TECHNICAL REPORT

ISO/IEC TR 15443-3

First edition
2007-12-15

Information technology — Security techniques — A framework for IT security assurance —

Part 3: Analysis of assurance methods

Technologies de l'information — Techniques de sécurité — Un canevas pour l'assurance de la sécurité dans les technologies de l'information —

Partie 3: Analyses des méthodes d'assurance

Reference number
ISO/IEC TR 15443-3:2007(E)

© ISO/IEC 2007

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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 2007

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

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO 2007 – All rights reserved

Not for Resale

Contents

Page

Foreword v

Introduction vi

1 Scope 1
1.1 Purpose 1
1.2 Application 1
1.3 Field of Application 1
1.4 Limitations 1

2 Terms and definitions 1

3 Abbreviated terms 4

4 Understanding Assurance 4
4.1 Setting the assurance goal 4
4.2 Applying assurance methods 7
4.3 Assessing assurance results 12
4.4 Example 14

5 Comparing, selecting and composing assurance 14
5.1 Selecting the assurance approach 14
5.2 Composing assurance methods 16
5.3 Comparing assurance methods 17
5.4 Focus on assurance properties 18

6 Guidance 23
6.1 Developmental Assurance (DA) 24
6.2 Integration Assurance (IA) 25
6.3 Operational Assurance (OA) 29

Annex A — Tabular comparisons 33
A.1 Methods and their target groups 33
A.2 Available Assurance Methods 34

Annex B — Assurance properties of selected methods 35
B.1 ISO/IEC 15408 35
B.2 ISO/IEC 19790 38
B.3 ISO/IEC 21827 40
B.4 ISO/IEC 13335 41
B.5 ISO/IEC 27001 and ISO/IEC 27002 43
B.6 IT Baseline Protection Manual 46
B.7 COBIT 48
B.8 ISO 9000 50

Annex C — Composition of assurance methods 53
C.1 ISO/IEC 15408 + IT Baseline Protection Manual 53
C.2 ISO/IEC 27002 + IT Baseline Protection 53
C.3 ISO/IEC 27001 and ISO/IEC 27002 53
C.4 ISO/IEC 27002 + ISO 9000 54
C.5 COBIT + IT Baseline Protection 54

Annex D — Case Studies 55
D.1 A chip-card manufacturer's assurance composition strategy 55
D.2 A service provider assures the upgrade of business processes 56

Annex E — Determination of the assurance goal 57
E.1 Risk Assessment 57

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.2 Risk Management 57
E.3 Security Model 58
E.4 Organizational security policy 59
E.5 Applicable Assurance goal 60
E.6 Security Measures 60
E.7 Example: ISO/IEC 15408 61

Bibliography 62

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 15443-3, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

– *Part 1: Overview and framework*

– *Part 2: Assurance methods*

– *Part 3: Analysis of assurance methods*

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

The objective of this Technical Report is to present a variety of assurance methods, and to guide the IT Security Professional in the selection of an appropriate assurance method (or combination of methods) to achieve confidence that a given deliverable satisfies its stated IT security assurance requirements. This report examines assurance methods and approaches proposed by various types of organisations whether they are approved or de-facto standards.

In pursuit of this objective, this Technical Report comprises the following:

– a framework model to position existing assurance methods and to show their relationships;

– a collection of assurance methods, their description and reference;

– a presentation of common and unique properties specific to assurance methods;

– qualitative, and where possible, quantitative comparison of existing assurance methods;

– identification of assurance schemes currently associated with assurance methods;

– a description of relationships between the different assurance methods; and

– guidance to the application, composition and recognition of assurance methods.

This Technical Report is organised in three parts to address the assurance approach, analysis, and relationships as follows:

Part 1: Overview and framework provides an overview of the fundamental concepts and general description of assurance methods. This material is aimed at understanding Part 2 and Part 3 of this Technical Report. Part 1 targets IT security managers and others responsible for developing a security assurance program, determining the security assurance of their deliverable, entering an assurance assessment audit (e.g. ISO 9000, ISO/IEC 21827, ISO/IEC 15408-3), or other assurance activities.

Part 2: Assurance methods describes a variety of assurance methods and approaches and relates them to the security assurance framework model of Part 1. The emphasis is to identify qualitative properties of the assurance methods that contribute to assurance. This material is catering to an IT security professional for the understanding of how to obtain assurance in a given life cycle stage of deliverable.

Part 3: Analysis of assurance methods analyses the various assurance methods with respect to their assurance properties. The analysis will aid the Assurance Authority in deciding the relative value of each Assurance Approach and determining the assurance approach(es) that will provide the assurance results most appropriate to their needs within the specific context of their operating environment. Furthermore, the analysis will also aid the Assurance Authority to use the assurance results to achieve the desired confidence of the deliverable. The material in this part targets the IT security professional who needs to select assurance methods and approaches.

This Technical Report analyses assurance methods that may not be unique to IT security; however, guidance given in this Technical Report will be limited to IT security requirements. Similarly, additional terms and concepts defined in other International standardisation initiatives (i.e. CASCO) and International guides (e.g. ISO/IEC Guide 2) will be incorporated, however, guidance will be provided specific to the field of IT security and is not intended for general quality management and assessment, or IT conformity.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Security techniques — A framework for IT security assurance —

Part 3: Analysis of assurance methods

1 Scope

1.1 Purpose

The purpose of this part of ISO/IEC TR 15443 is to provide general guidance to an assurance authority in the choice of the appropriate type of international communications techology (ICT) assurance methods and to lay the framework for the analysis of specific assurance methods for specific environments.

1.2 Application

This part of ISO/IEC TR 15443 will allow the user to match specific assurance requirements and/or typical assurance situations with the general characteristics offered by available assurance methods.

1.3 Field of Application

The guidance of this part of ISO/IEC TR 15443 is applicable to the development, implementation and operation of ICT products and ICT systems with security requirements.

1.4 Limitations

Security requirements may be complex, assurance methods are of great diversity, and organisational resources and cultures differ considerably.

Therefore the advice given in this part of ISO/IEC TR 15443 will be qualitative and summary, and the user may need to analyse on his own which methods presented in Part 2 of this Technical Report will suit best his specific deliverables and organisational security requirements.

2 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15443-1, ISO/IEC TR 15443-2 and the following apply.

2.1
assets
anything that has value to the organization

2.2
assessment
systematic examination of the extent to which an entity is capable of fulfilling specified requirements; synonymous to evaluation when applied to a deliverable

[ISO/IEC 14598-1]

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.3
assessment method
action of applying specific documented assessment criteria to a deliverable for the purpose of determining acceptance or release of that deliverable

2.4
assurance authority
person or organisation delegated the authority for decisions (i.e. selection, specification, acceptance, enforcement) related to a deliverable's assurance that ultimately leads to the establishment of confidence in the deliverable

NOTE In specific schemes or organisations, the term for assurance authority could be different such as evaluation authority.

2.5
assurance administrator
responsible (accountable) person for the selection, implementation, or acceptance deliverable

2.6
assurance goal
overall security expectations to be satisfied through application of formal and informal assessment activities

2.7
assurance concern
general type of assurance objective pursued by a major group of assurance authorities

NOTE In this part of ISO/IEC TR 15443, assurance concern is used for the purpose of establishing analyses and conclusions for assurance guidance given to that group of users.

2.8
deliverable
IT security product, system, service, process, or environment factor (i.e. personnel, organisation) in particular as object of an assurance assessment

NOTE 1 An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO/IEC15408-1.

NOTE 2 ISO 9000 holds that a service is a type of product and "product and/or service" when used in the ISO 9000 family of standards.

NOTE 3 For the purpose of this part of ISO/IEC TR 15443, and similar to the usage in ISO 9000, the term **product** will generally be used in place of deliverable throughout the document.

2.9
environment
environment of life cycle process execution (i.e. people, facilities and other resources) and associated environment assurance characteristics (e.g. reputation, certification)

NOTE In ISO/IEC TR 15443 environment assurance contrasts with product assurance and process assurance.

2.10
information security management system
ISMS
part of the overall management system based on business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

[ISO/IEC 27001:2005, definition 3.7]

2.11
method
a way of performing something according to a plan to obtain reproducible results in a systematic and traceable manner

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

2.12
metric
quantitative scale and method, which can be used for measurement

2.13
process capability
ability of a process to achieve a required goal

2.14
product
IT security product, system, service

NOTE 1 For the purpose of this part of ISO/IEC TR 15443, and similar to its usage in ISO 9000, the term **product** will be used in place of deliverable throughout the document.

NOTE 2 The term **product** is synonymous with **deliverable**.

2.15
residual risk
risk remaining after risk treatment

2.16
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002, definition 3.3.1]

NOTE 1 Risk evaluation is the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

NOTE 2 For the purpose of this part of ISO/IEC TR 15443, risk assessment, risk analysis and threat-risk-analysis are summarily called **risk assessment**.

2.17
risk treatment
process of selection and implementation of measures to modify risk

2.18
security
all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability

[ISO/IEC 13335-1:2004, definition 2.11]

2.19
security objective
statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions

[ISO/IEC 15408-1:2005, definition 2.42]

2.20
security policy
set of rules internal to an organizational unit that regulate how this unit protects the management of its assets conform to specified organizational objectives within its legal and cultural context

2.21
stage
period within the life cycle of a deliverable comprising processes and activities

NOTE Adapted from ISO/IEC 15288.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC TR 15443-1, ISO/IEC TR 15443-2 and the following apply.

COBIT Control Objectives for Information and related Technology, a method of **ISACA**

DA Developmental Assurance

IA Integration Assurance

ISACA Information Systems Audit and Control Association

ISSEA International Systems Security Engineering Association

OA Operation Assurance

ST Security Target

4 Understanding Assurance

Objective of assurance is to provide confidence that the product will operate securely in a given context. This clause gives consideration to some basic issues while detail analysis and guidance is presented in the remainder of this part of ISO/IEC TR 15443.

In terms of the concepts developed in Parts 1 and 2 of ISO/IEC TR 15443, this means that the product satisfies a given assurance goal. This goal has to be set in a more or less formal manner. The user of assurance has to be aware of the residual risk.

Confidence will be gained by use and interpretation of assurance results which may be already available or which may be gained by the application of assurance methods. These methods need to be properly selected and applied.

Numerous methods are available, and many are presented in Part 2 of ISO/IEC TR 15443. Some basic aspects of their application is explained in 4.2.

The user of the assurance result may present a varying level of sophistication. This sophistication may guide the associated level of rigor (refer to Subclause 4.2.1) of assurance methods, the extent application (refer to Subclause 4.2.2), and the Life Cycle stages to be covered (refer to Subclause 4.2.3).

Particular attention is to be given to the assessment of an assurance result. To gain higher levels of confidence formal assessment or certification may be required (refer to Subclause 4.3).

4.1 Setting the assurance goal

The assurance goals will depend on the assurance requirements to be satisfied:

– A product provider may have generic assurance requirements intended to satisfy the specific requirements of more than one user, i.e. those of a user community of its product, system or service.

– A product user typically has very specific assurance requirements, usually depending on a specific security policy of the user's organization.

The following explains this aspect and relates it to appropriate assurance offerings and use.

NOTE 1 The example comparison of Annex A.1 distinguishes between Hardware vendor, Software vendor, Network provider, Server operator, Content provider and Enterprise as user. In this example, the vendors clearly belong to the first group of assurance providers, and the user organization clearly belongs to the assurance user group. However, the others are both providers and users of assurance.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE 2 An organization may need to combine assurance results arising from two or more sources of assurance into a consistent compound assurance result. This is an important aspect and will be covered in subclause 5.2 and 6.2.3.1 of this Part of ISO/IEC 15443. This situation arises i.e. when multiple results of assurance are available to a user of assurance, or when a provider of assurance is projecting the use of two or more assurance methods.

Subclauses 4.1.1 and 4.1.2 typically relate to the assurance of product during development and integration. This difference of assurance concern is discussed in subclause 6.

NOTE 3 It is important to understand that the operation of a product typically is under the sole responsibility and supervision of the user organization even if security services are subcontracted to a service provider. Therefore subclauses 4.1.1 and 4.1.2 are not directly applicable to Operational Assurance.

4.1.1 Offering assurance

From the perspective of an organisation offering products, systems or services commercially (or to internal customers) the appropriate assurance method(s) will differ based on the prospective user or user community, their organizational size and expertise. Assurance will have to be customized according to these differences. In particular, assurance has to be sufficiently generic if a community of users is the recipient.

Providing assurances usually is an important factor in terms of additional time-to-market and/or cost involved. Organization providing assurance will have to weigh the benefit against its cost.

Given the above, the first two steps in the decision process are to identify:

– why the user might be willing to pay for assurance;

– to what purpose the user intends to put the assurance.

Taking these steps further we can derive customer assurance requirements and eventually derive the applicable assurance methods.

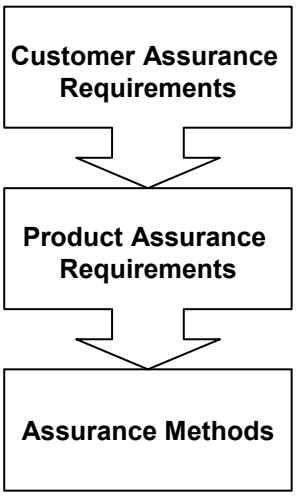

Figure 1 — Assurance Offering

In conclusion assurance may typically be offered as presented in Table 1.

The customer assurance requirements are identified in the form of assurance statement provided by the assurance method.

The supporting assurance arguments and in particular their assurance rigor (refer to Table 3) must be taken into consideration. The majority of assurance methods produce more than one type of assurance requirement and the assurance rigor varies depending upon the method. Thus the combination of assurance methods selected must be done carefully in order to ensure that the users' assurance requirements and ultimately their assurance goals are ultimately satisfied.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 1 — Assurance types offered

Assurance offered	Target customer	Customer assurance requirements	Required assessment rigor
Pass Through Assurance	End user	Content labelling; meaningful and recognisable to the end user	Low
Marketing Assurance	Generic user community	Mark, label, seal; labelling referring to generic assurance needs; presented in a very brief or encapsulated manner; meaningful and recognisable to end user, i.e. recognized "Quality Mark".	Low
Internal Assurance	Internal customer	Proprietary form of assurance statement; provided internal to the organization and based on trust	Any
External Assurance	Specific user community	Labelling including extensive supporting arguments and materials: may have restricted circulation	High
Small Organisation Assurance	Small organisations	Mark or Seal; intended to create trust through belief; meaningful and recognisable to end user, i.e. recognized "Quality Mark". Note: Usually, due to their small organizational size less expertise is available to verify presented assurance claims	Medium
Large Organisation Assurance	Large organisations	Detailed assurance statement Note: Expertise is available to verify assurance claims	High
Mandated Assurance	Specific sophisticated organization	Certificate or Fit-for-purpose statement Assurance form or even the method used is mandated by the organization, e.g. through contractual or registration requirements	High

4.1.2 Using assurance

The user of an assurance offering has a different perspective. Being the ultimate assurance authority this user's objective is to gain confidence that the specific product satisfies his specific assurance goal, which is the overall security expectation in the product, in the context of the organization in which the product is to be realized, deployed and/or operated.

The assurance goal ideally is established through a risk assessment or may be imposed by organizational policy (refer to Annex E).

Confidence may be gained through selection and application of formal and informal assessment activities which may be offered by vendors, system integrators, or executed by the user or under his mandate for the specific audience requiring proof.

Assurances may be used as presented in Table 2. The table also provides activities by which the user may establish ultimate confidence.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 2 — Assurance offerings used

User profile	Assurance to look for	User assurance appreciation activities	Related assessment rigor
Specific user	Content labelling	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal	Low
General user	Mark, label, seal	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal. A recognized "Quality Mark" is preferable.	Low
Internal customer	Proprietary form of assurance statement	Validate internal trust, e.g. through appropriate questioning.	Any
Member of specific user community	Labelling	Validate trust in the label, e.g. through questioning of other members of community or community organizations.	High
Small organisation	Mark or Seal	Check if content labelling is meaningful, recognisable and applicable to perceived assurance goal. A recognized "Quality Mark" is preferable.	Medium
Large organisation	Detailed assurance statement	Have assurance statements verified and validated by organization's experts.	High
Specific sophisticated organization	Certificate or Fit-for-purpose statement	Trust may be provided by third-party evaluation and/or certification, at least through reputation of assurance provider.	High

4.1.3 Residual risk

At its most basic level, assurance provides confidence to the user that a product will function as claimed by the provider, and will not show unintended behaviour. However, unlike other security safeguards, assurance does not provide any additional functionality (security mechanisms) in and of itself, and thus does not counter any additional vulnerability or threat.

