

Proposed Draft Technical Report ISO/IEC 1st PDTR 15443-3			
Date: 2006-06-16		Reference number: ISO/IEC JTC 1/SC27 N4870	
Supersedes document SC27 N4248			
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.			
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: 2006-09-16 Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.		
ISO/IEC 1st PDTR 15443-3			
Title: Information technology -- Security techniques -- A framework for IT security assurance -- Part 3: Analysis of assurance methods			
Project: 15443-3			
Explanatory Report			
Status	SC 27 Decision	Reference documents	
		Input	Output
NWI Proposal	8 th SC27 Plenary Resolution 20 (N1556), October 1996		NWI Proposal (N1560)
Subdivision of project 15443 1 st WD 15443-3	20 th /WG3 meeting Res. 5 (N2598), April 2000		Text f. 1 st WD (N2607) Liaison Org. comm. (N2653) Disp. of comm. (N2733)
2 nd WD 15443-3	11 th SC27 Plenary Res. 1 (N2746), Oct 2000		Text f. 2 nd WD (N2741)
	25 th WG3 meeting Res. 12 (N3218), Apr. 2002,		Editor's report on future directions WG3 (N572)
3 rd WD 15443-3	26 th WG3 meeting, Apr. 2003		Rep. on objectives (WG3 N630) Disp. of comm. (N3612)
	27 th WG3 Res. 2 (N3591r1) & 15 th SC27 Plenary Res. 2 (N3624), Apr. 2003		Text f. 3 rd WD (N3614)
4 th WD 15443-3	28 th WG3 Res. 2 (N3591r1) & 16 th SC27 Plenary Res. 2 (N4035rev1), Apr. 2004	NB comments (N4137)	Text f. 4 th WD (N4006) Disp. of Comm. (N4239)
5 th WD 15443-3	30 th WG3 Res. 2 (N3591r1) & 17 th SC27 Plenary Res. 3 (N4599), Apr. 2005	Liaison Org. comm. (N4709) NB comments (N4754) Editor's Report (N4859)	Text f. 5 th WD (N4248) Disp. of Comm. (N4876rev1)
1 st PDTR 15443-3	17 th SC27 Plenary Res. 23 on Delegation of Authority (N4035rev.1) Apr. 2005 & 31 st WG3 Res. 7 (N4858), Nov. 2005		Text f. 1 st PDTR (N4870)
1st PDTR Registration and Consideration			
In accordance with resolution 7 (SC27 N4858) of the 31 st SC27/WG3 meeting held in Kuala Lumpur, 7 th – 11 th November 2005, this document is registered as 1 st Proposed Draft Technical Report. Consequently, the attached document is hereby submitted for a 1 st PDTR letter ballot closing by			
2006-09-16			
Medium: Livelink-server			
No. of pages: 1 + 68			

(This page was intentionally left blank)

Reference number of working document: ISO/IEC JTC 1/SC 27 N **4870**

Date: 2006-05-12

Reference number of document: **ISO/IEC WD 15443-3**

Committee identification: ISO/IEC JTC 1/SC 27/WG 3

Secretariat: DIN

Information technology — Security techniques — A framework for IT security assurance – Part 3: Analysis of assurance methods

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: Technical Report
Document subtype: 3
Document stage: (30) Committee
Document language: E
Source: Project editor John Hopkinson

Copyright notice

This ISO document is a working draft or committee draft whose copyright has not yet been assigned to ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

SC27 Secretariat
DIN - Deutsches Institut fuer Normung e.V.
Burggrafenstrasse 6, D-10772 Berlin, Germany
Telephone: + 49 2601-2652
Facsimile: + 49 2601-1723
E-Mail: krystyna.passia@din.de

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Content	Page
1	Scope1
1.1	Purpose.....1
1.2	Application1
1.3	Field of Application1
1.4	Limitations.....1
2	Normative references1
3	Terms and definitions2
3.1	assets.....2
3.2	assessment2
3.3	assessment method2
3.4	assurance administrator2
3.5	assurance goal.....2
3.6	assurance concern2
3.7	development assurance (DA)2
3.8	information security management-process.....2
3.9	information security management system (ISMS)3
3.10	method3
3.11	metric3
3.12	process capability3
3.13	residual risk.....3
3.14	risk evaluation.....3
3.15	risk assessment3
3.16	risk treatment3
3.17	risk avoidance.....3
3.18	risk reduction3
3.19	risk mitigation3
3.20	risk transfer3
3.21	risk identification3
3.22	security4
3.23	security objective4
3.24	security policy.....4
3.25	stage.....4
4	Abbreviated terms4
5	Conceptual Framework.....4
5.1	Assurance goal4
5.2	Life Cycle Stages8
5.3	Assurance Approach.....9
5.4	Assurance Approach and Life Cycle stages.....10
5.5	Life Cycle Process Management.....11
5.6	Graphic Presentation of assurance methods12
5.7	Assurance Concern13
5.8	Assessment model15
6	General Guidance to Selection.....16
6.1	Assurance approach17
6.2	Composition of assurance methods18
7	Guidance Methodology19
7.1	Comparison of methods19
7.2	Assurance goal22

7.3	Target audience	23
7.4	Assurance methodology	23
7.5	Assurance versatility.....	23
7.6	Method's timeliness.....	24
7.7	Assurance completeness and detail	25
7.8	Assurance implementation cost/effort	25
7.9	Tool support.....	26
7.10	Cryptographic coverage	26
7.11	Assessment certification	26
7.12	Limitations.....	27
7.13	Tabular comparisons	27
8	Guidance to Developmental Assurance (DA)	29
9	Guidance to Integration Assurance (IA).....	30
10	Guidance to Operation Assurance (OA).....	32
10.1	Security Areas.....	32
10.2	Security management areas.....	33
10.3	Operational Assurance Maturity	34
11	Summary.....	34
Annex A	A - Assurance properties of selected methods.....	36
A.1	ISO/IEC 15408.....	36
A.2	FIPS 140-2.....	39
A.3	ISO/IEC 21827.....	41
A.4	ISO/IEC 13335.....	43
A.5	ISO/IEC 27001 and ISO/IEC 17799.....	44
A.6	IT Baseline Protection Manual	47
A.7	CobiT.....	49
A.8	ISO 9000.....	51
Annex B	B - Composition of assurance methods.....	54
B.1	ISO/IEC 15408 + IT Baseline Protection	54
B.2	ISO 17799 + IT Baseline Protection.....	54
B.3	ISO/IEC 27001 and ISO/IEC 17799.....	54
B.4	ISO 17799 + ISO 9000	55
B.5	CobiT + IT Baseline Protection.....	55
Annex C	C - Case Studies	56
C.1	A chip-card manufacturer's assurance composition strategy	56

Figures	Page
Figure 1 Security Model.....	5
Figure 2 Policy and Assurance Hierarchy	7
Figure 3 Hybrid Security Model	8
Figure 4 Process Management	12
Figure 5 Assurance Concern.....	14
Figure 6 Availability of Methods	18
Figure 7 Matrix Comparison Principle	20
Figure 8 System Testing and Evaluation.....	31

Tables	Page
Table 1 Life Cycle Stage Model	9
Table 2 Life Cycle Assurance Approach	10
Table 3 Life Cycle Assurance Model.....	10
Table 4 Life Cycle Process Types.....	12
Table 5 Assurance Approach.....	13
Table 6 Key aspects for comparison.....	21
Table 7 Assessment Rigor	24
Table 8 Assurance Type	25
Table 9 Methods and Target User Groups	27
Table 10 Major certification schemes.....	28
Table 11 Available Assurance Methods.....	29
Table 12 Security Areas.....	33
Table 13 Security management properties	33
Table 14 Overall OA Maturity.....	34

Foreword

The International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) together form a system for worldwide standardisation as a whole. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the representative organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of Information Technology (IT), ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. The main task of a technical committee is to prepare International Standards, but in exceptional circumstances, the publication of a Technical Report of one of the following types may be proposed:

Type 1: when the necessary support within the technical committee cannot be obtained for the publication of an International Standard, despite repeated efforts;

Type 2: when the subject is still under technical development requiring wider exposure;

Type 3: when a technical committee has collected data of a different kind from that which is normally published as an International Standard.

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.

At the plenary meeting of ISO/IEC JTC 1/SC 27 in November 1994, a study group was set up to consider the question of testing and assessment methods which contribute to assurance that IT products and systems conform to security standards from SC 27 and elsewhere (e.g. SC 21 and ETSI; and some Internet standards contain security aspects). In parallel, the Common Criteria project created a working group on assurances approaches in early 1996. This Technical Report resulted from these two activities.

ISO/IEC TR 15443, which is a Technical Report of type 3, was prepared by the Joint Technical Committee ISO/IEC JTC 1, Information Technology, Subcommittee 27, IT Security Techniques.

