	Configuration management (plan, CM system) Secure configuration of component products Reuse of product evaluation results
ATE: Tests	Operational system test (AOT)	Functional, coverage and depth test for SSFs Independent testing for SSFs Regression testing at maintenance/ modification time
AVA: Vulnerability assessment	Operational system vulnerability assessment (AOV)	Detection of insecure states and their recovery Penetration testing (both operation time and after maintenance/modification)
ACO: Composition	None	Not applicable to operational systems
-	Preparation for live operation (APR)	Awareness training and Communication of SSFs Confirmation and verification (operation time)
-	Records on operational system (ASO)	Records of SSFs log Management review on SSFs Independent verification of SSFs Confirmation and verification of records,

9.7 The System Security Target (SST)

The system owner shall record the security problem definition, the security objectives and the security requirements for an operational system in a System Security Target (SST). The owner shall also obtain and document the other information required to complete the SST as identified in Annex A.

NOTE A System Security Target is distinct from a Site Security Target, a form of documentation used in some certification schemes to enable reuse of product development environment evaluation results. Site Security Target is also often abbreviated to SST.

Where the owner of an operational system wishes to define the requirements for an operational system in an implementation independent way, he may first produce or adopt a System Protection Profile (SPP). The mandatory and optional contents of an SPP are defined in Annex A.

The SST serves as the basis for both the documentation of the operational system security capabilities and for the evaluation of those capabilities within the STOE. As such, it provides the evidence and information necessary to perform an evaluation.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

An SST differs from an ST due to its focus on both the technical and operational controls of the operational system. An SST may be broken down into several distinct security domains with different functional and assurance controls. However, like an ST, an SST can be evaluated for consistency independently from the STOE.

Subsequently, evaluation of the STOE may identify inconsistencies between the SST and the STOE. The types of discrepancies may include:

a) aspects of the operational system environment as implemented disagree with the operational system environment as specified in the SST;

b) aspects of the operational system security functionality as implemented are different from the operational system security functionality as specified in the SST;

c) aspects of the operational system interfaces and interconnects and their behaviour as implemented disagree with the operational system interfaces as specified in the SST.

The system owner must determine whether the implemented environment, functionality or interface/interconnect is as required, and the description in the SST is wrong, or if the environment, functionality or interface/interconnect should be as specified in the SST. Upon completion of the assessment, appropriate changes must be made. These changes may result in changes to the SST and/or to the operational system. For these reasons, it is impossible for SST evaluation to provide a final verdict as to whether the SST is a correct representation of the desired operational system. Only when STOE evaluation is complete and inconsistencies have been resolved can the SST be confirmed as a correct representation.

Table 4 shows a comparison between the ST defined in ISO/IEC 15408 and the SST defined in this Technical Report, and their applicability to operational system evaluation.

Table 4 — Comparison of security target elements

ISO/IEC 15408	Operational system	Applicability to operational systems
Introduction	Introduction	IT / operational parts of the STOE and interfaces to external operational systems should be defined. Domain organization could be defined.
Conformance claims	Conformance claims	Compliance claim for SPPs, PPs, and/or STs could be defined.
Security problem definition	Security problem definition	Risks should be defined instead of threats. Assumptions must not be defined, because environments are reality.
Security objectives	Security objectives	Security objectives for IT and operational parts of the STOE and external operational systems should be defined.
Security requirements	Security requirements	Functional requirements for IT parts of the STOE Operational requirements for operational parts of the STOE Assurance requirements should be defined.
TOE summary specification	STOE summary specification	Functional, operational and assurance specifications should be described.
	Domain introduction	IT / operational parts of the domain should be defined.
	Domain security problem definition	Risks and OSPs should be defined
	Domain security objectives	Security objectives for IT and operational parts of the domain should be defined.
	Domain security requirements	Functional requirements for IT and operational parts of the domain should be defined. - Assurance requirements for the domain should be defined.
	Domain summary specification	Functional, operational and assurance specifications for the domain should be described.
	Domain compliance claim	Compliance claim for SPPs, PPs, and/or STs for the domain could be defined

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

9.8 Periodic reassessment

The system owner shall specify controls to ensure that the results of evaluation of an operational system remain valid during system operation.