All elements of security, in particular risk management, independent of the method used, include uncertainty. This uncertainty arises from many sources such as incomplete knowledge of all factors, tolerances in measurements, extrapolation of factors, etc. This uncertainty can, in some cases, become so large that it represents the major factor of the residual risk. Other factors are the vulnerabilities of the target operating environment and the imperfection of security mechanisms. If the rigor of assurance the security properties and mechanisms is raised, then the uncertainty related to those factors is reduced, thus reducing overall risk.

In certain situations assurance may be the only way to reduce uncertainty. Without adding any new security mechanism, assurance may reduce risk to an acceptable level. In this case the cost of assurance can be directly attributed to the benefit of security. It can be seen from the above that assurance is targeted at risk reduction.

4.2 Applying assurance methods

Assurance methods possess distinguishable properties as components or aspects. To provide guidance in the choice of one or several methods it is necessary to characterize those components and aspects which can be found in different assurance methods in similar form. A given assurance method may include general assurance properties or might focus on specific ones.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

As described in Parts 1 and 2 of ISO/IEC 15443, methods may approach the assurance of a product by assessing:

– the product, either after of during creation of the product;

– the processes used during the creation of the product;

– the environment in which the product is realized, i.e. in terms of the personnel or organization involved.

4.2.1 Assurance rigor

The rigor provided by the assurance method generally prescribes its use as explicated in Table 3.

Table 3 — Assurance rigor and use

Rigor Level	Use
1	simple “Assurance Seal of Approval”,
2	comfort level statements about assurance,
3	detailed facts supporting the claimed assurance,
4	detailed facts supporting the claimed assurance that can be verified,
5	presentation to a general audience, e.g. a board of directors, and recognisable by that audience.
6	presentation to a security professional audience, and recognisable by that qualified audience.

NOTE 1 In addition the strength of that representation must be taken into consideration and the strength of the supporting arguments for the representation. Limitations and constraints may apply in particular situations.

NOTE 2 When combining assurance evaluated components into a deployable system, metrics may be overlap and/or gaps may be questioned.

NOTE 3 Part 2 of 15443 does not provide a rating of the rigor of assessment provided.

4.2.2 Extent of application

Assurance obtained also may vary by the extent to which the focus of the assurance approach is applied, refer to Table 4.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 4 — Extent of Assurance Approach application

Assurance Approach	Focus of the assurance method	Extent of application
Product	**Properties** of the (completed specific) product, system or service to determine the assurance that can be derived for that product or system	**some** aspects of the product or system
		all aspects of the product or system
Process	Development **process** used by the organization **for a specific** product or system to determine the assurance that can be derived for that product or system	**some** aspects of the development
		all aspects of the development
	Development **process** used by the organization **for all** products and systems	**some** aspects of the development
		all aspects of the development
Environment	Individual(s) employed to perform the tasks	qualification of the individuals(s)
		reputation
	organization	actions the organization will demonstrably take to address any problems found later and the speed of those actions
		reputation

4.2.3 Application and Life Cycle

Part 1 of ISO/IEC TR 15443 has adopted a stage model based on ISO/IEC 15288. Each life cycle stage corresponds to processes applied to a product in an environment. Each of the processes comprises a set of activities and uses resources of its environment.

Applying the processes of each stage, and their activities, a product, system or service deliverable is processed through its life cycle.

Part 1 of ISO/IEC TR 15443 introduced a framework allowing to characterize the type of product, assurance approach, and assurance stage to be assessed.

There are still many issues to be addressed. This clause of this part of ISO/IEC TR 15443 will extend the conceptual framework set up in Part 1 of ISO/IEC TR 15443 to allow further analysis.

In this part of ISO/IEC TR 15443 the Life Cycle stage model will be enhanced by adding the Conception/Specification stage (refer to Table 5).

Presence of processes corresponding to a Conception and/or Specification Stage is postulated by many standards. However, a separate life cycle stage is usually not postulated for these processes. Few assurance methods offer well defined associated processes and activities for this life cycle stage, i.e. a discipline also known as requirements engineering.

The reason for this enhancement in this part of ISO/IEC TR 15443 is the fact that ICT security requires particular attention and an increased effort to produce a coherent and non-contradicting specification for the security features of a product. Few assurance methods offer well defined processes and activities for this life cycle stage suitable to the ICT security domain.

In the enhanced model the different Life Cycle Stages of interest are represented by five columns of the table. For this and approaching the concepts of ISO/IEC 15288 and ISO 9000, the Technical Life Cycle Processes are grouped into five stages, one for each column and abbreviated by one (1) letter:

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C **C**onception, leading to the establishment of the security design requirements which may include an overall architecture

D **D**esign, including the processes Stakeholder Functional Requirements Definition, Requirements Analysis, Architectural Design and Implementation

I **I**ntegration, including the processes Integration and Verification

T **T**ransition, including the processes Replication, Transition, Deployment and Validation

O **O**peration, including the processes Operation, Maintenance and Disposal

Table 5 — Life Cycle Assurance Model

Assurance - Stage→ Assurance - Approach↓	Conception/ Specification	Design/ Implementation	Integration/ Verification	Deployment/ Transition	Operation
Product	⇒**C**⇒	⇒**D**⇒	⇒**I**⇒	⇒**T**⇒	⇒**O**⇒
Process	**C**	**D**	**I**	**T**	**O**
Environment	**C**	**D**	**I**	**T**	**O**

In Part 1 of this ISO/IEC 15443 the following concept was developed:

– Assurance may focus on the result of the processes, which result is the product, thereby leading to product assurance.

– The processes being applied usually are subject to attention of the organisation and its customers, i.e. as they are more or less formally specified and more or less frequently improved. Assurance may focus on processes applied to the product rather than the product itself, leading to process assurance.

– The processes require an environment to be executed in, that is people, facilities and other resources. Assurance may focus on environment in which a product is processed rather than on the product or the processes, leading to environment assurance.

NOTE The extent of the life cycles approach, as well as its processes and activities are not detailed in this technical report; detail may however be necessary in refining the comparison of assurance methods.

4.2.4 Life Cycle Process Management

The life cycle stages C-D-I-T-O comprise the processes that may be applicable to a specific ICT deliverable and its components, i.e. hardware, software, services.

In the interest of quality and improvement these processes and their activities may be subject to process management.

Process management is itself a process. It is executed not at the project level but on the organizational level. Process management therefore is an organizational process and independent of a particular project.

However, process management makes only sense if the processes are executed repeatedly (i.e. by the administrators of an IT operation or the product developers of ICT projects).

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The Life Cycle process model of Part 1 of ISO/IEC TR 15443 will be enhanced in this Part 3 of ISO/IEC TR 15443, by adding process management as another dimension.

In ICT security this dimension is particularly important for the security management methods applied to ICT systems in the operations stage, such as in the case of ISO/IEC 27002 and the associated ISO/IEC 27001.

Process management is concerning the development, use and improvement of the life cycle processes. It comprises essentially:

– process definition, including development and documentation;

– process repetitive use;

– process assessment and measurement;

– process improvement.

Processes may be subject to certification by third parties.

The numbers associated with these steps correspond to a progression and dependency:

– there is no repetitive use without developed and documented processes;

– there is no process assessment and measurement without process repetitive use;

– there is no process improvement without process assessment and/or measurement;

– finally there is no certification without process assessment and/or measurement.

As improvement is leading to changes in the processes and their documentation, process management may be thought of as a circular model of continuous improvement, as shown in Figure 2.

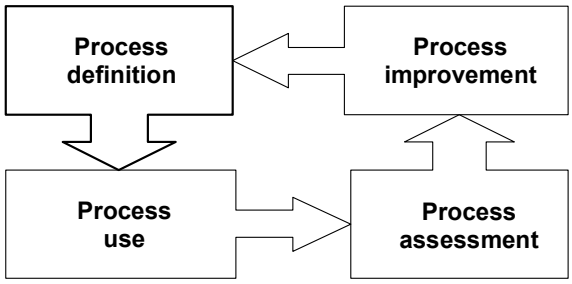

Figure 2 — Life Cycle Process Management

NOTE 1 To obtain measurability of processes these should only be used as documented.

Process management is a second dimension which is orthogonal to the processes of the C-D-I-T-O stage dimension. If an assurance method provides process assurance this means that the processes (which are applicable to a product) are subject to process management.

If a method's assurance stage is shown in grey (refer to Table 6, cells 2, 4, 6 and 7) the method provides process management.

NOTE 2 Product development and process development sound similar and therefore are subject to confusion. They must be distinguished and held apart.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.2.5 Cumulating life cycle properties

Methods may be more or less complete with respect to their Life Cycle properties. Life cycle properties may be cumulated which characterises the perfection but also the complexity of a method.

Part 1 of ISO/IEC TR 15443 specifies respective assurance approaches which may characterize an assurance method. These are represented symbolically as follows:

– Product Assurance: showing the life cycle stage letter within arrows, in a blank " field, e.g. ⇒**D**⇒;

– Process Assurance: showing the life cycle stage letter white on shaded background, e.g. **D**;

– Environment Assurance: showing the life cycle stage cell as with side bars left and right, e.g. ■ **D** ■.

The approaches may be cumulated as shown in Table 6. The seven (7) meaningful possibilities for a given assurance method and the respective life cycle stage are shown in Table 6.

Evidently, the Level 7 is most complete one in terms of number of components and presents at least the advantage of comprehensiveness and hopefully consistency in terms of vocabulary, processes and results. This should favourably impact training and cost.

NOTE Comprehensiveness does, however, not imply that the most complete method is necessarily the best for a specific assurance situation. Other aspects of a method have to be considered such as rigor, level of detail and associated cost.

Table 6 — Assurance Approach

Level	Product Assurance	Process Assurance	Environment Assurance	Graphical Representation for Life Cycle stage X
1	✔			⇒X⇒
2		✔		X
3			✔	X
4	✔	✔		⇒X⇒
5	✔		✔	⇒X⇒
6		✔	✔	X
7	✔	✔	✔	⇒X⇒

4.3 Assessing assurance results

The security relevant properties of a product, process or environment providing assurance are in their most primitive form claims made by the originating party, usually the producer of the deliverable, service or environment. To verify these claims assurance it may be necessary to assess and possibly certify the assurance result.

An assurance assessment model may be established. It defines a series of generic steps to be applicable to any of the assurance method subject to this Technical Report.

The assurance quality model requires:

– a person - the assessor - or body to verify that the criteria have been applied;

– assessment rules, criteria and /or methodology as a basis of an assessment;

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

– certification that the auditor is qualified and/or that the assessment process has been completed according to the rules;

– an assessment verdict to state the outcome of the assessment.

A complete model of this kind usually is called an assurance scheme.

4.3.1 Assessor

Assessment of security assurance properties of the product may be conducted by the user of the product. This involves specific knowledge. To save time and cost it may be advisable to call on an experienced third party.

Third party assessment may provide a further increment of assurance by the simple fact of its independence.

NOTE Personnel assurance would certify that the assessor's qualifications are acceptable.

4.3.2 Assessment criteria and methodology

Assessment rules need to be documented and be complemented by a methodology to warrant reproducibility.

NOTE In Personnel Assessment the deliverable being assessed is a person.

4.3.3 Assessment evidence

Common to all assessment methods is that their conclusions generally are based on evidence. This evidence is provided by statements which generally take the form of documentation.

Evidence proves the effective respectively presumed execution of actions within the corresponding processes, plans and procedures according to security policies and security concepts. These must be reviewed and if required, updated in a regular fashion.

The most important requirements of the documentation are:

– Suitability (documentation has to reflect the real-world situation);

– Completeness (all relevant concerns have to be documented);

– Sufficient degree of detail;

– Configuration control and integrity control (no unauthorized changes of the documentation).

In the detail analysis of assurance methods the requirements and comparability of this documentation may therefore be further investigated.

4.3.4 Assessment verdict

A qualitative or quantitative assessment result must be specified. This may in its simplest form be a pass/fail while a more refined result usually takes the form of a rating, e.g. several grades including, i.e. a rating corresponding to "failed".

Security as opposed to some other technical fields is characterized by constant evolution. Because of the complexity of the deliverables new security flaws may become apparent, and because of the threat environment, new threats may need to be countered.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

4.3.5 Assessment maintenance

Once an assessment has been made it therefore has to be questioned at periodic or event-triggered intervals.

Assessment maintenance is to ensure the validity of the assigned security assurance result or rating over time.

NOTE In Personnel Assurance this may mean continuing education and periodic re-assessment or re-certification of a person.

4.4 Example

The assurance authority - a vendor - builds a trusted system to satisfy generic security requirements according to ISO/IEC 15408 (assessment criteria). Evaluators (assessors of the assessment facility) assess the vendor's system to ensure that the system complies to the requirements and to ISO/IEC 15408.

For reproducibility the assessment facility applies ISO/IEC 18045 (assessment methodology) and issues the appropriate approval rating.

The Assessors and the Assessment Facility is accredited by a national accreditation body under the Common Criteria Mutual Recognition Agreement.

The national certification body issues a certificate showing to the evaluations results and the obtained rating.

This certificate may require evaluation maintenance to ensure that product updates do not jeopardize the initial rating.

5 Comparing, selecting and composing assurance

The purpose of this part of ISO/IEC TR 15443 is to provide guidance to an assurance authority in the choice of appropriate ICT assurance methods to attain a given assurance goal, i.e. to satisfy an organizational security policy. This guidance will help an assurance authority to determine:

– which assurance approach will provide the needed assurance results most appropriate to the needs of the Assurance Authority;

– the relative value of each Assurance Approach most appropriate to the specific context of the Assurance Authority; and

– how to deal with the assurance of a complex deliverable (i.e. several hardware and software components, security services, environment aspects, or a combination of these).

5.1 Selecting the assurance approach

Assurance may be obtained in varying degrees by using a variety of methods. At stake in this subclause is a comparison of each of the following assurance approaches (not methods) in a one-to-one comparison manner:

– Product vs. Process assurance;

– Process vs. Environment;

– Product vs. Environment;

These three approaches correspond to the first three entries Table 6. Goal of this comparison is to gain insight into which kind of assurance approach to choose in a general manner.

NOTE Composition of approaches corresponding to the entries 4 through 7 of Table 6 will be discussed in Subclause 5.2.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.1.1 Product vs. Process assurance

Product assurance focuses per definition on the **product** while process assurance focuses on the **processes** applied to the product in a given number of life cycle stages.

In product assurance the claim is that the product's features and performance have been intensively assessed, tested and or validated until the desired degree of trust in the product has been obtained. The degree of product assurance is a function of the criteria used (what is being assessed) and the assurance methodology (how compliance to the criteria is verified).

In process assurance the premise is that an organization's processes used to design, develop, produce and/or operate a product, have predictable and repeatable results and will therefore yield a product with established assurance.

However, even the highest trust of a user in the processes used by a producer cannot guarantee that these processes have been applied correctly and effectively to a given product. In other words, for high degrees of assurance of a product, product assurance (or evaluation) is necessary.

In product assurance each product has to be evaluated separately such that the total cost is increasing with to the number of products developed.

However, from a manufacturer's point of view these repeated evaluations of similar or identical products may be avoided if the user is satisfied with the manufacturer's process assurance, i.e. that the processes used conform to trustworthy process quality standards. The benefit of providing process assurance method is that the organization can produce different products without undergoing additional assessments (except for the periodic assessments to maintain its certificate).

This comparison evidently only holds for comparable efficiency, depth and correctness of the assurance methods, and possibly augmented by the trust provided by third parties called in for more objectivity.