The structure of ISO/IEC TR 15443 is currently as follows:

- Part 1: Overview and Framework.
- Part 2: Assurance Methods.
- Part 3: Analysis of Assurance Methods.

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(s) 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 must 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.

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 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 position his assurance requirements in terms of the general characteristic of available assurance methods and within typical situations.

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 product and ICT systems with security requirements.

1.4 Limitations

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.

Further analysis is required to determine which of the methods presented in Part 2 of this Technical Report will apply to deliverables and specific organisational security requirements.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9000:2000, *Quality management systems — Fundamentals and vocabulary*

ISO 9001:2000, *Quality management systems — Requirements*

ISO/IEC 13335:2004, *Information technology — Security techniques — Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 15288:2002, *Systems Engineering — - System Life Cycle Processes*

ISO/IEC 15408-1:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

ISO/IEC 15408-3:2005, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 21827:2002, *Information technology — Security techniques — Systems Security Engineering – Capability maturity model (SSE-CMM)*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems - Requirements*

ISO/IEC Guide 73:2002, *Risk Management — Vocabulary — Guidelines for use in standards*

3 Terms and definitions

The terms and definitions defined in earlier parts of this TR apply to Part 3. The following terms and definitions are used in this part for the first time.

3.1 assets

anything that has value to the organization.

3.2 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].

3.3 assessment method

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

3.4 assurance administrator

Responsible (accountable) person for the selection, implementation, or acceptance deliverable.

3.5 assurance goal

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

3.6 assurance concern

general type of assurance objective pursued by a major group of assurance authorities; an assurance concern is defined for the purpose of establishing analyses and conclusions for assurance guidance given to that group of users.

3.7 development assurance (DA)

assurance concern of organizations engaged in the design, development, and production of security hardware, software and systems.

3.8 information security management-process

systematic process in order to continuously identify and manage risks within an environment compromise relevant information's, processes and systems for information processing.

3.9 information security management system (ISMS)

that 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]

3.10 method

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

3.11 metric

quantitative scale and method, which can be used for measurement. [ISO/IEC 15408–1].

3.12 process capability

ability of a process to achieve a required goal. [ISO/IEC 21827].

3.13 residual risk

risk remaining after risk treatment.

3.14 risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

3.15 risk assessment

overall process of risk analysis and risk evaluation [ISO/IEC Guide 73:2002]

3.16 risk treatment

Risk treatment: Process of selection and implementation of measures to modify risk.

3.17 risk avoidance

Decision not to become involved in, or action to withdraw from, a risk situation.

3.18 risk reduction

Actions taken to lessen the probability, negative consequences, or both, associated with a risk.

3.19 risk mitigation

Limitation of any negative consequence of a particular event.

3.20 risk transfer

sharing with another party the burden of loss or benefit of gain, for a risk.

3.21 risk identification

process to find, list and characterize elements of risk

3.22 security

all aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability [ISO/IEC 13335-1]

3.23 security objective

statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions [ISO/IEC 15408]

3.24 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 [ISO/IEC 15408]

3.25 stage

period within the life cycle of a deliverable comprising processes and activities; adapted from [ISO 15288].

4 Abbreviated terms

The abbreviated terms defined in earlier parts of this TR apply to Part 3. The following abbreviations are used in this part for the first time.

COTS	Commercially of the shelf
DA	Developmental Assurance
FTA	Fast Track Assessment
IA	Integration Assurance
ISSEA	International Systems Security Engineering Association
OA	Operation Assurance
ST	Security Target
TRA	Threat Risk Assessment

5 Conceptual Framework

The objective of an assurance authority is to gain confidence that the deliverable satisfies a given assurance goals, that is the overall security expectations in the deliverable. Confidence may be gained through selection and application of formal and informal assessment activities which may be offered by assurance methods.

Assurance of the deliverable is achieved by assessing realised deliverable directly, by assessing its realisation processes and/or its environment. Assurance therefore requires an assurance goal and assessment activities.

5.1 Assurance goal

The guiding element in any security undertaking is the definition of an assurance goal.

Object of assurance is the deliverable, in the context of the organization in which the deliverable is to be realized, deployed and/or operated.

Goals depend on the stakeholder needs for assurance and audience requiring proof.

5.1.1 Threat-Risk-Assessment (TRA)

The assurance goal ideally are the product of Threat-Risk-Assessment (TRA) 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.

5.1.2 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.

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 deliverable only at acceptable and accepted residual risk.

The system security policy to be implemented corresponds to the risk treatment step 'mitigation' and result from risk assessment.

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

5.1.3 Security Model

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

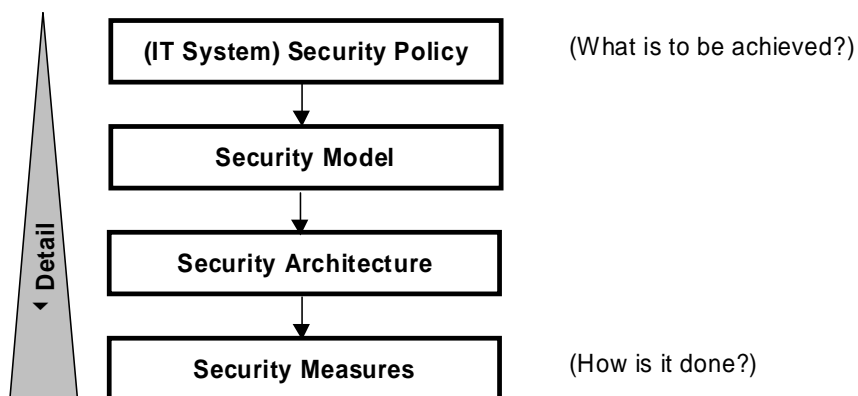


Figure 1 Security Model

Referring to Figure 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
 - the security services that a system is required to provide to meet the needs of its users,
 - the system elements required to implement the services, and
 - the performance levels required in the elements to deal with the threat environment and is part of system security engineering.
- 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 evaluation, measures to treat risks 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.

5.1.4 Organizational security policy

Organization may have an organizational security policy which has been derived by, and is being revisited periodically by threat-risk-analysis and taking into account i.e. its organizational objectives (e.g. business objective).

The organizational security policy is applicable to all organizational security concerns and its use is mandatory to guide all security efforts.

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 goals
- Classification of information
- Communication, awareness, education and training issues

For practical purposes, in large organizations the development of more specific security policies can be necessary for a given department, division or branch.

In these cases the organizational security policy is tailored and adapted in a hierarchical fashion to fit subordinate units of an organization and systems. For a possible policy hierarchy refer to Figure 2.

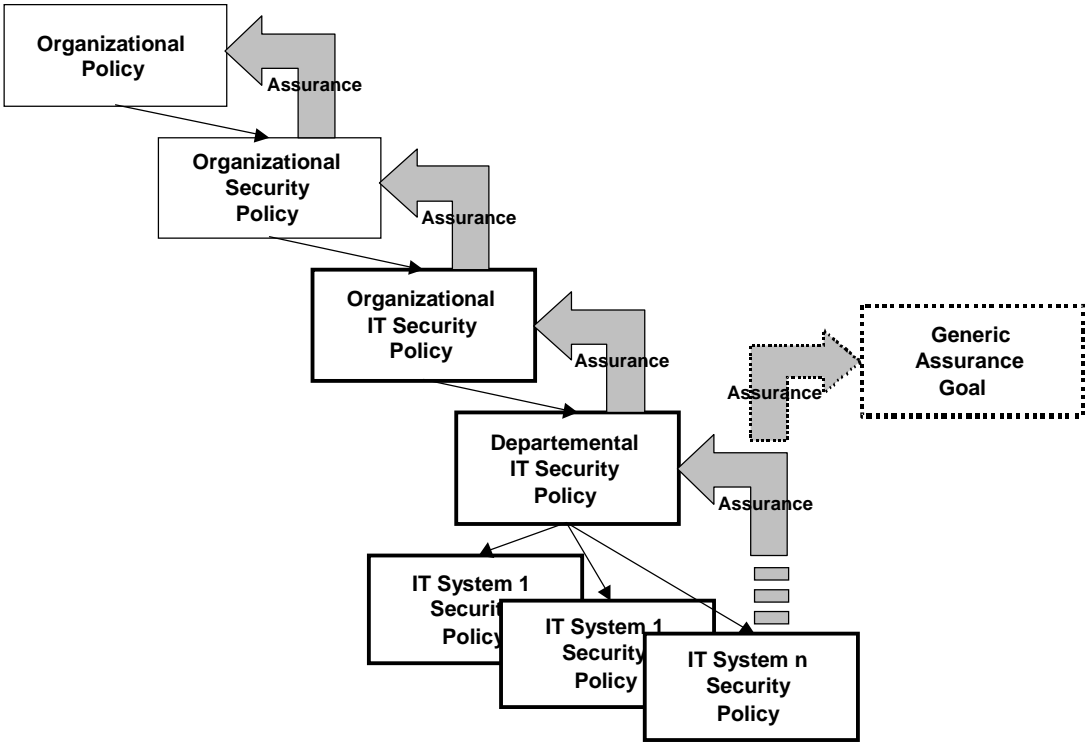


Figure 2 Policy and Assurance Hierarchy

IT Systems will respond to an IT system's security policy. In the presence of diverse individual systems the development of individual system security policies may be necessary.