This can be done in two ways:

— Management controls can be specified to check periodically that the configuration of the technical controls has been maintained and the operational control measures are being faithfully implemented. To do this, a set of processes and procedures must be created to manage the security impact of changes as they occur in the operational environment. It must include regression testing of all system changes, to ensure that system controls are not modified or disabled.

— An evaluator can periodically re-evaluate the operational system STOE, concentrating on whether the combination of technical and operational control measures needs adjustment to meet the changing security requirements of the organization, and to confirm that operational processes and procedures are being applied effectively.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Annex A
(normative)

Operational system Protection Profiles and Security Targets

A.1 Specification of System Security Targets

A.1.1 Overview

This section defines the concept and content of a System Security Target (SST).

Table A.1 — Summary of ST and SST differences

	"Product" ST	SST
Specification framework	Single "box" focus	Focus increase to address larger and more complex grouping of system components, which can be decomposed into security domains.
Security objectives	IT specific; and no direct mapping of security objectives to assurance requirements.	Specific objectives traced back to specific assurance requirements. Operational controls (physical, procedural and policy) relationships and their contribution to system security documented to and assurance measures selected.
Environment documentation	Minimally addressed outside of risk assessment arena and seen as assumptions	Should be clearly defined and documented. No assumptions.
Risk Assessment	Cites non-IT, especially procedures, as assumptions and product compliance related	Identifies risks as "known" and operational controls may call for evaluation as to their adequacy in integrated system environment
TOE description	IT focused	Defines technical and operational controls environment, their interfaces, and their inter-relationships.
Compliance claims	Strictly IT functionality	Can re-allocate functionality between system components (e.g., technical and operational controls).
System architecture	Based on "stand-alone" product	Typically broken into distinct security domains with different controls. Addresses interactions between domains and between domains and the surrounding environment

The SST provides a specification for the implemented security capabilities of an operational system as it is employed in a specific operational context to counter assessed risks and/or enforce stated organizational security policies to achieve an acceptable level of residual risk. The operational system is composed of an integrated combination of technical and operational control functions. The SST describes the requirements and behaviour of the functions that implement the security objectives through a combination of technology-based and operational-based mechanisms. Additionally, the SST describes the measures that provide

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

assurance in terms of the ability of the operational system to meets its functional objectives while operating at an acceptable level of residual risk.

The SST serves as a suitable basis for conducting the operational system evaluation. The SST must therefore provide a description of the operational system that is:

a) Sufficiently complete. Each risk is sufficiently countered and each organizational security policy is sufficiently enforced by the combination of technical and operational control functions.

b) An appropriate and necessary solution for the stated problem. The combination of technical and operational control functions is effective in countering the unacceptable risks and enforcing the organizational security policies, and the assurance measures provide sufficient assurance that the security functions are correctly and effectively implemented.

c) An accurate instantiation of any SPP, PP or ST to which it claims compliance, either in whole or in part.

The concept and structure of an SST are based on expansion of the ISO/IEC 15408 concept and structure for Security Targets (STs). Table A.1 above provides a summary of the conceptual differences between a ST and SST.

A.1.2 SST contents

An SST shall conform to the content requirements described in this annex. An SST should be presented as a user-oriented document that minimises reference to other material that might not be readily available to the SST user. The rationale may be supplied separately, if that is appropriate.

An SST shall include the following:

a) a common part applicable to the whole STOE;

b) domain parts, one for each security domain defined within the STOE, and describing the unique aspects of that domain.

The common part shall contain:

a) SST introduction;

b) conformance claims;

c) security problem definition;

d) security objectives;

e) extended components definition;

f) security requirements;

g) STOE summary specification.

For each security domain forming part of the operational system, the following shall be included:

a) security domain introduction;

b) security domain conformance claims;

c) security domain security problem definition;

d) security domain security objectives;

e) security domain security requirements;

f) security domain summary specification.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

Certain sections of the SST may be empty if there is no relevant information to be provided. Conformance claims only appears if the SST claims compliance with one or more SPPs, PPs or STs. Certain subsections of the security domain information are optional. They need only be specified if security domains have unique security problems, objectives or requirements that do not apply to the STOE as a whole.

The specifications presented in this section are derived in part from the ST specifications contained in ISO/IEC 15408-1, Annex A, and in part from additional SST requirements defined in this Technical Report.