Also synergetic considerations have to be applied when a combination of the two approaches is used. For example a manufacturer having implemented appropriate assurance of his processes will spend less resources for the evaluation of a product which he implements with processes which provide assurance.

5.1.2 Process vs. Environment assurance

Process assurance focuses per definition on these processes as applied to the product in specific life cycle stages while environment assurance focuses on the resources and the context in which these resources have been used.

The trust in a product using environment assurance is provided by trust in the organisation and/or its people, as well as on other resources applied to the product. This trust may be provided by certification of personnel and/or the organisation using standards or good professional practice, the lowest level being the reputation of the people or organisation in charge of the product.

It is evident - provided that comparable level of detail is applied - that environment assurance is generally less effective than process assurance. In fact, an organisation or person may have the generic knowledge and capability of the processes to be applied to a product. There is however no proof that the processes have been documented, are being assessed or have been certified.

Environment assurance is the lowest form of assurance, easiest to obtain. There are situations where environment assurance is the only assurance practicable and affordable. This may be the case

– in small organisations which cannot afford the cost of process or product assurance, or

– with Commercial Off-The-Shelf (COTS) products where the vendor will not allow or provide process or product assurance.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.1.3 Product vs. Environment assurance

From the previous discussion it becomes evident that there is a progression in assurance. Where product assurance is not accessible, process assurance is the "next better" assurance. Where process assurance is not accessible the remaining possibility is environment assurance.

5.1.4 Conclusion

In conclusion under the disclaimer of comparability of given assurance approaches the following may be stated:

– Product assurance should be chosen for highest assurance requirements.

– Process assurance provides reasonable and mostly affordable assurance through quality assurance of the relevant processes.

– Environment assurance must be chosen in small organisations or in cases where the product and/or its producer are not accessible for process and/or product evaluation.

In general it can be stated that (refer to Figure 3)

– Product Assurance of elevated rigor is limited to the Developmental Assurance of deliverables of lesser complexity relatively, while

– Environment Assurance is suitable mainly in Operational Assurance where the systems are relatively complex and assurance less rigorous.

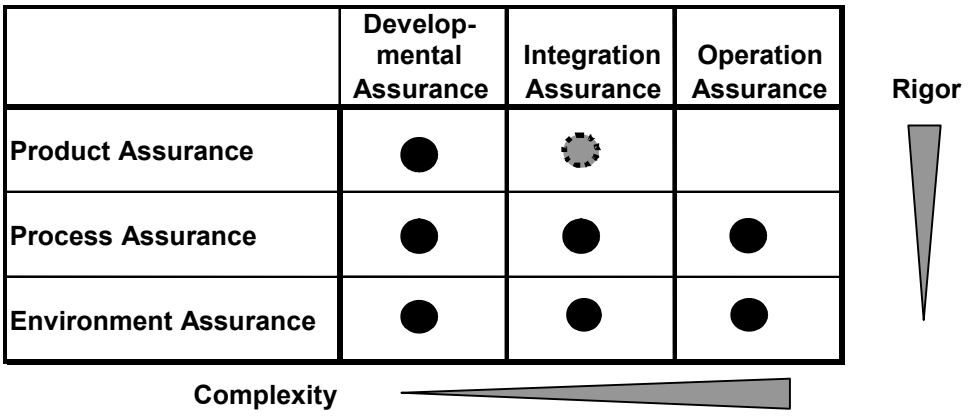

Figure 3 — Availability of Methods

5.2 Composing assurance methods

Inevitably, many users will be involved in more than one assurance method: perhaps ISO/IEC 15408 and ISO 9000, or ISO/IEC 15408 and ISO/IEC 21827.

This Technical Report provides a structure, which can be used to record the evidence/experience of those involved in more than one assurance method. This Technical Report provides concepts and a common language in which the interaction between methods and approaches can be described, and thus contributes to the investigation of possible combinations.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The ability to combine assurance properties from different assurance approaches will facilitate achieving assurance for products and systems by accepting assurance elements from other assurance approaches outside of the original assurance approach being used.

For example, if the organization has been certified to ISO/IEC 21827 Level 3, the organization may be given credit within the ISO/IEC 15408 evaluation scheme without having to make the organization resubmit evidence that they have already submitted for another assurance approach. Furthermore, this will facilitate the Certifier's job since they will have additional evidence which will now be admissible in determining the overall system assurance.

Comparing assurance methods may provide insight into potential limits of the assurance composition approach. This relates to the feasibility of trading off assurance properties when they may be based on different attributes.

Methods look at security from different angles and in different extent, may target different users or parts of the organization for different purposes. None of the methods considered in this Technical Report can promise “comprehensive“ security that is protecting an existing IT system appropriately against all relevant threats. In most cases it is therefore necessary to use combinations of methods synergistically.

An optimal level of security for an IT system will be reached if both vendors and users of IT contribute towards this goal in partnership.

Annex C provides a number of examples showing aspects of composing assurance methods.

5.3 Comparing assurance methods

Two principal approaches may be used to compare the relative value of Assurance Methods listed in Part 2 of this Technical Report:

– Property Matrix or

– Pairing (one-to-one comparison).

If many, i.e. more than three, complex items have to be compared to each other (see Figure 4) it becomes appropriate to compare the items along their common properties. This approach proves irrefutable with a growing number of items. Prerequisite is of course a sizeable number of similarities within these methods.

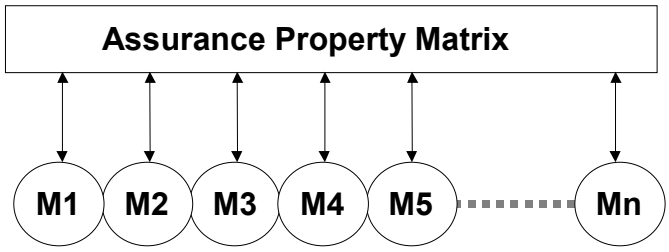

Figure 4 — Matrix Comparison Principle

For the purpose of matrix comparison, a list of assurance properties has to be developed. The challenge of this approach is the establishment of an optimal list of properties suitable to outline the major differences of the methods.

The matrix comparison of assurance methods consists in describing and rating the individual methods along a list. Quantitative measures or grades simplify the presentation of the results. An appropriate way of providing guidance to a choice from these benchmark results is the provision of graphical overview check-lists.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

To make an informed decision on which assurance methods to use and the value of the assurance result from a specific assurance method, matrix comparison analysis examines the composition of specific assurance methods.

Such matrix comparisons may be tailored to specific areas of concern according to types of interested parties, e.g. product manufacturer, large organization.

In this Part of ISO/IEC 15443 three assurance concerns have been defined in Clause 6 and selected for guidance.

As an example, Annex A.1 of this Technical Report shows a summary matrix comparison of the specific overall properties of selected methods.

5.3.1 One-to-one comparison

A more detailed comparison of items may use a custom list: Items are added or deleted to suit the pair of chosen items, and further details have to be investigated.

However, as the number of methods to be compared raises, the number of one-to-one comparisons will rise will rise with a binomial coefficient of "n" and 2; where n is the number of methods. (e.g., 6 items will lead to 15 individual comparison clauses). Therefore this type of comparison has not been retained for this Part of ISO/IEC 15443.

This type of comparison is left to the user who may establish such comparison on the basis of the descriptions provided by Part 2 of ISO/IEC 15443 and reference material listed there. The user may also prepare summaries to draw conclusions from a number of such one-to-one comparisons.

5.3.2 Assurance property matrix

Assurance properties are the actual source of assurance and may be subject to appropriate metrics. They include cost and various qualitative aspects like rigor, reliability, repeatability, efficiency, etc.

Which assurance method is the right one for the assurance problem at hand and how should it be applied? To answer this question the benefits of assurance methods in terms of assurance achieved by it has to be understood along with related costs. In other words: assurance features contributing to its value must be characterised to be more easily compared.

5.4 Focus on assurance properties

For the purpose of comparing established assurance methods a number of characteristic assurance properties have been developed. The aim of this part of ISO/IEC 15443 is to help a user to decide which single method or composite of two or more methods would be helpful in his/her particular case.

The assurance properties in Table 7 are of general nature and a number of assurance methods are analysed on that basis in Annex B.

The general orientation of the methods is presented in summary form in Annex A.1. From these table conclusions may be drawn on the applicability reps. non-applicability of a method in a specific context.

Another aspect may be the time required for the application of assurance method.

NOTE For source and further information on the methods refer to Part 2 of this Technical Report.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 7 — Key aspects for comparison

	Aspect	Description
1	Assurance goal	Does the method provide for the definition of an assurance goal? What is the method by which this goal has been derived? How is this assurance goal pursued?
2	Target audience	Which assurance concern does the method address? At which companies is the method aimed and at which roles within the enterprise is the content directed?
3	Properties	What is the purpose of the method concerned? What methodological elements does it contain essentially? How applicable to common enterprise structures is the method? How does the method map onto a specific application case?
4	Versatility	What is the relationship between the effort and cost of application? What size or complexity of the object under investigation can be handled? Can this be controlled, for example, by applying different levels of detail?
5	Timeliness	Does the present version of the method reflect the latest technology? If regular updating is necessary, then how is this ensured?
6	Completeness	Do the criteria on the focal point in question comprise a closed, exhaustive catalogue of items or are only selected aspects covered? For what level of security is the relevant catalogue of criteria suited?
7	Implementation cost/effort	What must be expected in the way of effort and costs when a given set of IT security criteria is applied to typical scenarios?
8	Tool support	Are there any tools which support the user in applying the method concerned?
9	Cryptographic coverage	Does the set of IT security criteria concerned contain any provisions or prescriptive guidance on cryptographic procedures and algorithms?
10	Assessment and certification	Does a qualification and/or certification system exist for the method? Is the method suitable for products or total solutions?
11	Credibility and recognition	The impact of a successful evaluation and certification, i.e., its potential satisfaction a customer or an administration, or at least as a basis for complementary tests. What is the maturity of the scheme? What are the market acceptance and its driving forces?

5.4.1 Assurance goal

The Assurance Authority has the task to approve the adequacy of assurance as well as the quantity and quality of assurance evidence to be collected to attain an acceptable risk level. This means that the residual risk for the intended environment will not exceed risk acceptable to and accepted by the stakeholders, e.g. an organisation.

To establish confidence in the assurance result the Assurance Authority must justify this result in a rational manner demonstrating that the product will perform as required providing the required functionality while enforcing the security policy. The confidence level will be a direct result of the assurance process and the stakeholder's individual comfort level.

Therefore the processes and standards used to create that assurance result must be understood and include definition, collection and review of the assurance evidence. Evidence may be collected through the methods used to develop, compose and maintain the assurance result.

An assurance goal may be based on risk assessment, security policy, baseline or Protection Profile (refer also to Annex E).

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Under the assurance property "assurance goal" the comparison will provide answers to the questions:

– Does the method provide for the definition of an assurance goal?

– What is the method by which this goal has been derived?

– How is this assurance goal pursued?

When a method does not provide an assurance goal, or if this goal does not correspond to the requirements of the assurance authority, it may be advisable to use risk assessment to establish the assurance goal, or to verify the validity of the proposed assurance goal. Where necessary the proposed assurance goal may be expanded to reflect practice in industry and administration.

NOTE 1 Risk assessment itself may be assured, e.g. by assessing the personnel delivering the risk assessment on their experience, their level of training, and/or other credentials, i.e. where this personal had been trained.

The assurance goal may prescribe properties that the prospective assurance method must possess, and/or the way in which that assurance representation is made, thus reducing the number of methods through which assurance may be obtained.

NOTE 2 Relevant concepts and processes are expressed in existing IT security Standards and Technical Reports such as ISO/IEC 13335, ISO/IEC 27002, ISO/IEC 21827 and ISO/IEC 15408.

5.4.2 Target audience

This part of ISO/IEC TR 15443 has been tailored to give guidance for three typical situations as explained in Clause 6. This assurance property will show the three categories:

– Developmental Assurance: the development of ICT products, e.g. towards a security objective;

– Integration Assurance: the procurement and/or composition of products into an ICT system, e.g. satisfying a security policy;

– Operational Assurance of an ICT systems, e.g. to satisfy a given organizational security policy.

Additionally, the entries may answer the following questions:

– at which companies is the method aimed?

– at which roles within the enterprise is the content directed?

– How applicable to common enterprise structures is the method?

5.4.3 Properties

The assurance approach as defined in Parts 1 and 2 of ISO/IEC 15443 and considered Subclause 6.1 is spelled out.

Additionally, the entries may answer the following questions:

– How applicable to common enterprise structures is the method?

– What is the purpose of the method concerned?

– What methodological elements does it contain essentially?

– How applicable to common enterprise structures is the method?

NOTE For general guidance on selecting the applicable assurance approach for a specific assurance goal refer to Subclause 5.1.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.4.4 Versatility

The possibility to reuse parts of an assessment allows to amortise the cost of the work done for a product, e.g. in the future evaluation of a similar product. In the case of singularity the cost has to be amortised with a specific version, e.g. of a product as opposed to a family of present or future deliverables.

Additionally, the entries may answer the following questions:

– What is the relationship between the effort and cost of application?

– What size or complexity of the object under investigation can be handled?

– Can this be controlled, for example, by applying different levels of detail?

5.4.5 Timeliness

Additionally, the entries may answer the following questions:

– Does the present version of the method reflect the latest technology?

– If regular updating is necessary, then how is this ensured?

– What is the market acceptance and its driving forces?

Additionally, the entries may answer the following questions:

– Do the criteria on the focal point in question comprise a closed, exhaustive catalogue of items or are only selected aspects covered?

– For what level of security is the relevant catalogue of criteria suited?

5.4.6 Completeness

The entries may answer the following questions:

– Does the method address the security objectives with a closed, exhaustive catalogue of items or are only selected aspects covered?

– For what level of security is the method suited?

5.4.7 Implementation cost/effort

Additionally, the entries may answer the following questions:

– What must be expected in the way of effort and costs when a given set of IT security criteria is applied to typical scenarios?

Assurance properties are the actual source of assurance and may be subject to appropriate metrics. They include cost and various qualitative aspects like rigor, reliability, repeatability, efficiency, etc.

Which assurance method is the right one for the assurance problem at hand and how should it be applied? To answer this question the benefits of assurance methods in terms of assurance achieved by it has to be understood along with related costs. In other words: assessment features contributing to its value must be measured and compared after alternatives have been identified.

Assessment is an assurance increment which is obtained at the expense of time, staff and considerable cost.

Therefore an assurance authority has to rationalise the value of using such assessment.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Assurance is cause for costs and therefore may be questioned for their value.

In determining the value of an assurance approach, it is essential that the specific context of the assurance authority be considered. This value is predicated on meeting the specific needs of the Assurance Authority for which it is being done and must correspond to the assurance needs, with particular attention being paid to the ultimate user of the assurance.

In cases where alternatives for assurance are available the relative value of assurance methods has to be established.

Organizational security policy or culture may impose the form of assurance. This form may be dictated by the amount of money the organization is willing to pay or by some other overriding criteria like political edict or legislation. These are intended to capture why the user of assurance would be willing to pay for Assurance and to what use they intend to put the assurance that they are paying for.

NOTE When considering assurance methods, the first step may be to identify why it is the user might be willing to pay for assurance and to what purpose the user intends to put the assurance. This may eliminate other assurance methods but also greatly impact the achievable assurance goals.

5.4.8 Tool support

The entries may answer the following question:

– Are there any tools which support the user in applying the method concerned?

5.4.9 Cryptographic coverage

The entries may answer the following question:

– Does the set of IT security criteria concerned contain any provisions or prescriptive guidance on cryptographic procedures and algorithms?

5.4.10 Assessment and certification

An even greater increment of assurance is achieved if the assessment of the assurance result is assessed and/or certified by some recognized certification scheme.

This assurance property entry may answer the following questions:

– Does a qualification and/or certification system exist for the method?

– Is the method suitable for products or total solutions?

– Does it rely on independent assessors to issue certificates? Or is assessment certification provided by a body or organisation?

– Is the certification body itself subject of assessment and certification? What are the certification rules?

– Are there mutual recognition agreements?

– What is the impact of a successful evaluation and certification? (i.e. its potential of satisfying a customer or an administration, or at least its value as a basis for complementary tests).