At the level of a implementable 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. Object of assurance may be the review or audit of the availability and coherence of the security policies.

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.

5.1.5 Applicable Assurance goal

Thus assurance for a given assurance case may be derived by TRA 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 / Protection Profile which has been prepared for a given target environment according to ISO/IEC 15408.

Note: Performing a TRA 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.

5.1.6 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.

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 risks are appropriately covered. 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 analysis has to be performed and will lead to specific measures. This hybrid approach is shown in Figure 3.

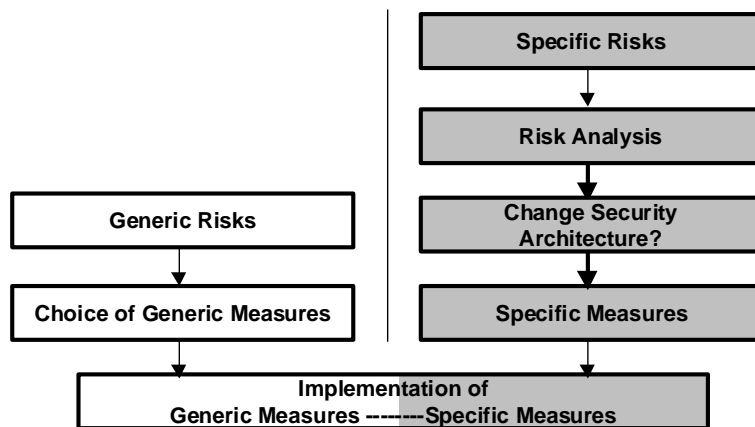


Figure 3 Hybrid Security Model

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 17799) or security targets (ISO/IEC 15408).

5.1.7 Example: ISO/IEC 15408

In ISO/IEC 15408 there are the following decompositions:

- Security Target (ST) — A set of security requirements and specifications to be used as the basis for evaluation of a deliverable.
- Security Function Policy (SFP) — The security policy enforced by an SF.
- Security Function (SF) — A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

5.2 Life Cycle Stages

Selecting assurance methods usually is a complex task. Many methods are available and many are presented in part 2 of ISO/IEC TR 15443.

ISO/IEC PDTR 15443-3

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.

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

There are still many issues to be addressed. This clause of 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.

Part 1 of ISO/IEC TR 15443 has adopted a simplified Life Cycle stage model based on the stage model of ISO/IEC 15288.

In this part of ISO/IEC TR 15443 the Life Cycle stage model will be enhanced by adding the Conception/Specification Phase (refer to Table 1).

Table 1 Life Cycle Stage Model

Assurance - Stage→	Conception/ Specifica- tion	Design/ Implemen- tation	Integration/ Verification	Deployment/ Transition	Operation
---------------------------	--	---	--------------------------------------	-----------------------------------	------------------

Presence of processes corresponding to a Conception/Specification Phase are postulated by many standards. However, a separate life cycle phase is usually not postulated for these processes. Few assurance methods offer well defined associated processes and activities for this life cycle stage.

The reason for this enhancement in this part of ISO/IEC TR 15443 is the fact that ICT security requires particular attention and a increased effort to produce a coherent and non-contradicting specification for the security features of a deliverable. 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 Phases 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:

- C** Conception, leading to the establishment of the security design requirements which may include an overall architecture.
- D** Design, including the processes Stakeholder Functional Requirements Definition, Requirements Analysis, Architectural Design and Implementation
- I** Integration, including the processes Integration and Verification
- T** Transition, including the processes Replication, Transition, Deployment and Validation
- O** Operation, including the processes Operation, Maintenance and Disposal

5.3 Assurance Approach

Methods may approach the assurance of a product by assessing:

- the deliverable, either after of during completion,

- the processes used during the creation of the deliverable,
- the environment in which the deliverable is realized, either in terms of the personnel or organization involved.

Methods also may differ by the extent to which the focus of the assurance approaches is covered.

Table 2 Life Cycle Assurance Approach

Assurance Approach	Focus	Extent
Product Assurance	completed deliverable	complete deliverable
Process Assurance	development process used	all aspects of the deliverable
		some aspect of the deliverable
Environment Assurance	relevant aspects of organization for the creation of deliverable	organizational processes used
		reputation regards specific other products and product warranty actions
		reputation of the organization for any product quality and warranty actions
	qualifications of the individuals employed	relevant tasks performed on deliverable

5.4 Assurance Approach and Life Cycle stages

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 comprise a set of activities and use 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. Assurance may focus on the result of the processes, that is the product, thereby leading to product assurance.

Table 3 Life Cycle Assurance Model

Assurance - Phase→ Assurance - Approach↓	Concep- tion/Specifi cation	Design/ Implemen- -tation	Integration/ Verification	Deployment /Transition	Operation
Product[/System/Service]		⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
Process		D	I	T	O
Environment [/Organization/Personnel]		D	I	T	O

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.

5.5 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).

In this part of ISO/IEC TR 15443 the Life Cycle process model Part 1 will be enhanced 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 phase, such as in the case of ISO/IEC 17799 and the associated ISO/IEC 27001.

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

- 1) Process definition, including development and documentation,
- 2) process repetitive use,
- 3) process assessment and measurement,
- 4) 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.

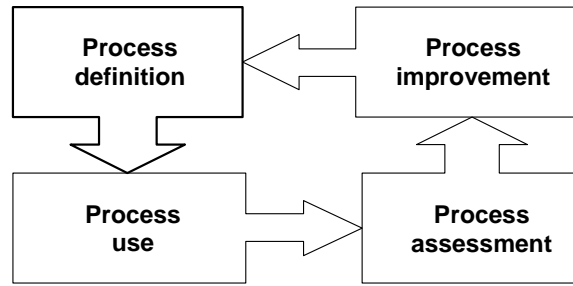


Figure 4 Process Management

Note: 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 deliverable) are subject to process management.

If a method's assurance phase is shown greyed (refer to Table 5, cells 2, 4, 6 and 7) the methods provides process assurance which may be more or less managed.

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

5.6 Graphic Presentation of assurance methods

Table 4 Life Cycle Process Types

Product[/System/Service]	⇒C⇒	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
Process	C	D	I	T	O
Environment [/Organization/Personnel]	C	D	I	T	O

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 phase letter within arrows, in a blank " field, e.g. ⇒D⇒
- Process Assurance: showing the life cycle phase letter white on shaded background, e.g., D
- Environmental assurance: showing the life cycle phase cell as with side bars left and right, e.g. D.

For a particular cell in Table 4 these approaches may be cumulated such that 7 meaningful possibilities as shown in Table 5 exist for a given assurance method and the respective life cycle phase.

Table 5 Assurance Approach

	Product Assurance	Process Assurance	Environmental Assurance	Graphical Representation for Life Cycle stage X
1	✓			⇒X⇒
2		✓		X
3			✓	X
4	✓	✓		⇒X⇒
5	✓		✓	⇒X⇒
6		✓	✓	X
7	✓	✓	✓	⇒X⇒

Note: Evidently, the Level 7 is most complete one in terms of number of components. This does however not imply that the most complete method is necessarily the best in a specific assurance situation. Other aspects of a method have to be considered such as rigor, the level of detail and the associated cost.

5.7 Assurance Concern

Any guidance requires abstraction and simplification to focus on the essential and the applicable. To reduce the number of applicable methods to be compared, respectively the required variety of detail analysis of these methods, this part of ISO/IEC TR 15443 is focussing on guidance in 3 typical situations with high communality of requirements and methods:

- the development of ICT products typically towards a security goal (Developmental Assurance);
- the procurement and integration of products into an ICT system to typically suffice a security goal or policy (Integration Assurance);
- the operation of an ICT systems to typically satisfy a given security policy (Operational Assurance).

5.7.1 Developmental Assurance (DA)

DA is present where a product, system or service is being developed. Development is ideally from scratch: starting with a concept, evolving it into a specification which then is materialized in a developmental process 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, assurance methods may be selected and applied to suit the requirements of Developmental Assurance. Guidance of this part of ISO/IEC TR 15443 will concentrate on the methods which are proven and widely accepted for this purpose, which therefore are few.

5.7.2 Integration Assurance (IA)

IA is present when a multitude of products of divers origin and assurance property are integrated in to a system with the constraint to satisfy a predetermined assurance goal, i.e. to suit an organizational security policy or a protection profile.

Many of the products are finished and proven commercial products. The assurance authority in most cases has to manage a complex assurance situation. The guidance of this part of ISO/IEC TR 15443 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.