A.1.3 SST introduction

The SST introduction shall identify the SST and STOE, and provide an STOE overview, an STOE description and domain organization. It shall contain document management and overview information as follows:

a) The **SST/STOE identification** shall provide the labelling and descriptive information necessary to control and identify both the SST and the STOE to which it refers.

b) The **STOE overview** shall summarize the objectives of the STOE in narrative form. The overview should be sufficiently detailed for a potential user of the SST to determine whether the SST is of interest.

c) The **STOE description** shall outline the functions and boundaries of the STOE in narrative form.

d) The **domain organization specification** shall describe the breakdown of the STOE into domains with unique security requirements.

There is no prescribed content or layout for the STOE overview, but it should specify the purpose or mission of the operational system, an overview of the system in the context of its operational environment and descriptions of the system from the point of business, management and technical architecture. It should define the relationship between the STOE and external operational systems, and the interfaces between the STOE and those systems.

There is no prescribed content or layout for the STOE description, but it should describe the scope and boundaries of the STOE from both logical and physical points of view. It should also describe the organisation and location where the STOE was developed, including any unique characteristics for individual domains e.g. domains based on commercial products.

Operational systems are composed of one or more security domains. Each security domain includes some components and may have its own security assurance requirements. The domain organization specification shall document the organization of the security domains, their domain boundaries and their interfaces in detail.

In the best possible case, the STOE will be composed of components that fully define the operational system as a closed entity whereby there are no interfaces to external operational systems that are not included in the evaluation. From a practical standpoint, this best case is sometimes not possible and it is necessary to define a clear partition between those parts of the operational system that will undergo evaluation as an integrated unit and those parts that are outside the scope of the evaluation. The components that are outside the scope of the evaluation are treated as part of external operational systems.

The operational system concept has basis in the interfaces that exist between the components of the operational system. Without interfaces, there is no operational system. Therefore, the interfaces are critical to the operational system definition and equally critical to the ability of the operational system to enforce a security policy across its interfaces. The domain organization specification will provide an overview of the various components of the operational system, including how they interface. The details of the interfaces are left to interface specifications for the design and integration of the operational system. However, the domain organization specification should identify all security properties of individual domains that are enforced on other domains, and also all security services offered by individual domains that are available to other domains.

A.1.4 Conformance claims

This section is only applicable if the SST claims compliance with one or more SPPs, PPs, STs or security requirement packages. The conformance claims section provides evidence that the SST is an acceptable

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

instantiation of any SPP, PP, ST or requirements package for which compliance is being claimed. A conformance claims rationale shall demonstrate consistency between the SST security objectives and requirements and those of any SPP, PP, ST or requirements package to which conformance is claimed.

The focus of the compliance claim is on “equivalence” in terms of meeting the base set of criteria stated in the SPPs, PPs, STs or requirements packages. The SST may be a functional superset of a package or profile but it shall not be a sub-set.

A primary difference between operational system and product compliance claims is that for the operational system it may be appropriate to reallocate functionality between the technical and operational control portions of the operational system because it is all considered part of the STOE. In a product evaluation, allocation of IT functionality to the non-IT environment changes the entire concept of the product and defeats the purpose of the product evaluation activity.

A.1.5 Security problem definition

A.1.5.1 Overview

The SST security problem definition section shall provide a coherent, consistent and sufficiently complete definition of the security problems that the operational system is intended to address. The security problems are stated in terms of the risks that will be countered by the operational system and the organizational security policies that support and govern the use of the operational system to reduce operational system risk to an acceptable level.

The security problem definition shall define:

a) all risks that are applicable to the STOE;

b) all organizational security policies that apply to the STOE.

In this section, security problems that are concerns to the whole STOE should be defined. It is possible that different security domains of the STOE will execute in different operational environments, and as a result, there may be different or unique risks or policies that must be addressed independently by different security domains of the operational system. For each security domain, additional security problems that are concerns to that domain only should be defined.

Recognising that this section is preceded by the STOE introduction, it is important that any material presented in this section of the SST is consistent with the information provided in the STOE introduction.

A.1.5.2 Risk identification

In this section all risks that are applicable to the STOE shall be described, based upon a risk assessment of the operational system. Each risk shall be categorised as acceptable or unacceptable, i.e. requiring reduction or elimination through technical or operational controls within the STOE. Those risks that are accepted must still be identified, since acceptability of risks may change over time.

The list of risks shall include risks relating to the development of the operational system. The description of each risk shall be sufficiently detailed to identify the assets that can be damaged or compromised, the threats and vulnerabilities applicable to each asset and the impact of successful attack. Threats should be characterised in terms of the associated threat agents and their potential adverse actions on assets. The risk assessment should identify all possible risks to the operational system, including those risks that are countered or eliminated by existing security controls.

NOTE Threat agents can include natural events such as accidents, as well as human beings and computer processes acting on their behalf.

With time, additional risks may be identified or the consequences of a security breach may change. Risk assessment must be repeated through the system life cycle, and, if necessary, the SST updated and the operational system re-evaluated.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

In this section, those risks should be identified and categorised that relate to operation of the system as a whole, for example risks relating to employees or business assets. Some risks, for example risks relating to application processing, may only apply to a particular security domain and should be therefore be identified and analysed for that domain only.

A.1.5.3 Organizational security policies (OSPs)

In operational systems, the OSP scope is expanded to include the life-cycle management and operations issues that are not addressed during a ISO/IEC 15408 evaluation. These policies include:

a) governing laws, mandates and directives;

b) business continuity;

c) inter-organizational use agreements (i.e. Inter-Service Agreement (ISA) or Memorandum of Understanding (MOU)).

A.1.6 Security objectives

The security objectives contained in the SST security objectives section shall provide a coherent, consistent and sufficiently complete high level description of the security solution based upon the definition of unacceptable risks and organizational security policies in the security problem definition section. The high level description is made in terms of functional security objectives that are subsequently allocated to the technical and operational controls of the operational system or to other operational systems that interface to the operational system. A security objectives rationale shall demonstrate that the stated security objectives are traceable to all of the aspects identified in the SST security problem definition and are suitable to cover them. It should provide complete traceability between the stated security objectives and all aspects of the statement of the security problem, and it should provide sufficient information to determine whether the security objectives sufficiently counter the stated unacceptable risks and enforce the stated organizational security policies.

There is another type of security objective which governs the verification activities to generate and analyse the evidence and to observe or test the implementation to determine that it is implemented in accordance with the requirements. This type of security objective is typically not justified in ISO/IEC 15408 evaluation (i.e. specific objectives are not traced back to specific assurance requirements). As a result, there is little, if any substance in product PP/ST documents that justifies the assurance measures selected. However, for an operational system, a clear statement of assurance objectives is needed, derived from assurance aspects of the security problem, in order to justify assurance measures that will apply to the whole of the operational system. These measures may apply either to the development environment of the TOE or its operation.

The statement of security objectives must cover all required controls, including both controls that already exist and those that must be created as part of the implementation of the operational system.

Security objectives selected to implement one aspect of the security problem may also provide solutions or partial solutions in other areas. In particular, security objectives may address risks which have been accepted following risk assessment, i.e. categorised as tolerable, acceptable, transferable or to be avoided. Such linkages must still be identified and recorded, as acceptability of risks may change over time.

The security objectives provide the highest level statement of the strategy and philosophy for countering the defined risks and for enforcing the defined organizational security policies. In operational systems, it is critical that security objectives are precise. Precision is required both in terms of how the objectives trace back and cover statements made in the security problem definition and also in terms of how the security objectives allocate the solution to the operational system components and physical processes.

The security objectives must be considered against the stated risks and organizational security policies in finer detail when compared to how they are considered in the product sense. This is because of the impact the environment has in regards to the operational system evaluation and the detailed knowledge about the environment that must be captured in the security objectives.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

In addition, operational system security objectives must ensure there is a balance achieved in the management of overall residual risk.

It is possible that different security domains of the operational system will support and execute in different operational environments. For example, the capability for the operational system to monitor internal network traffic might be configured as “off” whereas the capability for the operational system to monitor incoming traffic to the internal network is configured as “on”. As a result, there may be different or unique security objectives for different security domains. There may also be additional assurance objectives for particular security domains to meet unique assurance requirements that apply only to those domains.

A.1.7 Extended components definition

In some cases, suitable components to describe the security requirements will not exist within ISO/IEC 15408 or this Technical Report. In such cases, new components shall be defined within this section of the SST. These extended components can then be used to define additional functional and additional assurance requirements.