– What is the maturity of the scheme?

NOTE Methods with associated certification schemes are presented in Annex A.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

5.4.11 Credibility and recognition

The credibility of a methods and its possibly associated certification scheme has a strong impact on the acceptance of its result by the user.

Credibility may be established by its publicity in the market, support by a credible association, acceptance or even more promotion or imposition by government.

For global users the recognition has to be established on an international level.

6 Guidance

Any efficient guidance requires abstraction, simplification, and focus. In order to reduce the number of methods to be compared to those essential and applicable, 3 typical situations will be analysed. These situations will be termed 'Assurance Concern' and defined as:

– Developmental Assurance: the development of ICT products, typically towards a security objectives;

– Integration Assurance: the (procurement and) integration of products into an ICT system, typically to satisfy security objectives or policy;

– Operational Assurance: the operation of an ICT system, typically to satisfy a given security policy.

Each concern differs from the other with its own particularities and issues.

The concept of Assurance Concern may be easily visualized (refer to Figure 5) using the Life-Cycle and Assurance Approach concepts developed in Part 1, filled with content in Part 2 of ISO/IEC 15443, and extended with the Concept/Specification stage in Subclause 4.2.3 of this Part of ISO/IEC 15443.

Understanding the various assurance methods and approaches will allow an Assurance Authority to determine the methods that align with business requirements and assurance concern. The important aspect to keep in mind is the ultimate goal of assurance: to achieve stakeholder confidence regardless of the method(s) employed.

Because of the complexity of security requirements, the diversity of assurance methods and the difference between organisational resources and cultures the advice given in this part of ISO/IEC TR 15443 will be qualitative and summary.

Guidance in this part of ISO/IEC TR 15443 will concentrate on the few methods which are proven and widely accepted for these 3 assurance concerns.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

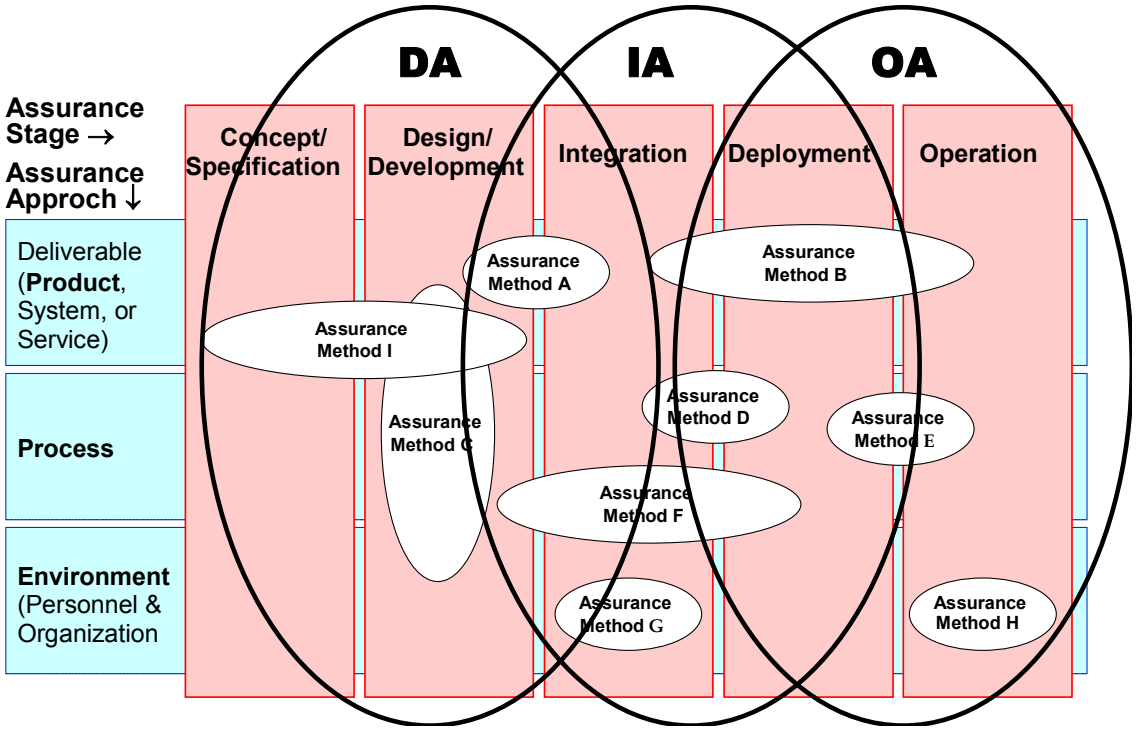

Figure 5 — Assurance Concern

6.1 Developmental Assurance (DA)

DA may be applied when a product, system or service is being developed. Development is ideally from scratch:

– starting with a concept;

– evolving the concept into a specification which then is materialized in a developmental process; and

– culminating in a product with specified claims; the successful demonstration of the product's specified characteristics; or even the validation of its features in a target environment.

Assurance requirements may be specified and assurance methods may be selected and applied to suit the requirements of DA.

6.1.1 Assurance goal

The assurance goal for DA has to be defined, e.g. as shown in Annex E. Alternatively, available methods may be chosen/composed such as to offer a conception stage allowing for the definition of security objectives with the required refinement.

In DA the security objectives may be:

– in the case of a singular product: a security policy;

– in the case of marketed products: generic security objectives common to the targeted user community.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO 2007 – All rights reserved

6.1.2 Available Methods

Some available assurance methods for DA have been outlined in A.2. Others may be chosen using Part 2 of ISO/IEC 15443.

The available methods available from Annex A.2 are: ISO/IEC 15408, ISO/IEC 19790, ISO/IEC 21827, ISO/IEC 27001 and ISO 9000. The major aspects of these methods are detailed in Annex B.

6.1.3 Major issues

For high security assurance requirements the strength and the correctness of the security functionality of the product has to be assessed. The chosen assurance method has then to contain (or to refer to, or to be complemented by) the assessment processes assuring these aspects.

6.1.3.1 Strength Verification

Strength verification is to ensure that critical mechanisms such as encryption, hash, password algorithms do withstand attack, in particular brute force attacks.

6.1.3.2 Correctness Verification

Correctness verification aims to ensure that the steps of the development process have been carried out correctly from the functional requirements to the system exploitation. Correctness verification is therefore concerned with assessing that a lower level of design (including the implementation) is consistent with the higher design levels. This activity does not address threat or security objective coverage but only that proper development has been done. It is closely related to a quality verification or quality assurance function.

Correctness verification is the process of confirming the system is compliant with the specification and a low level design and specification is compliant with the higher levels of design. This includes checking for compliance with the requirements specification as long as the requirements are stated in a way, which allows checking the compliance directly. Correctness Verification also includes testing procedures as well as informal or formal design analysis and verification techniques. The rigor that can be applied for Correctness Verification is dependent on the precise and unambiguous representation of the different design levels. Formal analysis and verification techniques require a higher level of precision in the design representation, which limits the methods that can be used for the description of the design. Especially for high levels of confidence in the correctness of a system, the design must not be subject to ambiguity.

6.2 Integration Assurance (IA)

IA may be applied when more than one product, typically a multitude of products of diverse origin and assurance results are integrated into a system.

Many of the products are finished and proven commercial products with assurance results available, but often these results are not available as desired by the user. Therefore in most cases the user - as ultimate assurance authority of a deployable system - has to manage a complex assurance situation.

The commercial system integrator developing a system usually is supplying, hence considering, only a part of the deployed system; this integrator therefore is facing a somewhat less complex situation unless tasked with total system responsibility.

Complex integration situations will generally require additional security products or measures be added in order to make up for the missing assurance level corresponding to the required assurance goal.

Complex integration situations will generally require additional security products or measures to be added and thereby may create a deficit of available assurance. This deficit has to be filled in order to reach given security objectives.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

An abstract or complex assurance result may have to be validated in operation to achieve the necessary confidence.

NOTE Not covered in ISO/IEC 15443 are aspects of system composability and its assurance: Even though each subsystem may meet its functional and security requirements when tested individually, the overall composed system may not function correctly and/or may not be secure. The composability assurance aspect may be subject of additional system test and validation.

6.2.1 Assurance goal

The assurance goal for IA has to be defined, e.g. as shown in Annex E. It may be:

– in the case of a singular system: a system security policy or a protection profile;

– in the case of marketed systems: generic security objectives common to the targeted user community; possibly in the form of a protection profile;

– in the case of a very complex user system: a pre-existing organizational security policy.

Alternatively, available methods may be chosen/composed such as to offer a conception stage allowing for the definition of security objectives with the required refinement.

6.2.2 Available Methods

Some available assurance methods for IA have been outlined in A.2. Others may be chosen using Part 2 of ISO/IEC 15443.

The available methods from A.2 are: ISO/IEC 21827 and ISO 9000.

NOTE The recent ISO/IEC 19791 may be added to the list of methods available for IA. However, no related guidance is provided by this TR.

6.2.3 Major issues

6.2.3.1 Using a combination of methods

The commercial integrator of complex products may need to apply more than one assurance method to obtain an assurance result corresponding to the assurance goal in terms of rigor and completeness.

Typically the integrator will be free to choose the applicable assurance methods. Immediate and future costs, for the present and possible future products will impact the choice, together with customer expectations and market factors.

The resulting assurance package will be a combination of results from the chosen methods.

The choice of methods may be based on assurance property analysis of the methods as they are presented in Part 2 of ISO/IEC 15443. The aim of this part of ISO/IEC 15443 is to compare the method's main features which may have pro and con aspects for fulfilling an integrator's needs.

Aspects of a combination of Assurance Methods are shown in the case study in Annex D.1.

6.2.3.2 Using diverse assurance results

IA implies integration of always more than one, typically of a multitude of products as components into the final operable and/or deployable system, together with an assurance package for this system.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

To create this assurance package the integrator will need to:

– compile pre-existing assurance from identical or similar methods of multiple sources;

– translate and harmonize assurance originating from different assurance methods;

– interpret uncertain assurance results;

– add non-existing assurance;

– integrate all of the above.

The assurance results will need to be reviewed in the context of the situation for which the security objectives were established and for which the subsequent assurance evaluation was performed.

Limitations may have to be formulated to avoid that the assurance provided by the package in not inadvertently used for unintended purposes.

Ultimate assurance result will need to be the confidence that "the system is secure" for use in the situation of concern.

6.2.3.3 Comparing and integrating assurance

A high level of confidence in an integrated system assurance result is closely related to a thorough understanding of the underlying assurance process, of each and every assurance component, in terms of:

– input leading to assurance;

– the rationale and concepts of the related assurance method;

– the associated assurance result.

Less confidence is achieved if assurance results are compared by evaluating the inputs and subsequent outputs only, considering each methods as a black box.

Least confidence is achieved if only assurance results are considered, standing on their own. However, this may be the only choice accessible to a small organization or in low assets-at-risk systems

6.2.3.4 Combining assurance results

Most assurance results are not directly comparable but must be aligned.

Methods may be of more or less rigor, and so are the related assurance results:

– Rigorous assurance methods are based on a specific methodology and that produce measurable and repeatable results, even though those results may be empirical and unique to the assurance method itself.

– Less rigorous assurance methods typically lack a specific methodology and are unlikely to be repeated with identical result. Such results, e.g. the estimated reputation of an organization, may be considered “fuzzy” and subjective.

In case of results from rigorous Assurance Methods only, combining results boils down to adjusting scales. The majority those methods include some form of “assurance scale” even though that scale may only contain a single ordinal, i.e. a “pass or fail” result. By analysis, it should be possible to identify a point of intersect or relativity between rigorous assurance methods' scales and to combine results after appropriate adjustment.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In case of results from less rigorous Assurance Methods, mingled with results from rigorous methods or not, combining results may be more complex, and will certainly be more intuitive, subjective, and therefore subject to challenge or questioning.

6.2.3.5 Composing assurance results

Assurance results, in particular when facing results from less rigorous methods, when difficult to combine may be composed in a rational manner.

The principle of composing is to make sure that

– supportive assurance results are gathered,

– all supportive assurance results taken together contribute to and strengthen the desired composed result,

– no assurance seriously weakens the contribution made by the other (otherwise the purpose of composition is defeated).

In cases of contradictory assurance results rational decisions have to be made about the use of one source of assurance or the other. This may be difficult unless the rationale used is included along with the result and understood.

Composing should be limited to a precise intended usage and purpose. This limitation should be formulated to avoid that the assurance package in inadvertently used for unintended purposes.

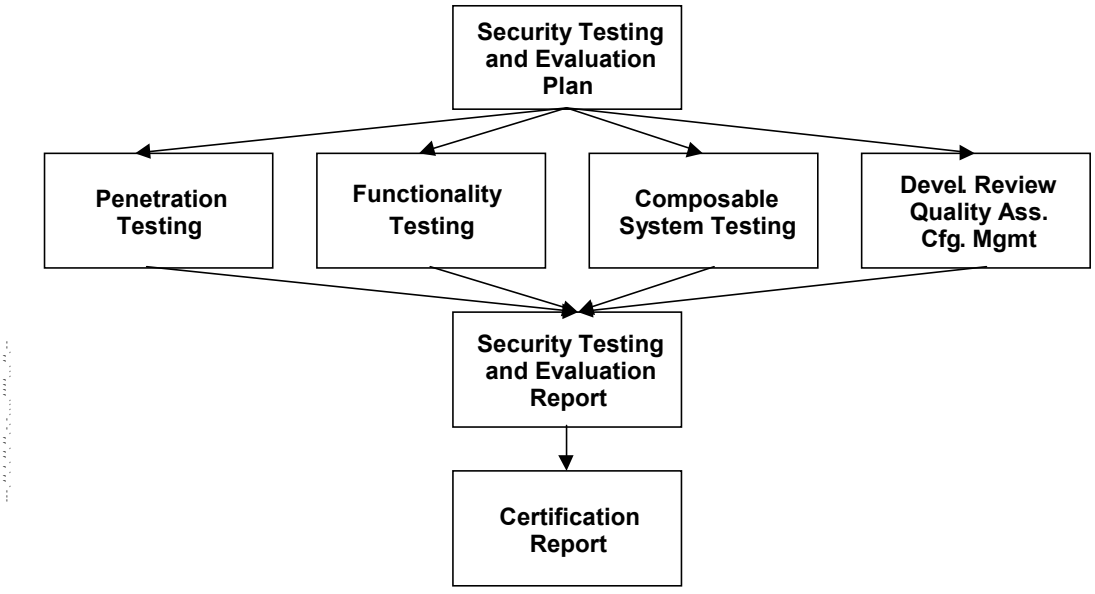

Figure 6 — System Testing and Evaluation

6.2.3.6 Assurance Validation

IA may include assurance of the transition of an ICT product from the vendor to the user, i.e. development/integration to operation.

The purpose of the assurance validation activities is to identify critical security problems possibly remaining after the system has been shown compliant with the specification.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Security requirements may be specified as high level objectives which are not always directly translatable to precise engineering requirements such that compliance cannot be shown by usual correctness verification activities.

The assurance validation may be the only means to prove the effectiveness of security functions and to cover side effects of the system or non-covered or non-suitable aspects.

Assurance validation typically includes vulnerability assessment, penetration testing, covert channel analysis, strength of security function analysis, misuse analysis, fault assumption validation and hardness testing.

6.3 Operational Assurance (OA)

OA is present where an ICT system or system of ICT systems is in exploitation under active ICT security management in a defined general security environment including people and facilities.

The assurance authority usually faces a live system, running to keep the organizational business operating. Many of the products are finished and the assurance authority in most cases has to manage a complex assurance situation. Therefore any guidance must take into account a multitude of pre-existing or possible non-existing or uncertain assurance properties attached to each individual component. This situation will generally require additional security products or measures be added in order to make up for the missing assurance level corresponding to the required assurance goal.

6.3.1 Assurance goal

The assurance goal for OA has to be defined, e.g. as shown in Annex E. Alternatively, available methods may be chosen and composed such as to offer a conception stage allowing for the definition of security objectives with the required refinement.

In OA security objectives may be:

– in the case of a larger organization: a security policy;

– in the case of smaller organizations: security objectives common to the targeted user community such as a baseline;

– in any other specific case: security objectives obtained through risk assessment.