5.7.3 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, a running to keep the organizational business operating. Many of the products are finished and the assurance authority in most has to manage a complex assurance situation. Therefore the guidance of this part of ISO/IEC TR 15443 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.

5.7.4 Assurance Concern Summary

The different areas of assurance concern may be shown graphically using Figure 2 of Part 1 of this Technical Report. This simplified representation (refer to 0) denotes the focus of the assurance concern.

Note: The circles denote the focus of the each of the assurance concerns. However, each of the three concerns will contain activities of the stages outside of the focus as shown graphically, these however generally to a lesser degree.

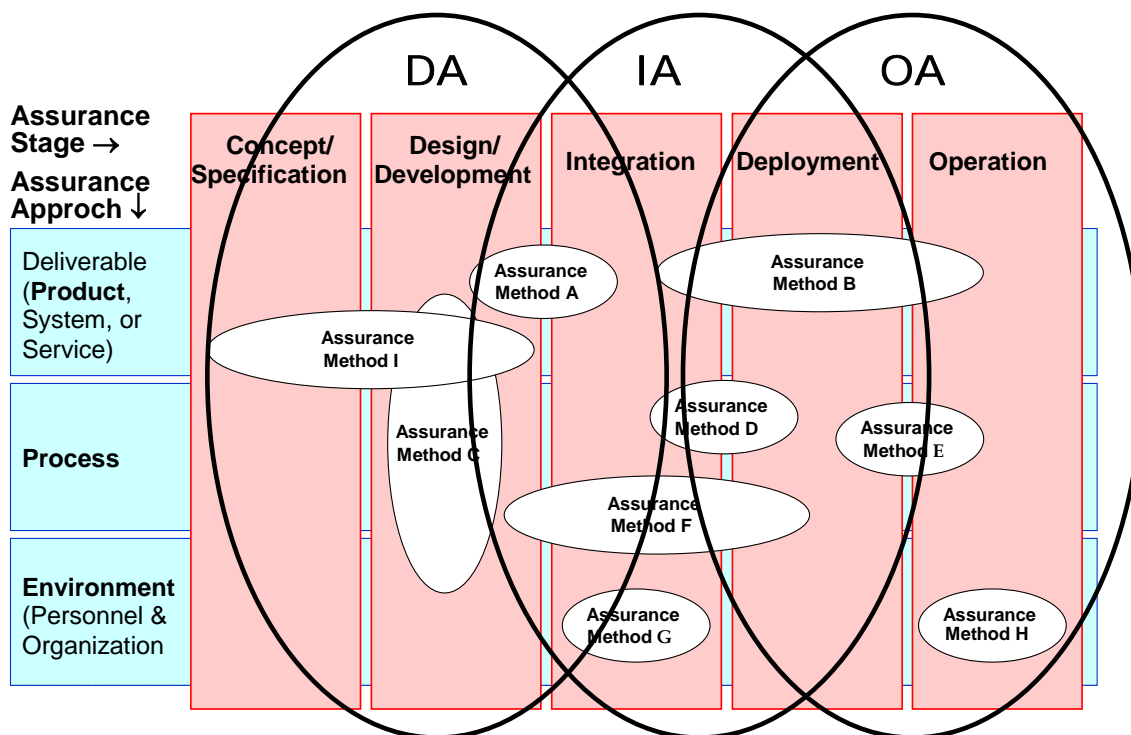


Figure 5 Assurance Concern

5.8 Assessment model

The security relevant properties of a deliverable, 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 gain further assurance that these claims are justified assessment and possibly assessment certification is necessary.

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 or criteria as a basis of an assessment;
- certification that the auditor is qualified and/or that the assessment process has been completed according to the rules

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

5.8.1 Assessor

Assessment of security assurance properties of the deliverable may be conducted by the consumer or user of the deliverable. 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 assessors qualifications are acceptable.

5.8.2 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.

5.8.3 Assessment Evidence

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

Evidence proves the effective resp. the 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.

5.8.4 Assessment verdict

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

5.8.5 Assessment maintenance

Security as opposed to some other technical fields are 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.

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.

5.8.6 Example: ISO/IEC 15408

The assurance authority, e.g., a vendor builds a trusted system to satisfy the security requirements contained in ISO/IEC 15408 (assessment criteria) and Evaluators (assessors in the assessment facility) assess the vendor's system to ensure that the vendor complied with 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 the applicable evaluation body (such as CSE, NSA, NIST, CESG, German BSI/GISA).

This complete process is known as Common Criteria scheme.

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

6 General Guidance to Selection

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 (i.e. several hardware and software components, security services, environmental aspects, or a combination of these).

6.1 Assurance approach

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

- Product[/System/Service] vs. Process assurance
- Process vs. Environment [/Organization/Personnel]
- Product[/System/Service] vs. Environment [/Organization/Personnel]

These 3 approaches correspond to the first three entries Table 5. Goal of this comparison is to gain insight into which kind of assurance approach to choose in a general manner.

Note: Not considered in this discussion are the effects of composition of approaches corresponding to the entries 4 through 7 of Table 5.

6.1.1 Product vs. Process assessment

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

In product assurance the claim is that the deliverable'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 assessment 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 TOE, have predictable and repeatable results and will therefore yield a TOE with established assurance.

However, even the highest trust of a consumer in the processes used by a producer cannot guarantee that these processes have been applied correctly and effectively to a given deliverable. In other words, for higher degrees of assurance of a deliverable, 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 consumer 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.

6.1.2 Process vs. Environment assessment

Process assurance focuses per definition on the processes applied to the product/deliverable in a given number of life cycle stages while environment assurance focuses on the resources and the context in which these resources have been used.

The trust in a deliverable using environment assurance is provided by trust in the organisation and/or its people, as well as on other resources applied to the product deliverable. 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 deliverable.

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 deliverable. There is however no proof that the processes have been documented, are being assessed or have been certified.

Environmental assurance is the lowest form of assurance easiest to obtain. There are situations where environmental assurance is the only assurance practicable and affordable such as in small organisations and with products not accessible to higher level assurance such as COTS. Product vs. Environment assessment

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.

6.1.3 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
- Environmental assurance must be chosen in small organisations or in cases where the organisation producing the deliverable or the deliverable itself is not accessible for process or product evaluation.

In general it can be stated that (refer to Figure 6)

- 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.

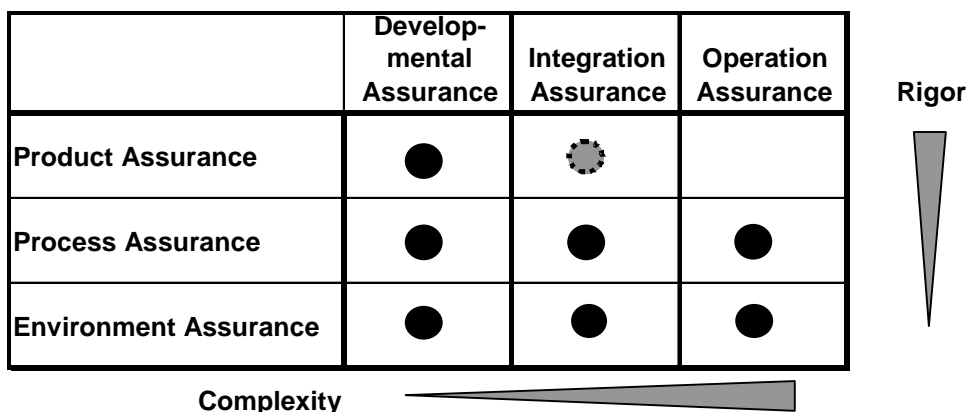


Figure 6 Availability of Methods

6.2 Composition of 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 can also provide a structure, which can be used to record the evidence/experience of those involved in more than one assurance method. This Technical Report provides a common language, etc. in which the interaction between the approaches could be described. This Technical Report can also contribute to the investigations of possible combinations.

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.

The following considerations may provide some 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.

At its most basic level, assurance provides confidence to the recipient that an entity, product or service, will function as claimed by the provider, and perhaps show no 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 in security, and more particularly in the risk equation, whichever version of the risk equation is used, include an element of 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 portion of the contributory factors to the risk. Some of the contributory factors are the vulnerabilities of the target environment and its constituent elements and the security mechanisms contained therein to protect the environment. If the assurance of the devices and security mechanisms within the target environment is raised, then the uncertainty related to those factors is reduced, and thus the overall risk and its associated uncertainty is reduced. In fact it may be that assurance is the only thing that can reduce uncertainty. While no new security mechanism has been added, the risk may have been reduced to an acceptable level, or at least closer to an acceptable level. Thus the organization has received a direct benefit from the assurance they obtained.

