

---

---

**Information technology — Security  
techniques — Security assessment of  
operational systems**

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

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC TR 19791:2010](https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010)

<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO/IEC TR 19791:2010](https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010)

<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010>



**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](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

# 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

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
<b>Annex C</b>	<b>(normative) Operational system assurance requirements.....</b>	<b>84</b>
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
<b>Annex D</b>	<b>(normative) Operational System evaluation methodology .....</b>	<b>162</b>
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
<b>Bibliography</b>	.....	<b>235</b>

[ISO/IEC TR 19791:2010](https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010)  
<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/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.

## 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.

# 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 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*

### 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]

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

#### 3.5

##### **operational system**

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

<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010>

#### 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]



**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

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[ISO/IEC TR 19791:2010](https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/iso-iec-tr-19791-2010)

<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-4faa3a6a423c/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.

## 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.

<https://standards.iteh.ai/catalog/standards/sist/13d40856-53b6-43a2-952e-19791-2010>

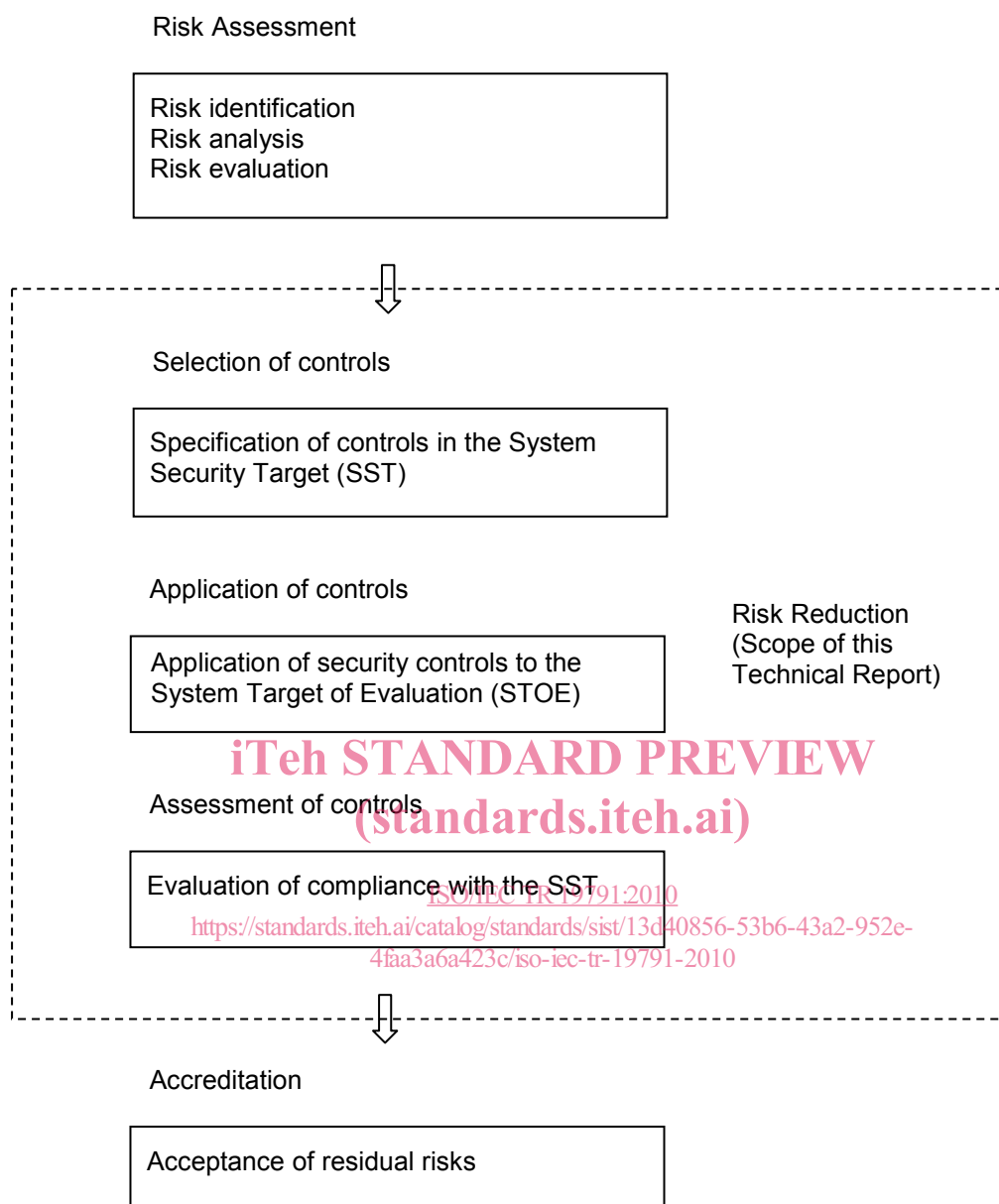
### 6.2 Establishing operational system security

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.



**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

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.

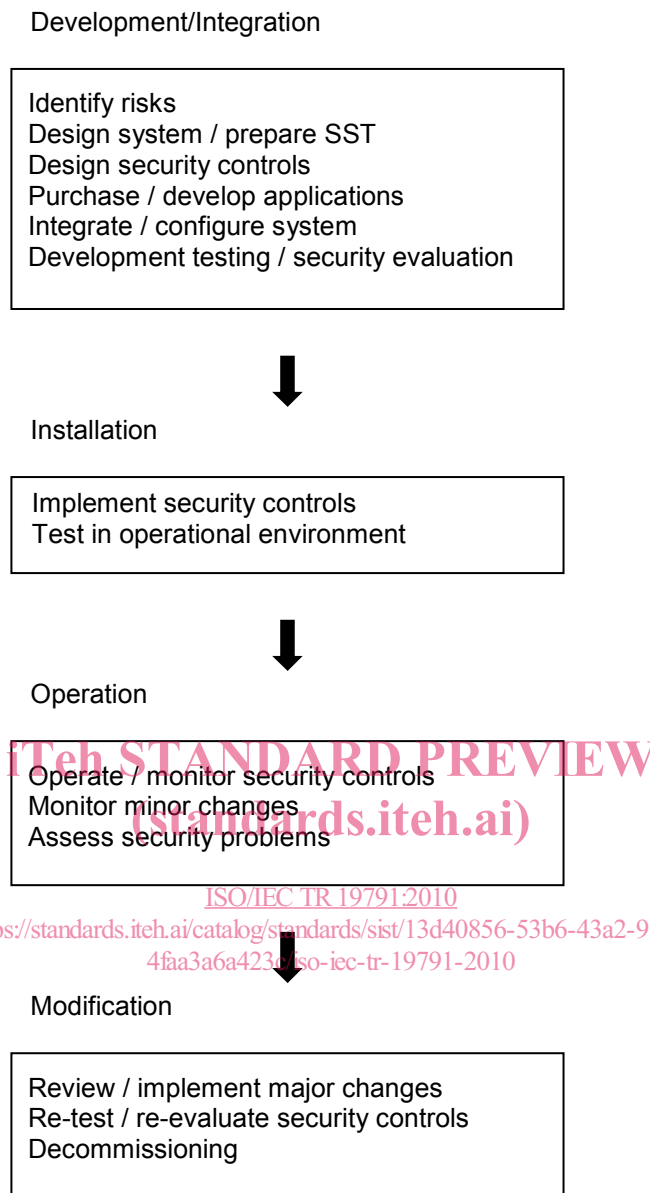


Figure 2 — Security within operational system lifecycle

### 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.

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.