To meet the real world demands (i.e. several hardware and software components, security services, environment aspects, or a combination of these items) assurance guidance for the operation stage needs to be suitable for complex systems composed of multiple items.

6.3.2 Available Methods

Some available assurance methods for OA have been outlined in A.2. Others may be chosen using Part 2 of ISO/IEC 15443.

The available methods available from A.2 are: ISO/IEC 27001, COBIT, IT Baseline Manual and ISO 9000. The major aspects of these methods are detailed in Annex B.

6.3.3 Major issues

6.3.3.1 Security Areas

A multitude of security areas may be concerned some of which have legacy character but are still frequently used (refer to Table 8). These areas may have security objectives and catalogues of measurers. It has to be made sure that these areas are covered according to up-to-date risk assessment.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 8 — Security Areas

Security Area
Administrative and Organizational Security
Personnel Security
Physical and Environment Security
Hardware Security
Software Security
Operations Security
Communications Security (COMSEC)
Transmission Security (TRANSEC)
Cryptographic Security (CRYPTOSEC)
Emission Security (EMSEC)
Network Security (NETSEC)

6.3.3.2 Security management areas

Table 9 shows an example of an extensive list of domains. Available methods may be mapped against this list to check if the required areas are covered in adequate detail.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 9 — Security management properties

Domain	COBIT Domain	Process
Planning & Organisation	PO1	Define a strategic IT plan
	PO2	Ensure compliance with external requirements
	PO3	Manage human resources
	PO4	Communicate management aims and direction
	PO5	Manage the IT investment
	PO6	Determine technological direction
	PO7	Define the IT organisation and relationships
	PO8	Define the information architecture
	PO9	Assess risks
	PO10	Manage projects
	PO11	Manage quality
Acquisition & Implementation	AI1	Manage changes
	AI2	Install and accredit systems
	AI3	Acquire and maintain technology infrastructure
	AI4	Develop and maintain procedures
	AI5	Acquire and maintain application software
	AI6	Identify automated solutions
Delivery & Support	DS1	Manage operations
	DS2	Manage facilities
	DS3	Manage data
	DS4	Manage problems and incidents
	DS5	Manage the configuration
	DS6	Assist and advise customers
	DS7	Educate and train users
	DS8	Identify and allocate costs
	DS9	Ensure systems security
	DS10	Ensure continuous service
	DS11	Manage performance and capacity
	DS12	Manage third-party services
	DS13	Define and manage service levels
Monitoring	M1	Provide for independent audit
	M2	Obtain independent assurance
	M3	Assess internal control adequacy
	M4	Monitor the processes

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

6.3.3.3 Operational Assurance Maturity

The implementation of Security Policy in an organization may be subject to maturity measurement. Table 10 shows an example of OA maturity levels. Certification of OA maturity will be a valuable addition to assurance.

Table 10 — Overall OA Maturity

OA Maturity Level	Description
1	All Specific or Generic Policies in place
2	Specific or Generic Risk managed and accepted
3	Measures defined, implemented and managed
4	Measures evaluated, revised & maintained
5	Measures and their maintenance certified

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO 2007 – All rights reserved
Not for Resale

Annex A — Tabular comparisons

The content of this annex has been adapted from publicly available material.

A.1 Methods and their target groups

For the identification of alternatives a tabular summary has been established. It characterizes the various assurance methods as to

– whether they concentrate more on the technical or organisational aspects,

– whether they refer in their use more to products or total systems, and

– whether they target more the vendor or the user.

Table A.1 — Methods and target user groups

Key: P: primary target group S: secondary target group X: any organisation		ISO/IEC 15408	ISO/IEC 19790	ISO/IEC 21827	ISO/IEC 13335	ISO/IEC 27001, ISO/IEC 27002	IT Baseline Protection Manual	COBIT	ISO 9000
Type of enterprise	**Hardware vendor**	S	P	P	S		S		X
	Software vendor	P	P	P	S	S	S		X
	Network provider		S	P	S	S		S	X
	Server operator		S	P	S	P	P	S	X
	Content provider			P	S	P	P		X
	Enterprise as user		S	S	P	P	P	P	X
Role within the enterprise	**Management**				P	P	S	P	P
	Project management	P	P	P	P	P	P	P	P
	IT security officer	P	P	P	P	P	P	S	S
	IT management	S	S	P	P	P	P	P	S
	Administrator		S			S	P	S	S
	Auditor				S	S	S	P	S

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Major certification schemes

A number of assurance methods have associated certification schemes for the assessment of the assurance result, refer to Table A.2.

Table A.2 — Major certification schemes

Assurance Approach	Assessment Criteria	Assessment Methodology	Personnel and/or Facility Accreditation	Assessment Scheme
Product	ISO/IEC 15408	ISO/IEC 18045	Accreditation?	National certification bodies with international mutual recognition
Process	ISO/IEC 21827	SSAM	SSO	National/international certification bodies, e.g. ISSEA
Environment (IT Operation)	ISO/IEC 27001		ISO/IEC 27006	
Environment (Organization)	ISO 9000		National/international certification bodies	National/international certification bodies

A.2 Available Assurance Methods

Mapping the methods presented in Annex B and using the conclusions for the user concerns of Subclause 5.1.4 the following Table A.3 is obtained:

Table A.3 — Available Assurance Methods

	Developmental Assurance	Integration Assurance	Operation Assurance
Product Assurance	**ISO/IEC 15408 ISO/IEC 19790**		
Process Assurance	**ISO/IEC 21827**	**ISO/IEC 21827**	**ISO/IEC 27001 COBIT IT Baseline**
Environment Assurance	**ISO/IEC 27001 ISO 9000**	**ISO/IEC 27001 ISO 9000**	**ISO/IEC 27001 ISO 9000**

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B — Assurance properties of selected methods

The content of this annex has been adapted from publicly available material.

B.1 ISO/IEC 15408

ISO/IEC 15408 originated from and is closely related to the Common Criteria. The fundamentals of the ISO/IEC 15408 methodology are well described in its Part 1.

In ISO/IEC 15408 the boundaries of what is evaluated is defined in the “Target of Evaluation” (TOE). This TOE is very carefully defined and represents the stated security functionality of a product.

The TOE does not necessarily describe a complete product. Nevertheless, for reasons of readability and simplicity, the TOE is called ‘product’ in this subclause.

B 1.1 Assurance goal

ISO/IEC 15408 permits comparability between the results of independent security evaluations. The standard does so by providing a common set of requirements for the security functionality of (collections of) products and for assurance measures applied to these products during a security evaluation. The evaluation process establishes a level of confidence that the security functionality of these products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help users to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of (collections of) products with IT security functionality.

The standard addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The standard may also be applicable to aspects of IT security outside of these three. The standard is applicable to risk arising from human activities (malicious or otherwise) and to risk arising from non-human activities. ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of competence in these areas.

ISO/IEC 15408 is applicable to IT security functionality implemented in hardware, firmware or software.

B 1.2 Target audience

There are three groups with a general interest in evaluation of the security properties of the target of evaluation: users; developers; and evaluators. They are all considered to be the principal users of ISO/IEC 15408.

B.1.2.1 Users

Users can use the results of evaluations to help decide whether a product fulfils their security needs. These security needs are typically identified as a result of both risk assessment and policy direction. Users can also use the evaluation results to compare different products. The standard gives users, especially in user groups and communities of interest, an implementation-independent structure termed the Protection Profile (PP) in which to express their special security requirements.

B.1.2.2 Developers

The standard is intended to support developers in preparing for and assisting in the evaluation of their products and in identifying security requirements to be satisfied by those products. These requirements are

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

contained in an implementation-dependent construct termed the Security Target (ST). This ST may be based on one or more Protection Profiles (the security requirements of the user as discussed earlier).

The standard can then be used to determine the responsibilities and actions to support evidence that is necessary to support the evaluation of the product against these requirements. It also defines the content and presentation of that evidence.

B.1.2.3 Evaluators

ISO/IEC 15408 contains criteria to be used by evaluators when forming judgements about the conformance of products to their security requirements. ISO/IEC 15408 describes the set of general actions the evaluator is to carry out, and the Security Functional Requirements (SFRs) on which to perform these actions. Note that ISO/IEC 15408 does not specify procedures to be followed in carrying out those actions.

B.1.2.4 Others

The standard may also be useful as reference material to all parties with an interest in or responsibility for IT security. Some of the additional interest groups that can benefit include:

– System custodians and system security officers;

– Auditors, both internal and external;

– Security architects and designers responsible for the specification of security properties of products;

– Accreditors responsible for accepting an IT solution for use within a particular environment;

– Sponsors of evaluation responsible for requesting and supporting an evaluation; and

– Evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

B 1.3 Properties

Confidence in IT security can be gained through actions that may be taken during the processes of development, evaluation, and operation. The product is specified by the Security Target. Design information is provided informally, semi-formally or formally.

Detailed testing instructions for assurance are provided in ISO/IEC 18045, the analogue of the “Common Evaluation Methodology” and are intended to ensure that an evaluation is performed consistently and provides repeatable results.

Formal schemes are organized, outside the scope of ISO/IEC 15408, to manage and oversee the activities of evaluation made by independent testing organizations.

B 1.4 Versatility

ISO/IEC 15408 offers sets of requirements for functional as well as assurance requirements to be selected by the user as appropriate to their needs. ISO/IEC 15408 contains 7 predefined assurance packages EAL1-7 to facilitate user selection and market recognition.

B 1.5 Timeliness

The sets of security assurance method are relatively stable and seldom modified. Previous sets of security criteria (TCSEC, ITSEC, etc.) have been replaced by ISO/IEC 15408, the first version published in 1999, with current version published in 2005.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 1.6 Completeness

This is specified in the ST.

B 1.7 Implementation cost/effort

Effort and costs for an evaluation against one of the sets of security criteria tend to rise as greater assurance is specified.

The length of time taken for an evaluation can depend on several factors including:

– the ability to re-use previous work;

– the maturity of the development organization;

– the maturity of the product, the experience of the lab;

– the evaluation strategy adopted (e.g. performing evaluation in parallel with development);

– the resources available to the validation body (scheme).

The cost for a formal evaluation includes elements for:

– scheme fees (varies by scheme);

– laboratory fees (varies by laboratory);

– internal work for contacts and minor modifications required for the evaluator;

– Security Target development.

In addition:

– Some documents are rarely produced by developers such as Security Policy model, and vulnerability analysis;

– The evaluation process frequently uncovers vulnerabilities in the product that need to be corrected. These can range from minor to severe.

B 1.8 Tool support

Few tools are available on the commercial market. Supporting documents are available for example ISO/IEC TR 15446 “Guide for the production of Protection Profiles and Security Targets.

B 1.9 Cryptographic coverage

A formal evaluation does not include an assessment of the quality of chosen cryptographic algorithms. However the correctness of the implementation of a chosen algorithm may be assessed.

B 1.10 Assessment and certification

Evaluation using methodologies appropriate to meet the requirements of ISO/IEC 15408 may be carried out by test laboratories. Using as an example of an evaluation scheme that specified by the Common Criteria Management Board; laboratories must be accredited to ISO/IEC 17025 and the results of the tests can be documented through the publishing of a validation report and the issuance of a certificate. These certificates are issued by accredited certification authorities (national schemes) and are published internationally.

For more information, see http://www.commoncriteriaportal.org.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 1.11 Credibility and Recognition

ISO/IEC 15408 is the International Standard that corresponds to the Common Criteria standards published by the Common Criteria Development Board.

ISO/IEC 15408 and the Common Criteria are well recognised and have much credibility.

B.2 ISO/IEC 19790

B 2.1 Assurance goal

The "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES", was initially published as "Federal Information Processing Standard (FIPS) 140-2" by the National Institute of Standards and Technology (NIST), USA and used for the specification of cryptographic modules. NIST and the Communications Security Establishment (CSE) of Canada established the associated Cryptographic Module Verification Program (CMVP) in July 1995, which operates a testing scheme and supplements FIPS 140-2 with further documentation including "FIPS 140-2 Implementation Guidance Document" and “FIPS 140-2 Derived test Requirements” intended to support and explain the standard and the testing and validation process.

The CMVP web site is at http://csrc.nist.gov/cryptval

Under the accreditation of the National Voluntary Laboratory Accreditation Program (NVLAP) and Standards Council of Canada, laboratories are accredited to perform conformance testing against this standard. NVLAP has accredited to date twelve laboratories located in the US, UK and Germany. The CMVP reviews the conformance test results and upon successful review, validates and issues validation certificates for the tested cryptographic modules. To date, over 650 certificates have been issued representing over 1,000 validated modules.

A sub-set of the requirements of FIPS 140-2 was published in 2006 as ISO/IEC 19790.

B 2.2 Target audience

19790 is applicable to cryptographic modules and mandatory for US government as FIPS-140-2, without waiver. Other organizations and governments have also specified its use.

B 2.3 Properties

The assurance method uses the conformance testing approach and is essentially applied to the following eleven areas:

– cryptographic module specification;

– ports and interfaces;

– roles, services and authentication;

– finite state machine model;

– physical security;

– operational environment;

– crypto key management;

– self-tests;

– design assurance;

– mitigation of other attacks.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 2.4 Versatility

The different test areas are structured in four levels 1-4 that are built one on top of the other. ISO/IEC 19790 testing is performed in reference to a specific version of a Cryptographic Module. If something is modified, the testing must be redone. The CMVP provides programmatic guidance on various methods for maintaining validation depending on the nature of change to provide timely and cost effective validation maintenance.

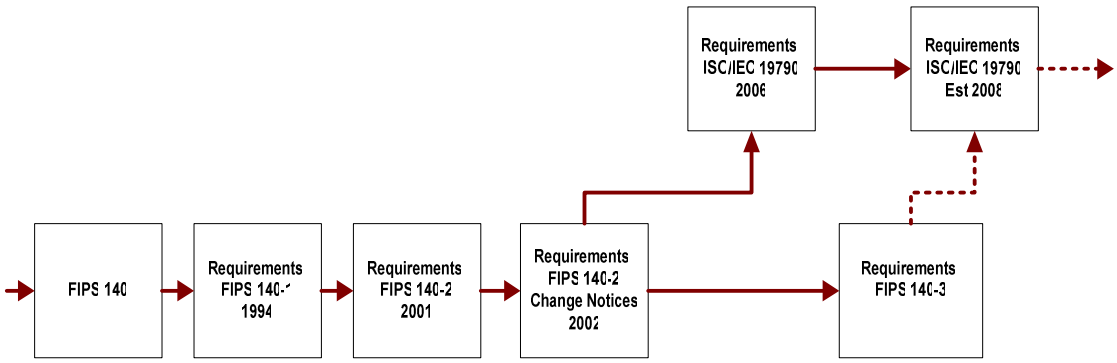

Figure B.1 — Evolution of test requirements

B 2.5 Timeliness

B 2.6 Completeness

As a conformance test the assurance that the cryptographic module meets the requirements of the specification (ISO/IEC 19790) is high.

Derived Test Requirements (DTR) and Implementation Guidance (IG) are produced to ensure completeness and reproducibility of tests.

B 2.7 Implementation cost/effort

The costs for an ISO/IEC 19790 validation may include the following elements:

– Validation organization costs (e.g. NIST CMVP cost recovery);

– Testing laboratory costs;

– The cost for the internal effort necessary to follow the validation, to provide minor modifications required by the tester and to write specific documents.

ISO/IEC 19790 testing always takes a shorter time than an ISO/IEC 15408 evaluation as the scope is narrower. The duration of ISO/IEC 19790 testing varies depending on:

– Development organization maturity;

– Lab experience;

– Validation body constraints;

– Product maturity;

– Conformance verses evaluation.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 2.8 Tool support

Few tools are commercially available. Supporting documents and toolkits are made available by NIST at http://csrc.nist.gov/cryptval.

B 2.9 Cryptographic coverage

The assurance method is exclusively defined for cryptographic modules. Approved security functions must be independently validated and certified for correct implementation under the Cryptographic Algorithm Validation Program (CAVP), also operated by NIST, which provides the algorithmic testing tools to the NVLAP accredited testing laboratories.