It can be seen from the above that the assurance is targeted at the "Risk Taker", at least in part. It would also seem that different aspects or types of assurance are targeted at different recipients or parts of the organization, and also for different purposes. Thus it would appear that combinations of assurance are required and that the ability to replace one type of assurance with another may be very limited. A trade-off between different types may certainly be possible, depending upon the situation, but not a realignment of one form of assurance with another.

None of the methods considered in this Technical Report promise "comprehensive" security that is protecting an existing total solution appropriately against the relevant threats. In each method only part of the problem is considered. In most cases it is therefore necessary to use combinations of methods synergistically.

The differences in objectives and target groups of the sets of IT security criteria show that it may only be possible to obtain a reasonable level of IT security for a total solution if both vendors and users of IT contribute towards this goal in partnership.

7 Guidance Methodology

7.1 Comparison of methods

The aim of this Part 3 is to shell out relative value of select Assurance Methods listed in Part 2 of this Technical Report. For this purpose two (2) principal approaches of comparison may be used: Property Matrix or Pairing (one-to-one comparison).

7.1.1 Matrix Comparison

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

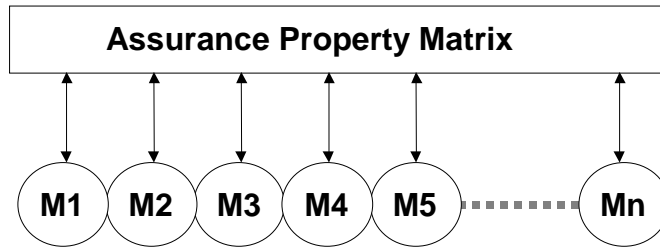


Figure 7 Matrix Comparison Principle

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.

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 user.

In this Part of ISO/IEC 15443 three (3) assurance concerns have been defined in sub-clause 5.7 and selected for guidance and , refer to

11 of this Technical Report show matrix comparisons of selected methods.

7.1.2 One-to-one comparison

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

However, as the number of methods to be compared raises, the number of one-to-one comparisons will rise according to a rule containing the square of the number of items (e.g., 6 items will lead to 15 individual comparison clauses). Therefore this type of comparisons 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.

7.1.3 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: assessment features contributing to its value must be characterised to be more easily compared.

For the purpose of comparing established assurance methods a number of characteristic assurance properties haven been developed. The aim of this part of ISO/IEC 15443 is to help a potential 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 the following **Fehler! Verweisquelle konnte nicht gefunden werden.** are of general nature and a number of assurance methods are analysed on that basis in 11.

The general orientation of the methods is presented in summary form in sub-clause 7.13. From these tables conclusions may be drawn on the applicability reps. non-applicability of a methods in a specific context.

Following this analysis composition of the obtained results for a given deliverable will be discussed in sub-clause 6.2.

The key aspects against which the assurance methods are compared are as follows:

Table 6 Key aspects for comparison

Aspect	Description
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?
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?
Assurance methodology	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?
Assurance scalability	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?
Method's actuality	Does the present version of the method reflect the latest technology? If regular updating is necessary, then how is this ensured?
Assurance Detail	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?
Effort / costs of implementation	What must be expected in the way of effort and costs when a given set of IT security criteria is applied to typical scenarios?
Tool support	Are there any tools which support the user in applying the method concerned?
Requirements for cryptographic	Does the set of IT security criteria concerned contain any provisions

procedures	or prescriptive guidance on cryptographic procedures and algorithms?
Qualification and certification systems	Does a qualification and/or certification system exist for the method? Is the method suitable for products or total solutions?
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 is the market acceptance and its driving forces?
Delay	How much time does the application of assurance method require?

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

7.2 Assurance goal

The Assurance Authority has the task to determine the type of assurance activities as well as the quantity and quality of 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 deliverable 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 stakeholders' individual comfort level.

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

Sub-clause 5.1 explained that an assurance goal may be based on Threat-Risk-Assessment (TRA), Security policy or Baseline reqs. Protection Profile.

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 requirement of the assurance authority, TRA it may be advisable to establish a security goals or to verify the validity of the proposed security goal. Where necessary the proposed goals may be expanded to reflect practice in industry and administration.

Note: Relevant concepts and processes are expressed in existing IT security standards, i.e. ISO/IEC13335, ISO/IEC17799 and ISO/IEC15408.

TRA itself may be assured, i.e. by assessing the personnel delivering the TRA on:

- their experience
- their level of training

- their 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.

7.3 Target audience

This part of ISO/IEC TR 15443 has been tailored to give suit 3 typical situations as explained in sub-clause 5.7. This assurance property will show into which category of

- 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., sufficing a security policy;
- the operation of an ICT systems e.g., to satisfy a given 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?

7.4 Assurance methodology

The assurance approach as defined in sub-clause 6.1 is spelled out. For general guidance on applicable methods refer to sub-clause 6.1

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?

7.5 Assurance versatility

The possibility to reuse parts of an assessment allows to amortise the cost of the work done for a deliverable, e.g. in the future evaluation of a similar deliverable. 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?

7.6 Method's 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? Assurance completeness/detail

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?

In each of the seven Assurance Types identified in 0, with the exception of the last entry, Mandated Assurance, the potential contributory capability of rigorous or soft assurance methods will vary considerable.

The following identifies the likely prime contributory assurance group for each of the first six Assurance Types.

The last Assurance Type is not included as the assurance recipient mandates the assurance form and method and thus contributory value is irrelevant. This consideration applies when specific assurance requirements exist (e.g., legislative dictates, cultural or national considerations) that might limit the list of assurance methods that are acceptable to all the stakeholders in the deliverable.

Assessment aspects are an integral part of the methods as they are presented in this part of ISO/IEC 15443. The aim of assessment aspect analysis is to compare the method's main features which may have pro and con features for fulfilling an assurance authority's needs.

The audience of the assurance verdict may present a varying level of sophistication. This sophistication may require a certain level of rigor (refer to Table 7) guiding the assurance requirements and consequently the method to be used.

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

Table 7 Assessment Rigor

Level	Description
LEVEL 1	Assessment provides a simple "Assurance Seal of Approval",
LEVEL 2	Assessment provides comfort level statements about assurance,
LEVEL 3	Assessment provides detailed facts supporting the claimed assurance,
LEVEL 4	Assessment provides detailed facts supporting the claimed assurance that can be verified,
LEVEL 5	Assessment provides a result that can be presented to a general audience, e.g. a board of directors, and that will be recognised by that audience.
LEVEL 6	Assessment provides a result that can be presented to a security professional audience and that will be recognised by that limited audience.

Note: In addition the strength of that representation must be taken into consideration and the strength of the supporting arguments for the representation.

Table 8 Assurance Type

Assurance Type	Basis	Description of assurance verdict
Pass Through Assurance	Labelling	intended not for the immediate recipient but for the end user, frequently takes the form of content labelling, must be meaningful and recognisable to the end user
Marketing Assurance	Labelling	intended to be used in marketing activities, thus the Assurance needs to be presented in a very brief or encapsulated manner, must be meaningful and recognisable to the end user
Internal Assurance	Trust	Assurance intended for internal uses only, thus can make use of proprietary forms of encapsulation;
External Assurance	Labelling	Assurance intended primarily for External consumption, likely to include much more extensive supporting arguments and materials, may have restricted circulation;
Small Organisation Assurance	Belief	Most small organisations tend to rely on “belief” rather than fact because due to their smaller size they have less specialists available to them to verify that facts are correct unless the organisations happen to specialise in the applicable area;
Large Organisation Assurance	Facts	Larger organisations with more experts available to them and thus more breadth of expertise have a greater ability to verify Facts and thus are more Fact Orientated
Mandated Assurance	Mandate	Assurance form or even the method used to generate the assurance may be mandated by the intended recipient of the assurance, this could be mandated through contractual or registration requirements

7.7 Assurance completeness and detail

The entries may answer the following questions:

- Does the method address the security goal with a closed, exhaustive catalogue of items or are only selected aspects covered?
- For what level of security is the method suited?

7.8 Assurance 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.

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 recipient 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 security assurance goals.

7.9 Tool support

The entries may answer the following question:

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

7.10 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?

7.11 Assessment certification

An even greater increment of assurance is achieved if the assessment is certified and recognized by some assurance 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?

ISO/IEC PDTR 15443-3

- What is 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?

Methods with certification aspects are presented in sub-clause 7.13.2.

7.12 Limitations

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.

This part of ISO/IEC TR 15443 will not contain new methods and international standards for applying these methods which may have been produced.

7.13 Tabular comparisons

7.13.1 Methods and Target User 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, and refer in their use more to products or total systems.