A.1.8 Security requirements

The security requirements section shall provide a complete and consistent set of security requirements for the STOE. This includes both the operational system security functional requirements and the operational system security assurance requirements. It applies to both the technical and operational control measures to be provided to meet the operational system security objectives. These requirements must provide an adequate basis for the development of security processes, procedures, mechanisms and services that may be configured to enforce defined policies and to counter identified risks. A security requirements rationale shall demonstrate that the set of security requirements is suitable to meet and traceable to all SST security objectives.

In some cases, the security requirements for an operational system may be stated without justification; i.e. they are not derived from security objectives which are themselves derived from definitions of security problems. In these cases, the objectives and security problem definition sections of the SST may be omitted.

The security requirements section shall describe all system security functions and systems security assurances required by the operational system in terms of completed security components.

It is possible that different security domains of the operational system will support and execute in different operational environments. As a result, there may be different or unique security functional requirements for each security domain, required to meet the unique security objectives of that domain. Similarly, security assurance requirements need not be applied across all operational system components to the same depth and breadth. It is necessary to allocate the appropriate level and types of assurance to the various security domains defined in the SST.

A.1.9 STOE summary specification

The STOE summary specification shall provide a coherent, consistent and sufficiently complete high-level description of the security mechanisms, services, interfaces, operational controls and assurance measures, and demonstrate that these satisfy the specified operational system security requirements. A STOE summary specification rationale shall show that the STOE security functions and assurance measures are suitable to meet the STOE security requirements.

It is necessary that enough of the operational system architecture is defined in the SST for a reader to understand the solution being provided to meet the requirements. Details on the definition of subsystems, interfaces and interconnections, and the allocation of functional requirements to the various subsystems that comprise the operational system should be left for design documentation to follow. The architecture and summary specification should address interactions between security domains and interactions between domains and their environment.

© ISO/IEC 2010 – All rights reserved

Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010

A.1.10 Security domain information

The security domain information section of the SST shall provide information concerning each security domain forming part of the complete operational system. It shall provide an accurate and correct identification of each security domain and any domain-specific security information that is required.

If there is only one security domain within the STOE, it need not be explicitly named or identified, and this section should be omitted.

The security domain information for each security domain shall contain the following:

a) The **security domain introduction** shall provide the labelling and descriptive information necessary to control and identify the security domain and the STOE to which it refers, and summarize the domain in narrative form. The overview should be sufficiently detailed to understand the business functions of the security domain and its security requirements.

b) The **security domain conformance claims** shall define any conformance claims that are unique to the domain. If the security domain has no unique conformance claims, this section may be omitted.

c) The **security domain security problem definition** shall define any security problems that are unique to the domain. This shall include policies and risks that are unique to the domain. If the security domain has no unique security problems, this section may be omitted.

d) The **security domain security objectives** shall define any security objectives that are unique to the domain. This shall include any security objectives that are available to other domains, or which are implemented by other domains. If the security domain has no unique security objectives, this section may be omitted.

e) The **security domain security requirements** shall define any security requirements that are unique to the domain. If the security domain has no unique security requirements, this section may be omitted.

f) The **security domain summary specification** shall define any mechanisms, services, interfaces, operational controls and assurance measures that are unique to the domain. If the security domain has no unique mechanisms, services, interfaces, operational controls or assurance measures, this section may be omitted.

A.2 Specification of System Protection Profiles

A.2.1 Overview

This section defines the concept and content of a System Protection Profile (SPP).

Table A.2 — Summary of PP and SPP differences

	Product PP	System PP
Specification Framework	Single “box” focus	Focus increase to address larger and more complex grouping of products, which comprise operational system, with physically dispersed distribution, and integrated security controls
Focus	More narrow and IT specific	Broader, flexible and incorporates security controls aspects of system security – flexible to account for varying business cases
Operational Controls (Physical, OSPs, Personnel..)	Minimally addressed outside of risk assessment arena – assumes environment contributions	Addresses as full partner with technical controls as contributor to system security to meet operational needs
Risk Assessment	Cites non-IT, especially procedures, as assumptions and product compliance related	Identifies risks as “known” and operational controls may call for evaluation as to their adequacy in integrated system environment
TOE description	Narrow and IT focused	Broader incorporating internal interfaces as well as interfaces to “external/remote” systems, subsystems, and components.

© ISO/IEC 2010 – All rights reserved
Documents
Document Sharing Hub
Full document details: PD ISO/IEC TR 19791:2010