B 2.10 Assessment and certification

A North American accreditation scheme, the CMVP, exists and is maintained in collaboration with NIST and CSE.

B 2.11 Credibility and Recognition

ISO/IEC 19790 is derived from FIPS 140-2, a recognized U.S. specification published by the government's standards agency (NIST). Conformance with the specification is required by US administration for security products incorporating a cryptographic device for use in the protection of sensitive unclassified data. Certificates are issued for cryptographic modules that pass the conformance tests and meet other programmatic requirements.

B.3 ISO/IEC 21827

B 3.1 Assurance goal

ISO/IEC 21827 aims to provide assurance regarding the system's security engineering processes as defined by the user organisation.

B 3.2 Target audience

This assurance method primarily covers Developmental and Integration Assurance and thus targets both developers and system integrators.

B 3.3 Properties

The assurance method uses the process assurance approach.

B 3.4 Versatility

ISO/IEC 21827 addresses requirements in five capability levels related to the maturity of the process as determined by the organisation based on its overriding objectives.

B 3.5 Timeliness

ISO/IEC 21827 has been based upon previous work performed by ISSEA in the period 1994-2001. The standard was published by ISO/IEC on 2001 based on a Publicly Available Specification submission from ISSEA. Revision of ISO/IEC 21827 was initiated in 2005, and completed in 2007.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 3.6 Completeness

ISO/IEC 21827 covers in detail five levels of capability requirements involving all aspects of the security engineering discipline. The organisation of base practises that contribute to the process permits the user organisation the flexibility to combine processes to fit its organisational structure.

B 3.7 Implementation cost/effort

The main cost for an ISO/IEC 21827 evaluation will occur during the first project. The cost for additional projects using the same methodology would be a fraction of this initial cost. This figure could be reduced through the use of internal assessors. Normally there are no specific documents to be provided.

If the necessary work-force is available, the evaluation process can be short and last from 2 to 3 weeks.

B 3.8 Tool support

There exist a number of generally available spreadsheet-based tools supporting the tracking of the results of the appraisal and summarises and presents these results.

B 3.9 Cryptographic coverage

No specific requirements.

B 3.10 Assessment and certification

Both training and qualification systems are available for appraisers against this method.

B 3.11 Credibility and Recognition

ISO/IEC 21827 scheme provides for an evaluation by an Appraisal Team.

The SSE-CMM Support Organization (SSO) provides expert ISO/IEC 21827 appraisal facilitators and teams to assist organizations in appraising their security engineering capability. The following are services provided:

– ISO/IEC 21827 Appraisal Facilitation

– ISO/IEC 21827 Appraisal

– ISO/IEC 21827 Follow-up Audit

– Security Engineering Process Improvement Plan

Contrary to ISO/IEC 15408 or ISO/IEC 19790 there is no official or governmental agency providing an ISO/IEC 21827 certification scheme.

B.4 ISO/IEC 13335

B 4.1 Assurance goal

The suite currently comprising

ISO/IEC 13335-1 has been published as Technical Report (Part 1 in 1996, Part 2 in 1997, Part 3 in 1998, Part 4 in 2000, and Part 5 in 2001). Part 1 titled “Concepts and models for IT Security“ defines basic terms relating to IT security and elementary aspects (threats, risk, vulnerabilities etc.) and processes (e.g. contingency planning, risk assessment, awareness raising). It is aimed at responsible managers and security officers in organisations. Part 2, “Managing and Planning IT Security“, provides information on the design of

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

the IT security process and its integration into existing enterprise processes, and proposes an IT security organisation. Part 3, “Techniques for the Management of IT Security“, refines the steps involved in the IT security process and provides information on methods and techniques which can be used for this purpose. Finally, Part 4, “Selection of Safeguards“, provides information on which safeguards are relevant to which threats and how, for example, a reasonable level of baseline protection can be determined for an organisation. Part 5 “Management guidance on network security” provides recommendations for IT security management without mandating any particular solutions.

A second edition ISO/IEC 13335 has been issued respectively is being developed as a 2-Part International Standard: ISO/IEC IS 13335-1 has been issued in 2004; it cancels and replaces ISO/IEC TR 13335-1 of 1996 and ISO/IEC TR 13335-2 of 1997. ISO/IEC IS 13335-2 will replace ISO/IEC TR 13335-3 and ISO/IEC TR 13335-4. ISO/IEC TR 13335-5 (Network Management) will be merged with ISO/IEC 18028-1.

It is intended to rename ISO/IEC IS 13335-2 to ISO/IEC IS 27005.

B 4.2 Target audience

This assurance method covers Operation Assurance.

The central target group are managers in an enterprise or organisation who are directly involved in planning or implementing the IT security process, whereby the individual parts differ as to their relevance.

Part 1 is directed at Board-level managers, especially at those responsible for an enterprise-wide IT security programme.

Part 2 is addressed at managers who are responsible for the IT systems in an enterprise or whose area of responsibility is heavily dependent on the use of IT.

Parts 3 and 4 are directed at all those who have to deal with IT security during the various stages of the life-cycle of projects.

The reports can be used by all institutions, irrespective of their initial structure. However, they are aimed at examining and, if necessary, modifying the structure with regard to the necessary IT security processes. The information provided for this is independent of the complexity of the existing structures and the target security level.

B 4.3 Properties

The assurance method uses the environment assurance approach. The individual parts of the standard do not lay down any specific procedures and solutions, but they contain advice as to how these can be developed and adapted for the enterprise and what methods and models are available for this. The documents are not intended to be used to measure an IT security level or to demonstrate conformity with a standard in any other way.

B 4.4 Versatility

The reports generally have to be adapted in principle to the specific peculiarities of any institutions and their IT infrastructure or of projects and they also are adaptable. The various parts of the standard provide recommendations from Board level through to project level. Realistically, the processes and procedures can only be implemented completely in medium-sized and large institutions. However, as guidelines the reports are of universal use.

B 4.5 Timeliness

ISO/IEC IS 13335 has been recently issued or is in the process of being issued. However, the general nature of the statements of ISO/IEC IS 13335 is unlikely to require another revision in the foreseeable future.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 4.6 Completeness

The reports are complete as regards the description of the organisation and components of an IT security process. As they only give guidance for the definition of these processes and structures within the organisation, no IT security level is specified either, as determination of this level takes place only within the thus created organisation and processes.

B 4.7 Implementation cost/effort

The costs of introducing and maintaining an IT security process in the enterprise depend on the existing organisational structure and cannot be stated across-the-board. The same considerations apply as for ISO/IEC 27002.

B 4.8 Tool support

Tool support does not appear expedient. The management decisions to be made regarding the shape of IT security management in the enterprise do not depend on metrics.

B 4.9 Cryptographic coverage

Cryptography is considered at the level of measures. Requirements are not specified, and instead reference is made to standard ISO/IEC 11770-1, especially as regards key management.

B 4.10 Assessment and certification

Certification is not provided for, nor does it appear appropriate.

B 4.11 Credibility and Recognition

Recognized as international meta-standard.

B.5 ISO/IEC 27001 and ISO/IEC 27002

B 5.1 Assurance goal

The aim of ISO/IEC 27001 and ISO/IEC 27002 is to provide requirements for a "best practice" approach in information security management. ISO/IEC 27002 presents guidelines for information security controls, while ISO/IEC 27001 specifies requirements for information security management systems.

The main topics considered include planning, implementing, operating and improving an information security management system. Associated topics concern identification and assessment of risk and the selection of appropriate control objectives and controls.

B 5.2 Target audience

ISO/IEC 27001 and ISO/IEC 27002 are directed at enterprises and agencies of all sizes, but not at private users. In addition, the standard can be used by service firms in the audit and certification sectors.

The target audience of the standards are:

– managers responsible for ensuring that information relevant to their responsibilities is adequately secured;

– parties who are responsible for selecting and implementing IT security measures, such as the IT Security Officer, Head of IT;

– staff with monitoring responsibilities, such as internal and external auditors;

– external stakeholders, such as customers or suppliers that rely on the information security measures of an organisation; and

– information security management system certification bodies.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The applicability of the standard is largely independent of the organisational structure. The management-oriented approach does not limit the applicability to particular technical systems and system types.

B 5.3 Properties

The assurance method uses the process assurance approach and covers the following steps:

– establishing an information security management system;

– implementing and operating an information security management system;

– monitoring and reviewing an information security management system; and

– maintaining and improving an information security management system.

Associated with these steps, ISO/IEC 27001 contains requirements for documentation, management responsibility, internal information security management system audits, management reviews of information security management systems, and information security management system improvement.

ISO/IEC 27001 includes requirements to select controls to treat information security risk based on ISO/IEC 27002.

The standards can be applied in several ways. Firstly, ISO/IEC 27002 can be used as a reference for specific guidance regarding the specification and use of individual controls. Secondly, ISO/IEC 27001 can be used to implement a state-of-the-art information security management system. Thirdly, ISO/IEC 27001 and ISO/IEC 27002 in combination can be used to implement an information security management system that can be certified by an independent certification body.

B 5.4 Versatility

ISO/IEC 27001 and ISO/IEC 27002 are explicitly intended for organizations of any size and also for separately identifiable sub-parts of organizations. If an organisation has several information security management systems covering different scopes (e.g. covering different sub-parts of an organization), there is no automated way to draw conclusions about the security of information overall. However, based on the documentation available in each information security management system it is possible to apply judgement and determine whether the approaches to information security are consistent with overall objectives.

B 5.5 Timeliness

ISO/IEC 27001 and ISO/IEC 27002 are mature and fully consistent. It is planned that regular updates occur – in accordance with the general approach for modification of ISO/IEC standards – and that such updates will preserve consistency.

B 5.6 Completeness

ISO/IEC 27001 and ISO/IEC 27002 are heavily oriented to the top-down approach and contain generic security requirements and guidance. These requirements cover all the areas currently of relevance. The standard does not contain any product-oriented requirements and technology-oriented requirements are aggregated and contain only a moderate amount of detail.

ISO/IEC 27001 and ISO/IEC 27002 are not restricted to one specific security level, but the recommended controls are oriented to a baseline security approach, and are only suitable for high to maximum security levels after modifications. The management-oriented approach, however, provides support for all security levels.

ISO/IEC 27001 permits controls described in ISO/IEC 27002 to be excluded with justification if, for example, they are not relevant to the activities within the scope, or if associated security risk does not require treatment. Modification to suit smaller enterprises is possible.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 5.7 Implementation cost/effort

The strong emphasis on management makes the effort required for implementation heavily dependent on the general organisational quality of an institution. Institutions which are not well organised require significantly more effort than ones that have well defined organisational structures.

The code of practice approach to providing guidelines for control implementation generally makes it possible – without additional costs – to use existing controls to meet requirements to which they are relevant.

The effort required to implement an information security management system based on the requirements of ISO/IEC 27001 is largely determined by its scope. The choice of the risk assessment method has a major effect on the amount of effort required.

The cost of ISO/IEC 27001 certification is of the same order as the cost of ISO 9000 certification.

It should be noted that the cost of certification needs to be considered separately from the cost of implementation of a suitable information security management system. Such costs depend on the size of an organisation, the nature of the activities undertaken and the threats encountered. It is not possible to make a generalised comment on such costs.

Evaluation is typically spread over a period of time, with gaps as different aspects of an ISMS are implemented or problems rectified. Typically, evaluation spans an elapsed time of three to twelve months.

B 5.8 Tool support

ISO/IEC 27001 and ISO/IEC 27002 can be supported by tools. Specific tools harmonised to ISO/IEC 27001 are available for risk assessment, for supporting the development and maintenance of the required documents and records, and for the comparison of implemented controls with targets.

B 5.9 Cryptographic coverage

Cryptography is covered in ISO/IEC 27002 which describes good practice concerning policy on the use of cryptographic controls and key management. Given the general nature of the standard, no product-specific recommendations are made.

B 5.10 Assessment and certification

ISO/IEC 27001 has been developed to allow implementations to be certified by independent certification bodies. Independent certification of an ISMS is valid for several years (typically three years). Surveillance audits are held every six to twelve months during that time. Certification is withdrawn if non-conformances are serious and/or are not rectified in a timely manner. ISO/IEC 27006, currently in development, specifies requirements for the accreditation of certification bodies.

B 5.11 Credibility and Recognition

Various national and regional accreditation services provide independent assurance that ISO/IEC 27001 certification bodies follow sound procedures, employ competent staff and produce consistent results. Examples of these accreditation bodies are UKAS in the UK and JASANZ in Australia and New Zealand.

National and regional accreditation services co-operate internationally through membership of bodies such as the European Co-operation on Accreditation (EA) and the International Accreditation Forum (IAF). These regional and international associations ensure consistency of accreditation activities internationally.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B.6 IT Baseline Protection Manual

B 6.1 Assurance goal

The IT Baseline Protection Manual provides standard security measures aimed at establishing a predefined level of security for IT systems. This level can also serve as a starting point for areas with more stringent security requirements. To this end, the IT Baseline Protection Manual contains lists of standard security safeguards in each of the areas of *Infrastructure, Organisation, Personnel, Hardware and Software, Communications* and *Contingency Planning.* The approach covers the activities *IT Structure Analysis, Assessment of Protection Requirements, Modelling, Basic Security Checks, Supplementary Security Analysis* and *Implementation of IT Security Safeguards*.

B 6.2 Target audience

This assurance method covers Operation Assurance, as well as Development and Integration Assurance in an IT service environment.

The IT Baseline Protection Manual is basically directed at agencies and enterprises of all sizes, but not at private users. To facilitate directing of the standard security safeguards at the responsible employees, the text for each safeguard begins with information on who is responsible for initiating and implementing the safeguard in question. In each case one or more roles within the agency or enterprise are specified here. Examples of such roles are *Head of IT Section, IT Security Officer, Human Resources, Fire Protection Officer, Administrator* and *IT User.*

On the basis of the typical components which are predominantly handled in the IT Baseline Protection Manual, the manual will be very useful to service providers which create content or provide content on the internet, but less useful to pure network providers. Because of the extensive collection of IT security requirements contained in the IT Baseline Protection Manual, the document is also suitable for vendors of hardware or software products. However, software development as such is only mentioned in passing. Administrators will find comprehensive and detailed technical information in the IT Baseline Protection Manual.

Since the IT Baseline Protection Manual follows the general approach of considering typical (IT) components, it is largely independent of the enterprise structure. It is suitable for all areas in which standard IT systems and IT applications are employed and in which, by and large, the security requirements are normal. IT security measures for higher security requirements are contained only to a limited extent.

B 6.3 Properties

The assurance method uses the process assurance approach but includes product assurance element as far as their updating in the operation is concerned. The IT Baseline Protection Manual is essentially component-oriented. Depending on the components of the IT environment under consideration, the user chooses appropriate chapters (or “modules“) from the IT Baseline Protection Manual and uses them to “model“ the IT environment. The approach is divided into five layers, Higher order aspects, Infrastructure, IT Systems, Networks and Applications.

Layer 1, Higher order aspects, covers IT security aspects which cannot be fixed to individual IT or components of the infrastructure but affect large areas or even the entire IT environment.

B 6.4 Versatility

As the IT Baseline Protection Manual is aimed at the components in an IT environment under consideration, the effort and costs involved in applying the method depend heavily on the homogeneity of the IT environment under consideration. The approach of the IT Baseline Protection Manual contains a mechanism for grouping identical components so that it is not generally necessary to handle such elements on an individual basis. If, however, the IT environment is not at all homogeneous, then in the worst-case effort and costs will rise in proportion to the number of components (IT systems, IT applications, etc.).

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 6.5 Timeliness

The IT Baseline Protection Manual is reviewed and extended twice a year. This is especially necessary in order to adapt the technical content to developments. The additional material is based on requirements identified by registered users of IT Baseline Protection Manual.

B 6.6 Completeness

The IT Baseline Protection Manual contains both generic and also product- and technology-specific standard security measures. The generic measures cover all the important aspects of IT security, for example, organisation and contingency planning. Given the enormous variety of products and solutions in the IT sector, inevitably the product- or technology-specific measures can only cover the most commonly used components.