Table 9 Methods and Target User Groups

		ISO/IEC 15408	FIPS 140	ISO/IEC 21827	ISO 13335	ISO 17799	CobIT	IT Baseline Protection Manual	ISO 9000
Key:									
P: primary target group									
S: secondary target group									
X: any organisation									
Type of enterprise	Hardware vendor	S	P	P				S	X
	Software vendor	P	P	P		S		S	X
	Network provider		S			S	S		X
	Server operator		S			P	S	P	X
	Content provider					P		P	X
	Enterprise as user		S		P	P	P	P	X
Role within the enterprise	Management				P	P	P	S	P
	Project management	P	P	P	P	P	P	P	P
	IT security officer	P	P	P	P	P	S	P	S
	IT management	S	S	S	P	P	P	P	S
	Administrators		S			S	S	P	S
	Auditors					S	P	S	S

7.13.2 Major certification schemes

A number of assurance methods have associated schemes for assessment.

Table 10 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 (Organization)	ISO 9000		National/international certification bodies	National/international certification bodies
Environment (IT Operation)	ISO/IEC 17799	ISO/IEC 27001	EA 7/03 based on ISO Guide 62, set by national or regional accreditation scheme operators (e.g. EA, UKAS, JASANZ)	Various national certification bodies

7.13.3 Available Assurance Methods

Mapping the methods presented in 11 against the conclusions in sub-clause 6.1.3 show that the following available methods are obtained for the user concerns:

Table 11 Available Assurance Methods

	Developmental Assurance	Integration Assurance	Operation Assurance
Product Assurance	ISO/IEC 15408 FIP 140		
Process Assurance	ISO/IEC 21827	ISO/IEC 21827	ISO/IEC 17799 COBIT IT Baseline
Environment Assurance	ISO 9000	ISO 9000	ISO 9000

8 Guidance to Developmental Assurance (DA)

The user target for DA has to be defined as shown in sub-clause 5.7.

Available methods have to be chosen/composed such as to offer a conception phase allowing for the definition of a security goal with the required refinement.

Some available assurance approaches for DA have been outlined in Figure 6. Others may be chosen using Part 2 of ISO/IEC 15443. The available methods from the choice in 11 are : ISO/IEC 15408, FIP 140, ISO/IEC 21827 and ISO 9000.

In DA the security goal may be:

- in the case of a singular product this may be a security policy,
- in the case of marketed products a generic security goal common to the targeted user community.

For high security assurance requirement the strength and the correctness of the security functionality of the deliverable has to be assessed. The chosen assurance method has then to contain assessment processes to assure these aspects.

8.1.1 Strength Verification

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

8.1.2 Correctness Verification

The 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.

9 Guidance to Integration Assurance (IA)

The user target for IA has to be defined as shown in subclause 5.7.

Available methods have to be chosen/composed such as to offer a conception phase allowing for the definition of a security goal with the required refinement.

Some available assurance approaches for DA have been outlined in Figure 6. Others may be chosen using Part 2 of ISO/IEC 15443. The available methods from the choice in 11 are : ISO/IEC 19791 (in development), ISO/IEC 21827 and ISO 9000.

In IA the security goal may be:

- in the case of a singular system this may be a security policy,
- in the case of marketed products a generic security goal common to the targeted user community, possibly in the forma of a protection profile.

The user target for IA has to be defined as shown in subclause 5.7.

In most cases an organization will have integrate assurance arising from multiple sources, and in all likelihood will need to integrate that assurance into a total assurance verdict for use in the situation of concern. There may be a lack in assurance requiring a complement.

If the chosen method does not provide for coverage of this aspects the following may be used as guidance.

9.1.1 Interpreting and using diverse assurance results

The level of confidence that can be achieved is closely related to the understanding of the assurance methods and their associated results. The assurance results will need to be reviewed in the context of the situation for which the security design and subsequent assurance evaluation were performed. Effectively, these assurance results can meaningfully be compared by evaluating the inputs and subsequent outputs, much as a black box.

The majority of assessment methods produce more than one type of assurance requirement but the strength of the way the assurance requirement is satisfied varies depending upon the method. Thus the combination of assurance methods selected must be done carefully in order to ensure that the overall assurance goal ultimately is satisfied.

The majority of rigorous assurance 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, in most cases it should be possible to identify a point of intersect or relativity between rigorous assurance methods' scales.

Combining assurance arising from less rigorous or soft assurance methods, while it may at first sight seem much easier as it is not based on detailed analysis, is in fact a much more complex undertaking. The manner in which this is performed will inevitably be much more subjective, and thus unless the rationale used is included along with the result, much more subject to challenge and disagreement. The manner in which the Assurance Package will be used and the purpose to which it will be put will have even greater influence on how soft assurance methods are combined. In all likelihood it will be necessary to include limitations and

constraints in the assurance verdict to help ensure that the assurance provided is not alienated for unintended purposes.

Finally we have the aspect of combining assurance disbaring from both rigorous and soft assurance methods. In this case the problem is some what simplified as in most cases the actual results of rigorous and soft assurance methods will not literally be combined, but in reality used in combination. In this case, the concern is to ensure that neither form of assurance weakens the contribution made by the other, and that they do contribute to and strengthen the other, otherwise the purpose of combination is defeated. Again, the manner in which this is performed will be influenced by the intended usage and purpose of the result.

IA in general includes the transition of an ICT product/system/service from the vendor to the user/operator.

This activity is complicated by the need to potentially combine components, each with a different Assurance Evaluation, into the final deployable product. There is only limited utility in attempting to directly combine the Assurance results. Most assurance schemes are not directly comparable. Instead, one must examine the underlying properties of the assurance processes and the nature of the residual risks resulting from each.

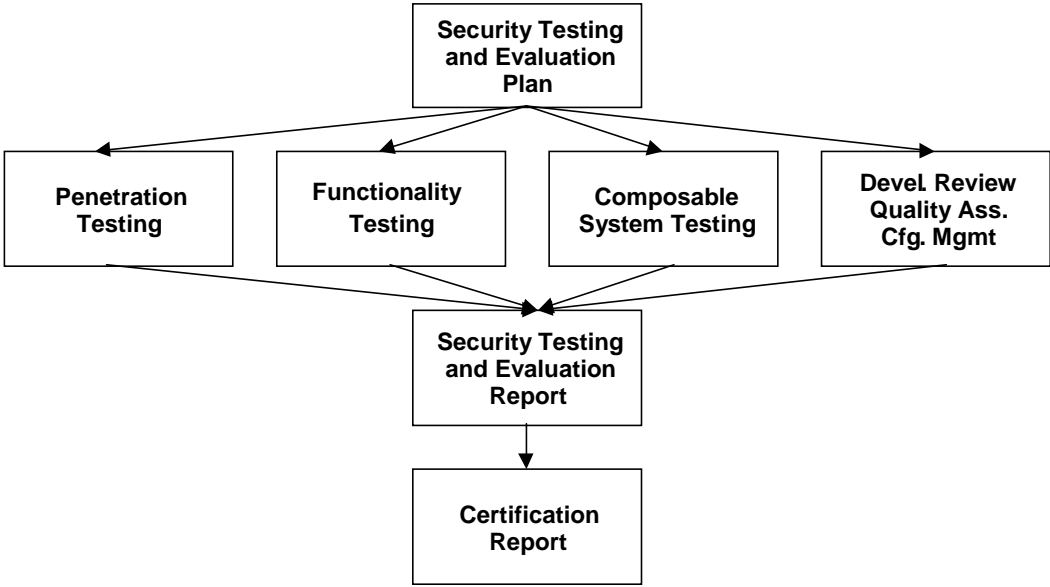


Figure 8 System Testing and Evaluation

9.1.2 Assurance Validation

The design of a system always starts with some high level objectives which are not always directly translatable to precise requirements, whose implementation can be shown using correctness verification arguments. security systems often have objectives or requirements stated in a form that compliance with them cannot be shown by usual Correctness Verification activities. The purpose of the assurance validation activities is to identify critical problems, where the system is compliant with the specification but does not fulfill the security objectives. The main task of all those activities is therefore, to identify side effects of the system or non-covered/suitable aspects, which may lead to critical situations by exploiting the appearance of potential security lacks.

The assurance validation checks that the security objectives are well covered with effectiveness by the security functions of the deliverable. In Integration assurance this amounts typically to a vulnerability assessment generally including penetration testing, covert channel analysis, strength of security function analysis, misuse analysis, fault assumption validation and hardness testing.

9.1.3 Penetration Testing

Penetration tests are performed by evaluators who try to circumvent security mechanisms in the system. The evaluators have access to all documentation describing the system and are given normal user access rights. Penetration tests are not required for all systems, and should only be included in the certification plan if required.

9.1.4 Functionality Testing

The system developer must provide documentation which describes the system's security functionality and functional tests of the security mechanisms. The documentation should include the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing. The tests should be replicable, and written so that the evaluator could carry out the test procedures.

9.1.5 Composable Systems Testing

Subsystems are often developed independent of other subsystems. Even though each subsystem meets the security requirements when tested outside the system, the overall system may not. If additional security mechanisms are added to the system, the effect on the overall system must be evaluated.

Note: Any formal assurance of systems composed of assured systems is in principle impossible without assurance of their composability. Formal composability assurance is not available at this time. With the advent of appropriate security architectures and system security interfaces it may, however, be possible at some time in the future,.