The IT Baseline Protection Manual is primarily oriented to the protection of information, IT applications and IT systems that have “normal“ security requirements. If the security requirements are higher than this, the standard security measures contained in the IT Baseline Protection Manual generally need to be supplemented by additional measures.

B 6.7 Implementation cost/effort

As the standard security measures are oriented to normal security requirements, generally no cost intensive services or expensive security or infrastructure components are required. The main costs of implementing the measures are therefore organisational effort and labour costs. The effort required to carry out the IT Baseline Protection analysis also has to be considered. This depends heavily on the homogeneity of the IT environment under consideration. For a medium-sized enterprise at least three months’ work should be planned in for this.

B 6.8 Tool support

The IT Baseline Protection Manual is supported by tools both as regards the approach (BSI IT Baseline Protection Tool) and also the content (USEIT - BSI tool secure UNIX administration).

Further development of these tools is oriented towards continuation of the IT Baseline Protection Manual. Other IT security tools which are oriented either to the approach or the content of the IT Baseline Protection Manual are also available on the market.

B 6.9 Cryptographic coverage

Like the other recommendations, the recommendations for the use of cryptographic procedures are also oriented to standard security requirements. The manual includes an introduction to cryptographic basic concepts, general recommendations for the use of cryptographic mechanisms and product specific recommendations.

B 6.10 Assessment and certification

A qualification scheme is currently developed so as to be able to offer authorities and enterprises the possibility of documenting the fact that they have successfully implemented IT Baseline Protection for the benefit of the outside world. Three levels are envisaged, a self-declared “entry-level“, a self-declared “higher level“ and the actual IT Baseline Protection Certificate. The latter is to be granted exclusively by independent certification authorities.

Within the individual chapters of the IT Baseline Protection Manual, it is made clear which measures are required for each qualification level. It is planned that the qualification scheme will be complete by the end of 2001.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 6.11 Credibility and Recognition

IT Baseline Protection Manual is a national standard, available in German and English.

B.7 COBIT

B 7.1 Assurance goal

Intensive use of IT to support and process business-relevant operations makes it imperative to set up a suitable control environment. COBIT (Control Objectives for Information and Related Technology) was developed by the Information Systems Audit and Control Association (ISACA, http://www.isaca.org) as a method for testing the completeness and effectiveness of such a control environment at limiting risk.

B 7.2 Target audience

This assurance method covers Operation Assurance.

COBIT distinguishes the following target groups:

– Management – for support when weighing up risk against the investment entailed by control measures.

– Users – for improved assessment of reliability and monitoring of IT services which are provided internally or by third parties.

– Testers – for objective justification of test evidence or for advice in connection with the establishment and operation of internal controls.

– Process owners or those responsible for IT – for support with their work.

COBIT can be used as a process-oriented method independently of the internal structure or legal form of an enterprise.

B 7.3 Properties

The assurance method uses the environment assurance approach.

When COBIT is used, the user determines at the outset which IT processes are relevant to the specific situation. For every control objective of the selected IT processes it is then necessary to weigh up the extent to which the existing measures satisfy the requirements.

COBIT differentiates seven different business requirements and groups them into the three categories of quality, security and regularity:

– The quality of the IT – determined by the effectiveness and economy of the processes operated – is reproduced in the criteria, effectiveness and efficiency.

– The security requirements confidentiality, integrity and availability are reflected in COBIT.

– The criterion of reliability is used by COBIT to ensure the reliability of financial reporting (financial reporting requirements) and the criterion adherence to legal requirements for adherence to internal and external standards.

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO 2007 – All rights reserved
Not for Resale

According to COBIT, IT-supported business processes are based on the following IT resources:

– Data: external and internal data elements in the widest sense.

– The totality of manual and programmed procedures is referred to as applications.

– Technologies includes hardware, operating systems, database administration systems, network, communications applications, etc.

– Assets: all the resources used to accommodate and support information systems.

– Personnel: knowledge, awareness and productivity relating to planning, organisation, procurement, compliance, support and monitoring of information systems and services.

The IT resources should be planned, developed, implemented, operated and monitored in a controlled fashion. With COBIT, 34 critical processes which play a material role in determining the success of IT management are defined. These IT processes underlying the IT resources can be grouped into four main domains which form a closed life-cycle:

– planning and organisation;

– procurement and implementation;

– operation and support;

– surveillance.

For the 34 critical IT processes a total of approximately 300 core tasks are listed. The necessary IT resources are assigned to each of the core tasks, and control objectives based on requirements from the categories of quality, security and regularity are defined.

B 7.4 Versatility

Thanks to COBIT's matrix structure, it is possible for the user to consider only individual domains or processes and/or to select a subset from the seven business requirements (e.g. only the security requirements confidentiality, integrity and availability).

B 7.5 Timeliness

COBIT was developed in 1996 by the Information Systems Audit and Control Foundation. In 1998 it was expanded and completely re-worked. The second edition offers materials and software for working with COBIT. The third edition (which came out in 2000) was published as an "open standard".

B 7.6 Completeness

COBIT offers a method for recording IT-oriented and accompanying processes. The associated control objectives are defined independently of technology and can be used for different system environments. However, to create security concepts it is necessary to add extra system-specific measures.

COBIT is oriented to the security interests of a typical enterprise. Preservation of fundamental company interests (integrity and confidentiality of internal information and processes) and also adherence to statutory regulations (data privacy protection, financial reporting) are considered.

There is no fixed security level, orientation is to enterprise objectives.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 7.7 Implementation cost/effort

A complete analysis of all control objectives within a medium-sized enterprise with COBIT should take no longer than one working month.

B 7.8 Tool support

The use of COBIT is supported by the tools, amongst others:

– "COBIT Advisor" from Methodware Limited in Wellington, New Zealand;

– "COBIT Self Assessment" from Certification Training Institute (CTI), USA.

The second edition of COBIT also contains useful background information, aids for the application and presentation material.

COBIT itself mentions examples for the implementation of checks (specific security measures). Using these examples, it is possible to estimate the extent to which individual control objectives are satisfied. However, usually users of COBIT (e.g. auditing organisations) use their own evaluation schemes.

B 7.9 Cryptographic coverage

Cryptographic procedures are cited as measures suitable for the protection of information and verification of authenticity. In this connection adherence to statutory requirements is covered, also the problems regarding the legal retention of encrypted data.

B 7.10 Assessment and certification T

No COBIT certificate exists in the real sense. However, generally the method is used by many auditing organisations in the context of the annual auditing of accounts to test the IT control environment. The results of IT testing are fed into the auditor’s report on the annual accounts.

B 7.11 Credibility and Recognition

COBIT is a standard which is supported by major international accounting firms.

B.8 ISO 9000

B 8.1 Assurance goal

The aim of the ISO 9000 series is to define a test method in which requirements for a quality management system are specified that have to be documented by an organisation as proof of its ability to satisfy customer requirements and enable this capability to be assessed by internal and external inspectors. Checks are also carried out as to whether the IT environment in the organisation satisfies customer requirements and is appropriate to the business objectives.

The purpose of this standard is not to imply the uniformity of quality management systems. The design and implementation of a quality management system in an organisation are influenced by its objectives, customer requirements, the products or services offered and processes.

B 8.2 Target audience

This assurance method covers Environment Assurance within any organization at a relatively high level.

The requirements contained in ISO 9000 are high level and, along with that, independent of any specific industrial or economic sector. They apply to organisations of any type and any size.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Here, documentation of processes helps the organisation to achieve uniformity, define interfaces and explain work routines to every employee.

Thanks to integration into the management processes, the structure of the standard is 100% directly applicable to the enterprise. The standards are appropriate for all areas in which the IT structure is used to support the internal processes and/or customer requirements. Furthermore, as they are overriding, they can be applied to all product or service categories and to every industrial or economic sector. They are also independent of organisation type and size.

B 8.3 Properties

The assurance method uses the environment assurance approach.

The requirements contained in the standard do not force enterprises to alter the structures of their quality management systems or to align their documentation to the structure of the standard.

Documentation of processes in an organisation's quality management system should furthermore be established in a fashion that is appropriate to its own activities.

Documentation of IT support in the enterprise is integrated into the process environment of the quality management system and, as such, can only be seen in the context of other management processes.

Here IT serves to support the internal processes and customer requirements and should always be viewed as an interface. The functional aspect exists only as a function of other documented management processes of the organisation.

B 8.4 Versatility

As IT in the ISO 9000 series of standards is dependent on other management processes, the amount of effort involved in testing depends on the coherence of the documentation and the functionality of the other processes. If the proportion of IT in the production or service process or according to customer requirements is very complex, then the test method will be more in-depth. However, as the IT process can never be viewed in isolation from the other management processes, the amount of testing remains proportionally constant.

B 8.5 Timeliness

The requirements contained in standard ISO 9001 are relatively stable and are seldom modified.

However, they are regularly reviewed to ensure that they are up-to-date and usable. Thus, for example, ISO Technical Committee has published a revision of the standard under the name ISO 9000:2000. The title of that revision no longer includes the words "Quality Assurance", nor does the revised area of application. This makes it clearer that what matters is the capability to fulfil customer requirements and achieve continuous improvement. Moreover, the result fits better with the ISO 14000 series of standards and with the environment management system.

B 8.6 Completeness

The requirements regarding the quality management system primarily serve the purpose of achieving customer satisfaction through fulfilment of customer requirements, as a minimum, by applying those requirements, continuously improving them and the prevention of errors. Thus, only the functionality of the IT environment within the documented processes is assured here. There is therefore no claim to review the technology of itself, but the functionality within the organisation, e.g. contingency concept, appointment of a data privacy protection officer.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

B 8.7 Implementation cost/effort

The effort and costs associated with integration of the IT environment into the process environment are relatively low. Given that the focus is on internal processes and customer requirements, there will not normally be any requirement for cost-intensive services or security components here. Most of the costs that arise here reflect labour and organisational efforts involved in integrating the processes into the process environment and defining interfaces.

As this IT process cannot be made independent of overall consideration of the ISO 9000 documentation, an estimate of the effort required for this sub-area is barely possible.

B 8.8 Tool support

Here the question of which tools should be integrated for support depends strongly on the enterprise.

All the tools available on the market can be considered.

B 8.9 Cryptographic coverage

As in all other processes for the IT environment, ISO 9000 is oriented to the business activities of an organisation and the customer requirements that are applicable to that organisation. Major differences may therefore be involved.

B 8.10 Assessment and certification

Testing and certification against ISO 9000:2000 is carried out by accredited, independent bodies, and the results of the tests are documented through issue of a certificate. These certificates are issued and published, in many countries and by multiple organizations.

B 8.11 Credibility and Recognition

The probably most widely recognized international standard.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C — Composition of assurance methods

The content of this annex has been adapted from publicly available material.

Hardware and software manufacturers must provide their products with security functions that are suitable for the intended purpose and the envisaged operational environment. With regard to a systematic approach, established assurance method such as ISO/IEC 15408 and ISO/IEC 19790 should be used for this.

On the users' side, steps must be taken to ensure that the accompanying measures that are necessary for the secure operation of a total solution are implemented. These include effective IT security management as well as suitable organisational, personnel and technical IT security measures. For these aspects methods like ISO/IEC 13335, ISO/IEC 27002 and the IT Baseline Protection Manual can be applied.

The Protection Profiles introduced with ISO/IEC 15408 can serve as a bridge between manufacturers and users. Protection Profiles can help users to formulate precise requirements for security features and functions of products. For their part, manufacturers can specify what Protection Profiles are covered by a particular product and support such claims by a certificate.

Often a combination is used such as shown in this Annex C.

C.1 ISO/IEC 15408 + IT Baseline Protection Manual

IT Baseline Protection and parts of ISO/IEC 15408 may be used in combination. Application of the standard security safeguards listed in the IT Baseline Protection Manual results in basic protection of the entire system, covering both IT security management and also technical measures at component level. However, generally it becomes apparent during the assessment of protection requirements or a comparable security analysis that special security needs or requirements exist in parts of an establishment that cannot be sufficiently protected using the IT Baseline Protection Manual alone. Here, Protection Profiles can be used to formulate the security requirements and select suitable – and, if possible, appropriately certified – products which provide the necessary security functions. In this way an appropriate level of IT security can be achieved through combined use of the IT Baseline Protection Manual and ISO/IEC 15408.

C.2 ISO/IEC 27002 + IT Baseline Protection

Standard ISO/IEC 27002 is concerned with the management of information security and offers process oriented access. The primary content is a catalogue of generic "best practice" measures. To protect a total solution against the relevant threat, these generic measures must be put into practice through specific and also technical instructions on actions to be taken and security measures. Here the IT Baseline Protection Manual can provide useful assistance. The IT Baseline Protection Manual contains catalogues with detailed recommendations drawn from the areas of Organisation, Personnel, Infrastructure and Technology. A combination of ISO/IEC 27002 and IT Baseline Protection can thus produce an approach which strictly separates control of IT security and practical implementation. Also in this scenario, in the case of sub-areas with special security requirements, recourse can be made to ISO/IEC 15408 and/or to Protection Profiles.

C.3 ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27001 specifies requirements for information security management systems. Certification standards exist based on ISO Guide 62 and ISO/IEC 17021. The approach can be applied in quite different enterprises and organisations. It allows information security management activities to be integrated into management systems that are based on other ISO-standardised management systems.

Assessable requirements are specified for information security management in all life cycle stages. Documented processes can be assessed in the context of an organisation's objectives. Associated records

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

can be assessed to determine whether the processes are correctly followed, and whether desired outcomes are achieved. Management system requirements include requirements for corrective and preventive actions if circumstances arise where the management system may not achieve the required outcomes. Compliance with ISO/IEC 27001 requires management to demonstrate commitment to information security management by playing an active leadership role, providing adequate resources, and ensuring that staff are adequately trained.

ISO/IEC 27001 requires that the controls specified in ISO/IEC 27002 are used as the basis for treating unacceptable risk.

C.4 ISO/IEC 27002 + ISO 9000

ISO 9000 specifies requirements for quality management systems and defines a corresponding test method. The approach can be applied in quite different enterprises and organisations; however there is no specific coverage of information security considerations. All that is specified is a test as to whether the IT environment in the organisation satisfies customer requirements and is appropriate to the business objectives. To increase coverage in the area of information security, ISO/IEC 27002 can be used as a supplement that is specifically concerned with the management of information security.

In particular, ISO/IEC 27002 also contains measures covering development processes so that the two standards complement each other. It is still necessary to substantiate the requirements and put them into practice, as both ISO 9000 and ISO/IEC 27002 are directed at management level.

C.5 COBIT + IT Baseline Protection

While IT Baseline Protection is oriented at the protection of technical systems, COBIT is aimed at basic objectives of management. As the internal organisation of an enterprise is generally structured in a task-oriented rather than a technology-oriented manner, it is often easier with COBIT to assign activities and responsibilities to individual organisational units. On the other hand COBIT only produces requirements for necessary IT security mechanisms, without specifying any specific technical measures. Combining the two approaches can result in an efficient approach for the creation of enterprise-specific IT security concepts. To this end the essential business processes are picked up with COBIT and their security requirements are determined. A technology profile (assignment of IT systems to business processes) is assembled, following which the IT Baseline Protection approach is a useful way of drawing up specific measures for implementing the relevant security requirements.

The scenarios described should simply be viewed as examples of ways of usefully combining sets of security criteria. In a specific application case it is possible that other approaches could be appropriate. For example, COBIT is recommended where auditing is a primary consideration and ISO/IEC 19790 when the subject of interest is cryptographic procedures.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D — Case Studies

D.1 A chip-card manufacturer's assurance composition strategy

The chip-card manufacturer chose a composition of ISO/IEC 15408 + ISO/IEC 19790 + ISO/IEC 21827. The assurance strategy was based on of past experience and future cost savings.

The company had conducted a successful EAL4 augmented evaluation, and an EAL1 augmented evaluation. This means that several teams have experience with ISO/IEC 15408.

Additionally the company had conducted 3 successful ISO/IEC 19790 level 3 evaluations.

The company was attracted by certification of the processes but had no previous experience with ISO/IEC 21827.

The object of this composition is the requirement of a manufacturer for his optimal assurance mix.