10 Guidance to Operation Assurance (OA)

The user target for OA has to be defined as shown in subclause 5.7.

Available methods have to be chosen/composed such as to offer a conception phase allowing for the definition of a security goal with the required refinement.

Some available assurance approaches for OA have been outlined in Figure 6. Others may be chosen using Part 2 of ISO/IEC 15443. The available methods from the choice in 11 are : ISO/IEC 17799, COBIT, IT Baseline, ISO 9000

In OA the security goal may be:

- in the case of a larger organization a security policy,
- in the case of smaller organizations a generic security goal common to the targeted user community such as a baseline
- a security goal for OA obtained through TRA.

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

10.1 Security Areas

A multitude of security areas may be concerned some of which have legacy character but are still widely considered (refer to Table 12). These areas may have security goals and catalogues of measurers. It has to be made sure that these areas are covered according to up-to-date TRA.

Table 12 Security Areas

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

10.2 Security management areas

Table 13 (source: COBIT) shows an extensive list of domains. Available methods may be mapped against this list to check if the required areas are covered in adequate detail.

Table 13 Security management properties

DOMAIN	COBIT Domains	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

DOMAIN	COBIT Domains	PROCESS
	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

10.3 Operational Assurance Maturity

The implementation of security policy in an organization may be subject to maturity measurement, e.g. as shown in Table 14. Certification of OA maturity will be a valuable addition to assurance.

Table 14 Overall OA Maturity

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

11 Summary

[...to be developed in next stage]

Annex A - Assurance properties of selected methods

The contents of this Annex A has been adapted from publicly available material.

A.1 ISO/IEC 15408

In ISO/IEC 15408 the boundaries of what is evaluated are very carefully defined, and do not always describe a complete product, rather, the boundary described include the stated security functionality of a product. The term used to describe that which is evaluated is "Target of Evaluation" or TOE.

ISO/IEC 15408 is closely related to Common Criteria. The fundamentals of the methodology are well described in ISO/IEC 15408-1.

A 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) IT products and for assurance measures applied to these IT 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 consumers to determine whether these IT products fulfill 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 risks arising from human activities (malicious or otherwise) and to risks 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.

A 1.2 Target audience

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

Consumers

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

Developers

The standard is intended to support developers in preparing for and assisting in the evaluation of their TOEs and in identifying security requirements to be satisfied by those TOEs. These requirements are 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 from consumers 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 TOE against these requirements. It also defines the content and presentation of that evidence.

Evaluators

The CC contains criteria to be used by evaluators when forming judgements about the conformance of TOEs to their security requirements. The CC describes the set of general actions the evaluator is to carry out and the SFRs on which to perform these actions. Note that the CC does not specify procedures to be followed in carrying out those actions.

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

- a) System custodians and system security officers;
- b) Auditors, both internal and external;
- c) Security architects and designers responsible for the specification of security properties of Products;
- d) Accreditors responsible for accepting an IT solution for use within a particular environment;
- e) Sponsors of evaluation responsible for requesting and supporting an evaluation; and
- f) Evaluation authorities responsible for the management and oversight of IT security evaluation programmes.

A 1.3 Assurance methodology

Confidence in IT security can be gained through actions that may be taken during the processes of development, evaluation, and operation. The TOE 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.

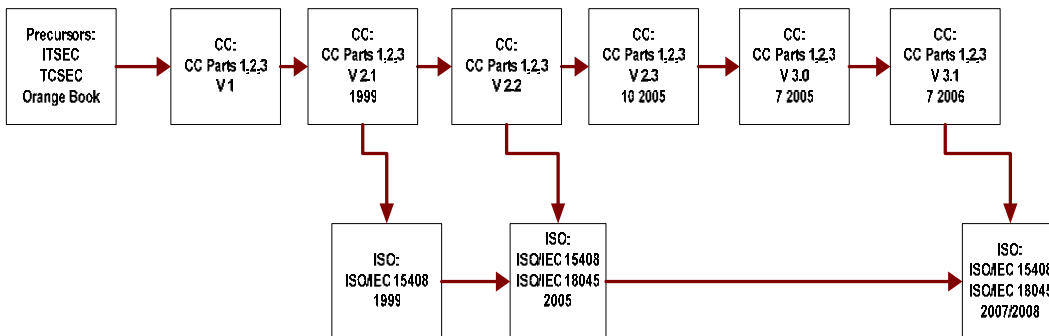
Formal schemes are organized, outside the scope of ISO/IEC 15408, to manage and oversee the activities of evaluations made by independent testing organizations.

A 1.4 Assurance 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.

A 1.5 Method's timeliness

The sets of security assurance method is relatively stable and are 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.



A 1.6 Assurance completeness and detail

This is specified in the ST.

A 1.7 Effort / costs of implementation

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 TOE that need to be corrected. These can range from minor to severe.

A 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.

A 1.9 Requirements for cryptographic procedures

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.

A 1.10 Qualification and certification systems

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/>

A 1.11 Credibility and Recognition

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

The Common Criteria are well recognised and have much credibility.

A.2 FIPS 140-2

A 2.1 Assurance goal

The "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES", published as "Federal Information Processing Standard (FIPS) 140-2" by the National Institute of Standards and Technology (NIST), USA, is 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.

Note: ISO/IEC 19790 was published in 2006 and presents an internationalised version of FIPS 140-2 (ISO/IEC 19790 is a sub-set of the requirements of FIPS 140-2).

A 2.2 Target audience

FIPS 140-2 is applicable to cryptographic modules used in the US government and is mandatory without waiver. Other organizations and governments have also specified its use.

A 2.3 Assurance methodology

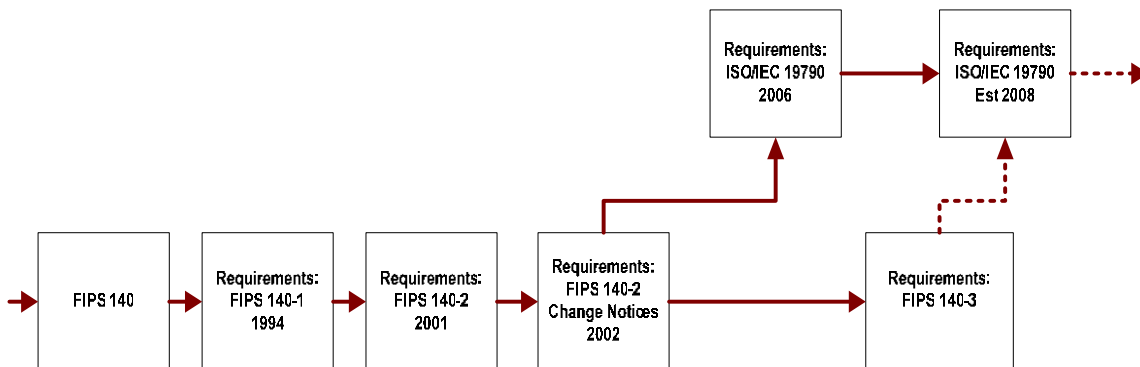
The assurance method uses the conformance testing approach and is essentially applied to the following eleven areas:

- cryptographic module specification
- Ports and interfaces
- roles, services and authentication
- finite state machine model
- physical security
- operational environment
- crypto key management
- EMI/EMC
- self-tests
- Design assurance
- Mitigation of other attacks

A 2.4 Assurance versatility

The different test areas are structured in four levels 1-4 that are built one on top of the other. FIPS 140-2 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.

A 2.5 Method's timeliness



A 2.6 Assurance completeness and detail

As a conformance test the assurance that the cryptographic module meets the requirements of the specification (FIPS 140-2) is high.

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

A 2.7 Effort / costs of implementation

The costs for a FIPS 140-2 validation may include the following elements:

- Validation organization costs, (e.g. NIST CMVP cost recovery)
- Testing laboratory costs

ISO/IEC PDTR 15443-3

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

FIPS 140-2 testing always takes a shorter time than a Common Criteria evaluation as the scope is narrower. The duration of FIPS testing varies depending on:

- Development organization maturity
- Lab experience
- Validation body constraints
- Product maturity
- Conformance versus evaluation

A 2.8 Tool support

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

A 2.9 Requirements for cryptographic procedures

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.

A 2.10 Qualification and certification systems

A north American accreditation scheme, the CMVP, exists as a collaboration with NIST and CSE.

A 2.11 Credibility and Recognition

FIPS 140-2 is a U.S. specification published by the governments' 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.

A.3 ISO/IEC 21827

A 3.1 Assurance goal

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

A 3.2 Target audience

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

A 3.3 Assurance methodology

The assurance method uses the process assurance approach.

A 3.4 Assurance 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.

A 3.5 Method's 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 Publically Available Specification submission from ISSEA. Revision of ISO/IEC 21827 was initiated in 2005.

A 3.6 Assurance completeness and detail

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.

A 3.7 Effort / costs of implementation

The main cost for a 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.

A 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.

A 3.9 Requirements for cryptographic procedures

None.

A 3.10 Qualification and certification systems

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

A 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 FIPS 140 there are no official, governmental agency to upholding the scheme.

A.4 ISO/IEC 13335

A 4.1 Assurance goal

The suite currently comprising four Technical Reports (a fifth report covering the security of networks is planned) provides recommendations for IT security management without mandating any particular solutions. Part 1, „Concepts and models of IT Security“, defines basic terms relating to IT security and elementary aspects (threats, risks, vulnerabilities etc.) and processes (e.g. contingency planning, risk analysis, 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 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.

A 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 phases 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.

A 4.3 Assurance methodology

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.

A 4.4 Assurance 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.

A 4.5 Method's timeliness

Part 1 dates from 1996, Part 2 1997, Part 3 1998 and Part 4 2000. Part 5 has not yet appeared. ISO Technical Reports can be updated at irregular intervals if required. However, the general nature of the statements is unlikely to require this in the foreseeable future.

A 4.6 Assurance completeness and detail

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.

A 4.7 Effort / costs of implementation

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 17799.

A 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.

A 4.9 Requirements for cryptographic procedures

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.

A 4.10 Qualification and certification systems

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

A 4.11 Credibility and Recognition

Recognized as international meta-standard.

A.5 ISO/IEC 27001 and ISO/IEC 17799

[Editing Note: It is proposed to change the number of ISO/IEC 17799 to ISO/IEC 27002 in 2007. If this document is not completed prior to this change, references to ISO/IEC 17799 will be replaced by references to ISO/IEC 27002.]

A 5.1 Assurance goal

The aim of ISO/IEC 27001 and ISO/IEC 17799 is to provide requirements for a "best practice" approach in information security management. ISO/IEC 17799 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 information security risks and the selection of appropriate control objectives and controls.

A 5.2 Target audience

ISO/IEC 27001 and ISO/IEC 17799 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.

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.

A 5.3 Assurance methodology

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 risks based on ISO/IEC 17799.

The standards can be applied in several ways. Firstly, ISO/IEC 17799 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 17799 in combination can be used to implement an information security management system that can be certified by an independent certification body.

A 5.4 Assurance versatility

ISO/IEC 27001 and ISO/IEC 17799 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.

A 5.5 Method's timeliness

ISO/IEC 27001 (2005) and ISO/IEC 17799 (2005) are mature and fully consistent. It is planned that regular updates should occur – in accordance with the general approach for modification of ISO/IEC standards – and that such updates will preserve consistency. There are no fixed, organised, mandatory review cycles.

A 5.6 Assurance completeness and detail

ISO/IEC 27001 and ISO/IEC 17799 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 17799 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 17799 to be excluded with justification if, for example, they are not relevant to the activities within the scope, or if associated security risks do not require treatment. Modification to suit smaller enterprises is possible.

A 5.7 Effort / costs of implementation

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 risk analysis method has a major effect on the amount of effort required.

The cost of 7799-2 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.

A 5.8 Tool support

ISO/IEC 27001 and ISO/IEC 17799 can be supported by tools. Specific tools harmonised to ISO/IEC 27001 are available for the risk analysis phase, for supporting the development and maintenance of the required documents and records, and for the comparison of implemented controls with targets.

A 5.9 Requirements for cryptographic procedures

Cryptography is covered in ISO/IEC 17799 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.

A 5.10 Qualification and certification systems

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 [editing note: the preceding phrase will be deleted if 27015 is published before this document is finalised], specifies requirements for the accreditation of certification bodies.)

A 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.

A.6 IT Baseline Protection Manual

A 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*.

A 6.2 Target audience

This assurance method covers Operation Assurance, as well as Product 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.

A 6.3 Assurance methodology

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 infrastructural components but affect large areas or even the entire IT environment.

A 6.4 Assurance 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).

A 6.5 Method's 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.

A 6.6 Assurance completeness and detail

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.

A 6.7 Effort / costs of implementation

As the standard security measures are oriented to normal security requirements, generally no cost intensive services or expensive security or infrastructural 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.

A 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.

A 6.9 Requirements for cryptographic procedures

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.

A 6.10 Qualification and certification systems

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.

A 6.11 Credibility and Recognition

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

A.7 CobiT

A 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 the risks arising.

A 7.2 Target audience

This assurance method covers Operation Assurance

CobiT distinguishes the following target groups:

Management – for support when weighing up risks 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.

A 7.3 Assurance methodology

The assurance method uses the environment assurance approach.

ISO/IEC PDTR 15443-3

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.

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 approx. 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.

A 7.4 Assurance 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).

A 7.5 Method's 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“.

A 7.6 Assurance completeness and detail

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.

A 7.7 Effort / costs of implementation

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

A 7.8 Tool support

The use of CobiT is supported by the following 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.

A 7.9 Requirements for cryptographic procedures

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.

A 7.10 Qualification and certification systems 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.

A 7.11 Credibility and Recognition

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

A.8 ISO 9000

A 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.

A 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.

Here, documentation of processes helps the organisation to achieve a 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.

A 8.3 Assurance methodology

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.

A 8.4 Assurance 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.

A 8.5 Method's 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 environmental management system.

A 8.6 Assurance completeness and detail

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.

A 8.7 Effort / costs of implementation

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.

A 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.

A 8.9 Requirements for cryptographic procedures

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.

A 8.10 Qualification and certification systems

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

A 8.11 Credibility and Recognition

The probably most widely recognized international standard.

Annex B - Composition of assurance methods

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 FIPS 140 should be used for this.

On the part of the users, 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 17799 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.

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

Often a combination, such as, for example, IT Baseline Protection and parts of ISO/IEC 15408, is used. 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 make available 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.

B.2 ISO 17799 + IT Baseline Protection

Standard ISO 17799 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 17799 and IT Baseline Protection can thus produce a 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 had to ISO/IEC 15408 and/or to Protection Profiles.

B.3 ISO/IEC 27001 and ISO/IEC 17799

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 other ISO-standardised management systems.

Assessable requirements are specified for information security management in all lifecycle phases. Documented processes can be assessed in the context of an organisation's objectives. Associated records 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 PDTR 15443-3

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 17799 are used as the basis for treating unacceptable risks.

B.4 ISO 17799 + 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 standard 17799 can be used as a supplement that is specifically concerned with the management of information security.

In particular, ISO 17799 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 17799 are directed at management level.

B.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 FIPS 140 when the subject of interest is cryptographic procedures.

Annex C - Case Studies

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

The chip-card manufacturer chose a composition of ISO/IEC 15408 + FIPS 140-2 + 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 FIPS 140-2 level 3 evaluations and a level 3 evaluation.

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:

- FIPS 140-2 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 a ISO/IEC 21827 conforming processes to develop products ready for FIPS 140 or ISO/IEC 15408 evaluations. The benefits are:

- Documents required for ISO/IEC 15408 EAL4 or FIPS 140-2 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 resp. FIPS 140-2 will be done.

Bibliography

ISO/IEC 17025:1999: General requirements for the competence of calibration and testing laboratories. (ISO/IEC 17025 replaces guide 25 and is identical to ISO/IEC EN45001.)

ISO/IEC 17024 Personnel assessment (the document refers to assuring personnel)

ISO/IEC Guide 61 General requirements for assessment and accreditation of certification/registration bodies

ISO/IEC Guide 65 General requirements for bodies operating product certification systems

ISO/IEC Guide 67 on the fundamentals of product certification

ISO/IEC Guide 70, first, second and third party certification

Cohen, Aaron, *Review of ISO Assurance Approaches*, The First Annual International Systems Security Engineering Conference, San Antonio, Texas, February 3-4, 2000

AAWG, *Task 1 Report, Draft Version 0.9. ISO/IEC 15408 Project: Assurance Approaches Working Group* (report: AAWG-97/037, annex A: AAWG-97/038), August 1997.

EN 45001: General criteria for the operation of testing laboratories. (CEN/CENELEC)

EN 45013: General criteria for certification bodies operating certification of personnel. (CEN/CENELEC)

FIPS 140-1: Federal Information Processing Standard: Security Requirements for Cryptographic Modules, U.S. Department of Commerce, National Institute of Standards and Technology, January 11, 1994,

FIPS PUB 31: Guidelines For Automatic Data Processing Physical Security And Risk Management

IT Baseline Protection Manual Standard, Security Safeguards Standards, BSI/GISA, October 2000

Example: Philippe Kruchten, *The Rational Unified Process -- An Introduction*, Addison-Wesley-Longman, Reading, MA, USA

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

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>

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>

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>

A Comparative Study of IT Security Criteria, Initiative D21, *****

Fiona Pattinson, *Comparing ISO 17799:2000 with SSE CMM V2, 2002*, *****