The rationale was based the benchmark analysis. The choice was made because of following coverage:

– ISO/IEC 19790 addresses:

  - the suitability of the security functions of the product for the requirements;
  - the resistance of the product.

– ISO/IEC 15408 addresses:

  - the suitability of the security functions of the product for the requirements;
  - the resistance of the product;
  - the development methodology and environment.

– ISO/IEC 21827

  - addresses the process used to develop secure services or products;
  - is mapping very well with ISO/IEC 15408.

The general approach is to use an ISO/IEC 21827 conforming processes to develop products ready for ISO/IEC 19790 or ISO/IEC 15408 evaluations. The benefits are:

– Documents required for ISO/IEC 15408 EAL4 or ISO/IEC 19790 could come as a normal output of the conforming processes.

– For less critical products assurance will be obtained according to ISO/IEC 21827 without having to pay the cost and delay for a full product evaluation. Both the certified process and reference to evaluated products would give assurance adequate to the customers.

– For critical products and depending on financing and customer requirements, evaluation and certification to ISO/IEC 15408 EAL4 respectively ISO/IEC 19790 will be done.

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.2 A service provider assures the upgrade of business processes

A service-providing company needed to upgrade its business processes to:

– supply goods and services on-line in addition to using traditional channels;

– reduce costs associated with supply chain transactions; and

– provide teleworking capabilities for staff.

Information security and privacy were recognized as critical to the success of the necessary business process and IT system changes. Specific requirements were formulated taking into account internal and external audit reports, industry reports, and feedback from customers, business partners and suppliers.

The company chose to use ISO/IEC 27001 and ISO/IEC 27002 because of its internationally recognized best practice foundation and suitability for all of its information security management.

Importantly, it was recognised that the information security management programme must cover all information, regardless of the media used to carry it and the technology used to process it. Risk management techniques and documentation were based on the requirements of ISO/IEC 27001. ISO/IEC 27002 was customised with additional detail concerning information security control requirements that meet the company's specific needs.

The implementation was undertaken as a project using the company's normal internal project management procedures, with implementation driven by the risk profile of each affected area. Implementation of the chosen approach involved a lot of hard work up front informing stakeholders and gaining the necessary support. However the support gained through this initial effort produced the benefit of easier implementation.

In a post implementation review, the company found that critical success factors were:

– gaining early management endorsement;

– using risk management techniques to justify the chosen approach and prioritise activities;

– involving as many people as possible in planning and implementation;

– informing employees of what was being done, and why, during implementation; and

– recognising that information security management is ongoing with no end-point.

Lessons learned were to:

– focus energy on information security management system maintenance as early as possible;

– strive to keep processes as simple as possible (some processes were found to initially be more complicated than necessary); and

– ensure that management system documentation focuses on management issues and is not too technical.

As a consequence of implementation of their information security management system, the company is satisfied to have justifiable information security that meets its needs. The company also has the capability to describe its information security programme to customers and other external stakeholders using an internationally recognized benchmark.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex E — Determination of the assurance goal

E.1 Risk Assessment

The assurance goal ideally is the product of risk assessment and risk treatment. The residual risk is the risk remaining after risk treatment. The residual risk needs to be acceptable to, and to be accepted by the stakeholders. If not acceptable then risk treatment, e.g. additional safeguards are required.

NOTE The residual risk may be used as an indicator of the value assurance provides.

E.2 Risk Management

The implementation of any security measure, and its scale, is guided by risk management. Risk management is the process of identifying, controlling and eliminating or minimizing harmful events which may affect assets, at an acceptable cost.

NOTE The terminology used within this document is based on ISO/IEC Guide 73. ISO/IEC 27005 may be applied when available.

Possible risk treatments are:

– risk avoidance;

– risk reduction;

– risk mitigation;

– risk transfer.

Risk remaining after risk treatment is the residual risk. Good practice is to operate a product only at acceptable and accepted residual risk.

The system security policy to be implemented corresponds to the risk treatment step ‘mitigation’ and results from risk assessment.

The risk management itself, and the resulting system security policy, may be subjected to an assurance process.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.3 Security Model

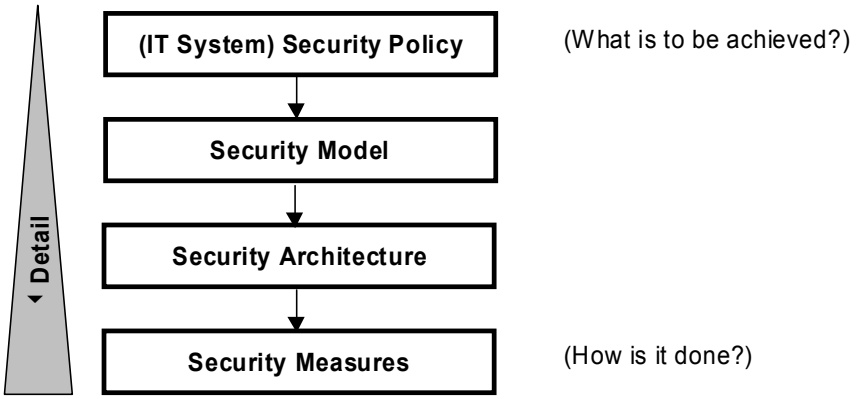

Figure E.1 — Security Model

Referring to Figure E.1, the following definitions may apply:

– A security model is a schematic description of a set of entities and relationships by which a specified set of security services are provided by or within a system.

– A security architecture is a plan and set of principles that describe as part of system security engineering:

  - the security services that a system is required to provide in order to meet the needs of its users;
  - the system elements required to implement the services; and
  - the performance levels required in the system elements to deal with the threat environment.

– A security measure is a process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within a system, e.g. mechanism for the prevention of events, measure to detect attacks, measure for recovery after an event.

Based on the results of the risk assessment, measures to treat risk can be defined within the process of developing a security concept.

Within the security concepts security measures are defined, which were identified in the context of a risk assessment as necessary.

Object of assurance related to the security model may be the review or audit of the availability and coherence of the security model.

Assurance methods based on risk assessment propose a staged approach with increasing refinement, leading from the policy to the determination of the implemented security measures.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.4 Organizational security policy

IT Systems will respond to an IT system's security policy which may respond to an organizational security policy. An organizational security policy generally is derived from risk assessment taking into account i.e. its organizational objectives (e.g. business objective). It is applicable to all organizational security concerns and its use is mandatory to guide all security efforts.

In these cases the organizational security policy is tailored and adapted in a hierarchical fashion to fit subordinate units of an organization and systems.

Any security policy has to be revisited periodically to take into account changes in threats, risk and assets.

A security policy may contain the following topics:

– scope of the security policy;

– accountability of the management;

– accentuation of the importance of security;

– definition of general and specific roles and responsibilities; assignment of positions;

– definition of security objectives;

– classification of information;

– communication, awareness, education and training issues.

In large organizations the development of more specific security policies may be necessary for a given department, division or branch, and/or in presence of diverse individual systems. At the level of a specific system, service or product deliverable it takes the form of a target IT system security policy which will respond to this hierarchy of policies.

To assure the dependencies of the hierarchy of policies there should be a corresponding effort of assurance actions. Additional object of assurance may be the review or audit of the availability and coherence of the security policies.

For a possible policy hierarchy refer to Figure E.2.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

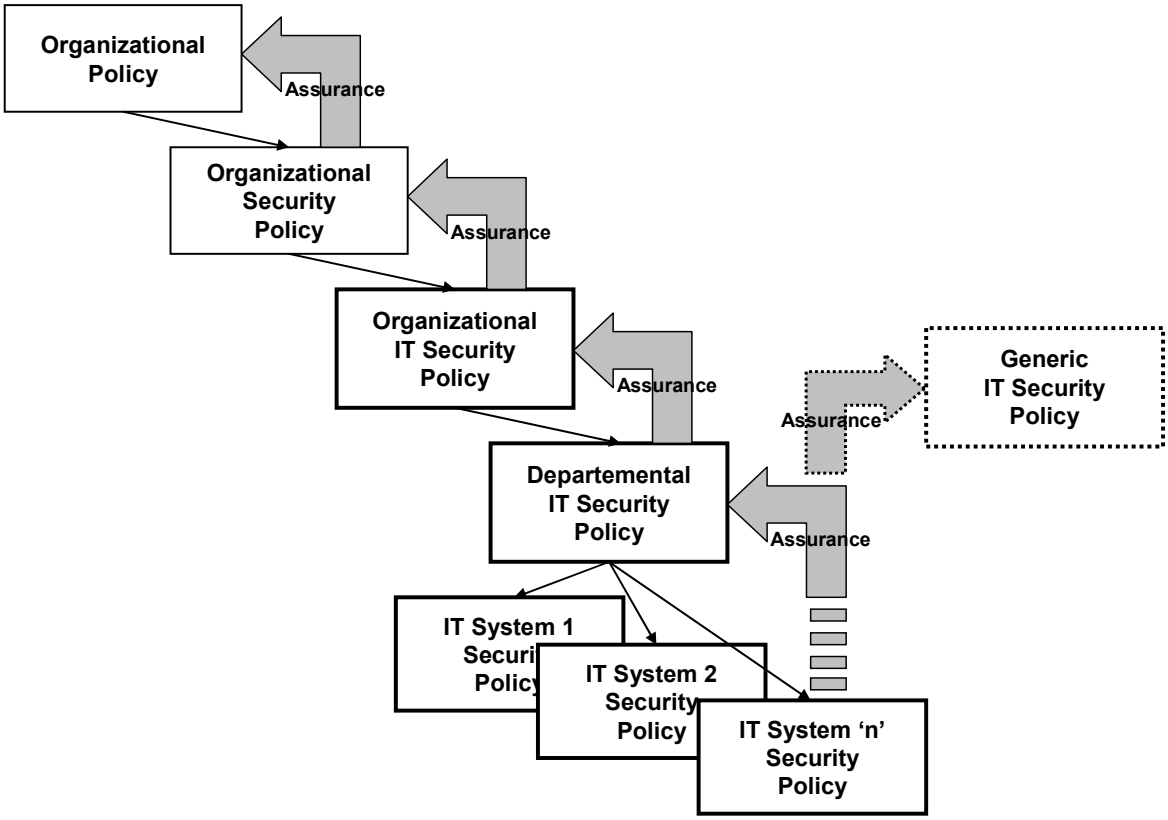

Figure E.2 — Policy and Assurance Hierarchy

E.5 Applicable Assurance goal

Goal of any security assurance is to provide confidence that the IT system of the deliverable is in line with the governing policy at the next higher level to assure that deliverable corresponds to the organizational policy.

Thus assurance for a given assurance case may be derived by risk assessment and/or the organizational security policy.

In many IT operations, in particular those of medium and small organizations, there is no prescribed IT security policy. In this case, an available generic "off-the-shelf" security policy may be applied.

This is also the case when a user implements off-the-shelf security, i.e. baseline security guides. In this case assurance is applied to the generic needs of an environment which should be spelled out in the applied baseline security guides.

Another approach is the use of an existing Security Target or Protection Profile which has been prepared for a given target environment according to ISO/IEC 15408.

NOTE Performing a risk assessment is a process which may itself be subject to process assurance. This type of assurance approach would assess the application of the processes and its output including its feedback loops to assure that the security personnel have applied the process, obtained the results, and processed them in the prescribed manner.

E.6 Security Measures

Security measures defined in the risk management process will be added to the functional requirements of a deliverable to yield engineering or procurement specification.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

In cases where a generic policy is used, its security policy, model and architecture are pre-determined and essentially non-modifiable. However, in most cases a choice or catalogue of security measures is proposed to choose from to suite the individual threat situation.

In this case it is vital to check with the description of the existing security objectives if all applicable risk is mitigated. This may not be the case, i.e. if the assets are of special value and/or exposed to special threats. In this case, and in case of doubt, a specific risk assessment has to be performed and will lead to specific measures. This hybrid approach is shown in Figure E.3.

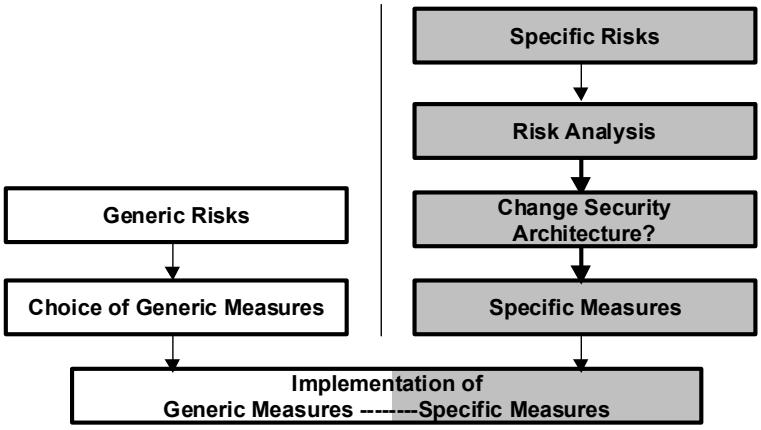

Figure E.3 — Hybrid Security Model

Object of assurance related to the definition of the security measures may be the review or audit of the availability and coherence of the security model.

NOTE Depending on the assurance methods used treatments are measures that take the form of, e.g. safeguards (ISO/IEC 13335), controls (ISO/IEC 27002) or security targets (ISO/IEC 15408).

E.7 Example: ISO/IEC 15408

In ISO/IEC 15408 there are the following decompositions:

– Target of evaluation (TOE) — an IT product or system and its associated guidance documentation that is the subject of an evaluation.

– TOE security policy (TSP) — a set of rules that regulate how assets are managed, protected and distributed within a TOE.

– Security Target (ST) — a set of security requirements and specifications to be used as the basis for evaluation of a product.

– Security Function (SF) — a part or parts of the product that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

– Security Function Policy (SFP) — the security policy enforced by a SF.

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC Guide 61 [1)], *General requirements for assessment and accreditation of certification/registration bodies*

[2] ISO/IEC Guide 65, *General requirements for bodies operating product certification systems*

[3] ISO/IEC Guide 67, *Conformity Assessment — Fundamentals of product certification*

[4] ISO/IEC Guide 73, *Risk Management — Vocabulary — Guidelines for use in standards*

[5] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[6] ISO 9001, *Quality management systems — Requirements*

[7] ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[8] ISO/IEC 15288, *Systems and software engineering — System life cycle processes*

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

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

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

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

[13] ISO/IEC 17024, *Conformity Assessment — General requirements for bodies operating certification of persons*

[14] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*

[15] ISO/IEC 19791, *Information technology — Security techniques — Security assessment of operational systems*

[16] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

[17] ISO/IEC 21827, *Information technology — Security techniques — Systems Security Engineering — Capability maturity model® (SSE-CMM®)*

[18] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[19] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

1) ISO/IEC Guide 61 has been cancelled and replaced by ISO/IEC 17011.

© ISO 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

[20] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[21] CEN/CENELEC EN 45013: General criteria for certification bodies operating certification of personnel

[22] FIPS 140-1: Federal Information Processing Standard: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[23] IT Grundschutz (Baseline Protection) Manual, Bundesamt für Sicherheit in der IT (BSI), 2004, http://www.bsi.bund.de/english/

[24] A Comparative Study of IT Security Criteria, Initiative D21, Initiative D21 e. V., Siemensdamm 50, 13629 Berlin, Germany

[25] A Guide to Certification and Accreditation for Information Technology Systems (MG-4), January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 or http://www.cse.dnd.ca

[26] A Guide To Risk Assessment and Safeguard Selection for Information Technology Systems, January 1996, CSE, The ITS Publications Section, (613) 991-7514/7468 or http://www.cse.dnd.ca

[27] COBIT MAPPING - Overview of International IT Guidance, IT Governance Institute, January 2004, IT Governance Institute, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA, (847) 590 7491 or http://www.itgi.org

[28] Fiona Pattinson, Comparing ISO 17799:2000 with SSE CMM V2, 2002, http://www.cccure.org/Documents/ISO17799/ISO17799_SSE_CMM_comparison.pdf

[29] Susanne Röhrig, Using Process Models To Analyse IT Security Requirements, Thesis, Faculty of Economics, University of Zurich, Switzerland, March 2003

© ISO 2007 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 63 pages

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2007 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale