



ISO/IEC JTC 1/SC 27 N 3592

ISO/IEC JTC 1/SC 27/WG 3 N 617

REPLACES: N 3371

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Text for DTR

TITLE: Text for ISO/IEC 1st DTR, Information technology - Security techniques – A framework for IT security assurance - Part 1: Overview and framework

SOURCE: Project Editor (Aaron Cohen)

DATE: 2003-06-11

PROJECT: 1.27.21.01

STATUS: In accordance with resolution #10 (reference document SC 27 N 3624) of the 15th SC 27 plenary meeting in Québec City, Canada, 2003-05-05/06 this document has been sent to the JTC 1 Secretariat for a 3-month letter DTR ballot. It is circulated within SC 27 for information.

DISTRIBUTION: P- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners

ACTION ID: FYI

DUE DATE:

MEDIUM: Livelink-Server

NO. OF PAGES: 27

Secretariat ISO/IEC JTC 1/SC 27 –

DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany

Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;

[HTTP://www.ni.din.de/sc27](http://www.ni.din.de/sc27)

Contents

1	Scope	5
1.1	Purpose.....	5
1.2	Approach	5
1.3	Application	5
1.4	Field Of Application	5
1.5	Limitations	5
2	Normative references	5
2.1	ISO references	5
2.2	Non-ISO references	6
3	Terms and definitions	6
4	Abbreviated terms	10
5	Concepts.....	14
5.1	Why do we need assurance?	14
5.2	Assurance is distinguishable from confidence.....	14
5.3	What is a deliverable?	14
5.4	Assurance requirements.....	15
5.5	Assurance methods applicability to IT security	15
5.6	Assurance schemes	16
5.7	Quantifying assurance risk and mechanism strength.....	16
5.8	Assurance reduces security risk	16
5.9	Quantifying assurance	17
5.10	Stakeholders	17
5.11	Assurance authority	17
6	Selecting security assurance	18
6.1	Assurance requirements specification	19
6.2	Economical aspects	19
6.3	Organisational policies	19
6.4	Security Assurance Model.....	20
6.5	Technical aspects	20
6.6	Optimisation considerations	21
7	Framework.....	21
7.1	Assurance approach	21
7.2	Assurance Methods.....	22
7.3	Assurance and life cycle aspects	23
7.4	Correctness versus effectiveness assurance	24
7.5	Categorisation of assurance methods	24
7.6	Composite assurance	25
7.7	Assurance rating	26
8	Bibliography.....	27

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 assurance 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) a framework model to position existing assurance methods and to show their relationships;
- b) a collection of assurance methods, their description and reference;
- c) a presentation of common and unique properties specific to assurance methods ;
- d) qualitative, and where possible, quantitative comparison of existing assurance methods ;
- e) identification of assurance schemes currently associated with assurance methods;
- f) a description of relationships between the different assurance methods ; and
- g) 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, SSE-CMM, 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

To introduce, relate and categorise security assurance methods to a generic life cycle model in a manner enabling an increased level of confidence to be obtained in the security functionality of a deliverable.

1.2 Approach

The approach adopted throughout this Technical Report presents an overview of the basic assurance concepts and terms required for understanding and applying assurance methods through a framework of identifying various assurance approaches and assurance stages.

1.3 Application

Using the categorisation obtained through Part 1 of this Technical Report, Parts 2 and 3 will guide the reader in the selection, and possible combination, of the assurance method(s) suitable for application to a given deliverable.

1.4 Field Of Application

Part 1 of this Technical Report will provide guidance for the categorisation of assurance methods including those not unique to IT security. It may be used in areas outside of IT security where criticality warrants assurance.

1.5 Limitations

Part 1 of this Technical Report will apply to deliverables (refer to clause 3.19) and their related organisational security issues only.

2 Normative references

Refer to the following sub-clauses for normative ISO references and non-ISO references for further clarification of terminology, concepts and explanations. These references may be used to further the reader's understanding of Part 1 of this Technical Report. At the time of publication, the editions indicated were used in the composition of Part 1 of this Technical Report.

2.1 ISO references

All normative documents are subject to revision. The most recent editions of the normative documents indicated may contain variations. Members of IEC and ISO maintain registers of current valid International Standards.

ISO Guide 2: 1996 Standardisation and related activities - General vocabulary.

ISO 9000:2000 Quality management systems - fundamentals and vocabulary.

ISO 9001:2000 Quality systems - Model for quality assurance in design, development, production, installation and servicing.

ISO/IEC 9126-1 FDIS Software engineering - Product quality - Part 1: Quality model.

ISO/IEC 13335 Guidelines for the Management of IT Security.

ISO/IEC TR 13335-1 1996 Information technology -- Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.

ISO/IEC 14598-1:1999 Information technology - Software product evaluation - Part 1: General overview.

ISO/IEC 15288 FCD System Engineering - System Life Cycle Processes.

ISO/IEC 15504, Information Technology –Software Process Assessment (all parts).

ISO/IEC 15443-1 WD3

ISO/IEC 15408, Parts 1-3, IT Security Evaluation.

ISO/IEC 18045, Methodology for IT security evaluation (also known as Common Evaluation Methodology (CEM)).

ISO/IEC 17799:2000, Information Technology – Code of Practice for Information Security Management.

ISO/IEC 21827, Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM).

2.2 Non-ISO references

This clause contains non-ISO references that are considered normative for the purposes of this Technical Report.

AGCA: A Guide to Certification and Accreditation for Information Technology Systems, Communications Security Establishment, Government of Canada, Ottawa, 1996.

Information Technology Security Evaluation Criteria (ITSEC), Version 1.2 (Provisional), Office for Official Publications of the European Communities, June 1991.

SSAM® (method) *System Security Engineering Capability Maturity Model, Appraisal Methodology*, Version 1.1. June 1997. Available from Internet: < <http://www.issea.org> >.

The Canadian trusted computer product evaluation criteria: version 3.0e / Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993. Available From: National Library of Canada [xxv, 208 p. : ill. ; 28 cm], LC Call no.: QA 76.9 .A25 C36 1991.

Trusted Computer System Evaluation Criteria (TCSEC), DoD Standard 5200.28-STD, U.S. Department of Defense, December 1985.

Trusted Product Evaluation Program (TPEP) Overview, National Computer Security Center (NCSC), National Security Agency (NSA). Available from Internet: < <http://www.radium.ncsc.mil/tppep/process/procedures.html> >.

3 Terms and definitions

The terms and definitions have been developed to be as generic as possible to support the assurance model developed in Part 1 of this Technical Report. The assurance model, being applicable to a broad spectrum of assurance approaches, requires non-specific terminology to be applicable to a broad spectrum of assurance approaches.

Defining terms for a generic assurance model is a difficult task owing to the myriad of assurance terms that exist to satisfy the available assurance approaches. Furthermore, similar terms have different definitions and many are unique to a particular assurance approach making it difficult to construct a generic language for the assurance model. Owing to these difficulties, terms and definitions have been crafted to ensure the neutrality of the assurance framework and applicability to a wide range of assurance methods. Relevant ISO standards are used wherever possible, in particular to maintain compatibility to ISO/IEC 15408 Parts 1 - 3 and ISO 9000 series.

The next difficulty was how to address the multiple definitions that existed for the same term and definitions that were not used, as they were not generic enough for the model. Should these terms be ignored or maintained for reference purposes? Ignoring definitions posed the problem of confusing readers when discussing the assurance approach from which they came. Maintaining definitions specific to a unique assurance approach added a level of formatting complexity to this Technical Report; however, the appropriate definition could then be used within the correct context. It was decided to maintain the previous definitions and to present them in a clear manner. Where multiple definitions exist for the same term, the principal definition for the purpose of this Technical Report is listed first. Alternate definitions are only applicable when cited in the context of their source, are bulleted and denoted in italics.

3.1 accreditation

Procedure by which an authoritative body gives formal recognition, approval, and acceptance of the associated residual risk:

- a) for the operation of an automated system in a particular security mode using a particular set of safeguards [adapted from AGCA];
- b) that a security body or person is competent to carry out specific tasks [adapted from ISO Guide 2]; and
- c) that a security service is suitable for the target environment.

3.2

approach

The method used or steps taken in setting about a task or problem.

3.3

assessment

Verification of a deliverable against a standard using the corresponding method to establish compliance and determine the assurance.

3.4

assurance

Performance of appropriate activities or processes to instil confidence that a deliverable meets its security objectives.

- *Grounds for confidence that an entity meets its security objectives [ISO/IEC 15408–1].*

3.5

assurance approach

A grouping of assurance methods according to the aspect examined.

3.6

assurance argument

A set of structured assurance claims, supported by evidence and reasoning, that demonstrate clearly how assurance needs have been satisfied.

3.7

assurance assessment

Verification and recording of the overall types and amounts of assurance associated with the deliverable (entered into the assurance argument).

3.8

assurance authority

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

Note: In specific schemes or organisations, the term for assurance authority may be different such as evaluation authority.

3.9

assurance evidence

Work products resulting from the assurance analysis of the deliverable (including summary reports or other justification) that supports the assurance claim.

3.10

assurance level

The amount of assurance obtained according to the specific scale used by the assurance method.

Notes:

1. the assurance level may not be measurable in quantitative terms.
2. The amount of assurance obtained is generally related to the effort expended on the activities performed.

3.11

assurance method

A recognised specification for obtaining reproducible assurance results.

3.12

assurance property

A characteristic of an assurance method that contributes to the assurance result.

3.13

assurance result

Documented numerical or qualitative assurance statement pertaining to a deliverable.

3.14

assurance scheme

The administrative and regulatory framework under which an assurance method is applied by an assurance authority within a specific community or organisation.

- *The administrative and regulatory framework under which the Common Criteria is applied by an evaluation authority within a specific community [ISO/IEC 15408–1].*

3.15

assurance stage

The deliverable life cycle stage on which a given assurance method is focused. The overall deliverable assurance takes into account the results of the assurance methods applied throughout the deliverable life cycle.

3.16

assurance evidence

Workproducts or any items generated from the assurance analysis of the deliverable including reports (justification) to support the assurance claim.

3.17

certification

Procedure by which a formal assurance statement is given that a deliverable conforms to specified requirements. Certification may be performed by a third party or self-certified. [adapted from ISO/IEC Guide 2:1996].

- *The issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used where correctly applied [ITSEC].*
- *The certification process is the independent inspection of the results of the evaluation leading to the production of the final certificate or approval [ISO/IEC 15408–1].*
- *Certification The comprehensive assessment of the technical and non-technical security features of an information technology system, made in support of accreditation that establishes the extent to which a system satisfies a specified security policy [AGCA].*

3.18

confidence

A belief that a deliverable will perform in the way expected or claimed (i.e. properly, trustworthy, enforce security policy, reliably, effectively).

3.19

deliverable

An IT security product, system, service, process, or environmental factor (i.e. personnel, organisation) or the object of an assurance assessment. An object may be a Protection Profile (PP) or Security Target (ST) as defined by ISO 15408-1.

Note: ISO 9000:2000 holds that a service is a type of product and "product and/or service" when used in the ISO 9000 family of standards.

3.20

evaluation

Assessment of a deliverable against defined criteria (adapted from ISO/IEC 15408–1).

- *Systematic examination (quality evaluation) of the extent to which an entity is capable of fulfilling specified requirements [ISO/IEC 14598-1].*

3.21**guarantee**

Refer to the definition for *Warranty* in clause 3.35.

3.22**IT security product**

A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems [ISO/IEC 15408–1].

3.23**life cycle stage**

An instance within the deliverable life cycle that relates to the state of the deliverable.

- *A period within the system life cycle that relates to the state of the system description and/or the system itself [ISO/IEC 15288].*

3.24**pedigree**

Informal recognition of the vendor's consistent repeatability to provide deliverables that satisfy its security policy or to perform as claimed (pedigree is an environmental factor associated with the vendor or deliverable).

3.25**process**

An organised set of activities which uses resources to transform inputs to outputs [ISO 9000: 2000]

3.26**process assurance**

Assurance derived from an assessment of activities of a process.

3.27**product**

Refer to the definition of deliverable.

3.28**scheme**

Set of rules defining the environment, including criteria and methodology required to conduct an assessment [adapted from ISO 18045 (Common Evaluation Methodology)].

3.29**security**

All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability [ISO 13335-1].

Note: A product, system, or service is considered to be secure to the extent that its users can rely that it functions (or will function) in the intended way. This is usually considered in the context of an assessment of actual or perceived threats.

- *The capability of the software product to protect information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them [ISO/IEC 9126-1].*

3.30**security assessment**

Verification of a security deliverable against a security standard using the corresponding security method to establish compliance and determine the security assurance.

- *The last stage of the product evaluation process [ISO/IEC 14598-1].*

3.31**security element**

An indivisible security requirement.

**3.32
service**

A security process or task performed by a deliverable, organisation, or person.

**3.33
system**

A specific IT installation, with a particular purpose and operational environment [ISO/IEC 15408–1].

- *A combination of interacting elements organized to achieve one or more stated purposes [ISO/IEC 15288].*

NOTES:

1. A system may be considered as a product and/or as the services it provides [ISO/IEC 15288].
2. In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g. aircraft system. Alternatively the word system may be substituted simply by a context dependent synonym, e.g. aircraft, though this may then obscure a system principles perspective [ISO/IEC 15288].

**3.34
system life cycle**

The evolution with time of the system from conception through to disposal [ISO/IEC 15288].

**3.35
warranty**

A security service to correct or mitigate the deliverable's operation (deployment, performance, or delivery) if it does not satisfy its security policy.

**3.36
work product**

All items (i.e. documents, reports, files, data, etc.) generated in the course of performing any process for developing and supplying the deliverable [SSE-CMM].

- *Result of a system of activities, which use resources to transform inputs into outputs [ISO 9001].*

4 Abbreviated terms

The following abbreviations are used in this Technical Report.

AAWG

Assurance Approaches Working Group (Common Criteria Project)

AST

Abstract Security Target

ATM

Attack Tree Methodology

BP

Base Practice

BSI

Bundesamt für Sicherheit in der Informationstechnik (German Information Security Agency)

CASCO

Committee on conformity assessment

CC

Common Criteria (precursor of, and equivalent to ISO/IEC 15408)

CEM

Common Evaluation Methodology (previous title for NP N2729r1 Methodology for IT security evaluation)

CMM

Capability Maturity Model

CMS

Certificate Maintenance Scheme

COTS

Commercial off the shelf (products)

CSE

Communications Security Establishment (Canadian IT Security Agency)

CT

Conformance Testing

CTCPEC

Canadian Trusted Computer Product Evaluation Criteria (edited by CSE)

DA

Developmental Assurance

DAL

Developmental Assurance Level

EA

Evaluation Assurance

EAL

Evaluation Assurance Level (Term specific to 15408; defined in ISO/IEC 15408-1)

EMC

Electromagnetic Compatibility

FHM

Flaw-hypothesis methodology

FM

Formal Method(s)

FR

Flaw Remediation

FRITSA

Framework for IT Security Assurance (synonym to ISO/IEC 15443)

GMITS

Guidelines for the Management of IT Security (synonym to ISO/IEC 13335)

GP

Generic Practice (Term specific to CMM)

HCD

Human Centered Design

ISO/IEC 15443-1 WD3

- IEC**
International Electrotechnical Commission
- IT**
Information Technology
- ISO**
International Organization for Standardisation
- ITSEC**
Information Technology Security Evaluation Criteria (Office for Official Publications of the European Communities)
- ITSEM**
Information Technology Security Evaluation Methodology (Office for Official Publications of the European Communities)
- KISEC**
Korean Information Security Evaluation Criteria
- KISPEP**
Korean Information Security Product Evaluation Program
- KPA**
Key Process Area (CMM)
- LVD**
Low Voltage Directive
- NIST**
National Institute of Standards and Technology (Government Agency of the USA)
- NSA**
National Security Agency (Government Agency of the USA)
- PA**
Personnel Assurance
- PP**
Protection Profile (defined in ISO/IEC 15408-1)
- QM**
Quality Management
- RAMP**
Ratings And Maintenance Phase (NSA process following TCSEC evaluations)
- RM**
Ratings and Maintenance phase (CSE process following CTCPEC evaluations)
- SCT**
Strict (Security) Conformance Testing
- SdoC**
Suppliers' declaration of Conformity
- SE**
Software Engineering

SE-CMM

System Engineering Capability Maturity Model (Capability Maturity Model is a Trade Mark™ of Carnegie-Mellon University)

SEI-CMM

Software Engineering Institute Capability Maturity Model (Capability Maturity Model is a Trade Mark™ of Carnegie-Mellon University)

SPICE

Software Process Improvement and Capability d'-Etermination (precursor of, and equivalent to ISO/IEC 15504)

ST

Security Target (defined in ISO/IEC 15408-1)

SSAM®

SSE-CMM Appraisal Methodology (promoted by Support Organization), an entity within the International Systems Security Engineering Association (ISSEA)

SSE-CMM®

System Security Engineering - Capability Maturity Model ISO/IEC 21827 (submitted to ISO as a publicly available standard by the Support Organization of the International Systems Security Engineering Association (ISSEA))

TAL

Testing assurance level

TCMM

Trusted Capability Maturity Model (refer to NSA)

TCSEC

Trusted Computer System Evaluation Criteria (edited by NSA)

TOE

Target of Evaluation (Term specific to ISO/IEC 15408 and defined in ISO/IEC 15408-1)

TPEP

Trusted Product Evaluation Program (TCSEC and CTCPEC)

TRA

Threat and Risk Assessment

TSDM

Trusted Software Development Methodology (refer to NSA)

TTAP

Trust Technology Assessment Program (successor to TPEP, refer to NSA)

TQM

Total Quality Management

VSA

Vendor Security Analyst (refer to RAMP)

WA

Warranty Assurance

5 Concepts

This section introduces the concepts of assurance and aims to differentiate the applicability of assurance concepts between general IT assurance and IT security assurance. The concepts are broad and should not be applied specifically to IT security or conformity assessments.

5.1 Why do we need assurance?

IT systems are prone to failure and security violations due to errors and vulnerabilities. These errors and vulnerabilities can be caused by rapidly changing technology, human error, poor requirement specifications, poor development processes or as a result of underestimating the threat. In addition, system modifications, new flaws, and new attacks are frequently introduced contributing to increased vulnerabilities, failures, and security violations throughout the IT system life cycle.

Due to human error or oversight, component or equipment failure, and due to imperfection of the opposing security mechanisms, error-free, failure-free and risk-free operation is not usually achievable within acceptable cost and time constraints over the deliverable of the IT system life cycle. This situation makes it almost impossible to guarantee an error-free, risk-free, and secure IT system.

From the above paragraphs, it can be seen that errors, vulnerabilities and risks will probably always exist and may change over the deliverable's life cycle. Therefore, the errors, vulnerabilities and risks will have to be managed over the deliverable's life cycle within acceptable parameters otherwise the deliverable assurance will change. The task of IT security engineering and management is to manage the security risk by mitigating the vulnerabilities and threats with technological and organisational security measures to achieve a deliverable with acceptable assurance. IT security management has an additional task of establishing acceptable assurance and risk objectives. In this way, the stakeholders of an IT system will achieve reasonable confidence that the deliverable performs in the way intended or claimed with acceptable risk and within budget. From a security standpoint, this translates into confidence that the deliverable enforces the applicable security policy.

5.2 Assurance is distinguishable from confidence

It is important to point out that assurance and confidence are not identical and cannot be used in place of one another. Too often, these terms are used incorrectly as they are closely related. It is important for the reader to understand the distinction between these two terms. Confidence is related to the belief that one has in the assurance of the deliverable whereas assurance is related to the deliverable's ability to perform (satisfy) its security objectives. Therefore, confidence is not a certainty but an expression of trust and belief created through assurance.

Assurance is determined from the evidence produced by the assessment process of the deliverable. The evidence, usually composed of an assurance argument, documentation, and other related work products, substantiates the claimed assurance based on the security engineering and assessment activities.

Confidence is subject to the individual's perception of their own security requirements and to the knowledge gained in assessment processes that the deliverable will perform in the way expected or claimed. Starting with the assurance criteria and method to the scheme and assessment process, and finally of the reputation of methods and assessors, and experience in assessment and operation. As a consequence, by their individual perception, stakeholders may have different degrees of confidence after the performance of a given assurance method by a given person or organisation.

5.3 What is a deliverable?

Traditionally, assurance has only been associated with IT products and systems composed of hardware or software and referred to as product or system assurance. It is now recognized that to address a wider range of risks, there is a need for assurance of other security objectives such as a security service, process, personnel, organisation, or other environmental factors. To address this new requirement, the term "deliverable" is used to refer to the objective of the security assessment.

IT security products, services, and any other tangible or intangible security item sold (whether one-of-a-kind or mass produced), leased, trained, or contracted out are listed as line items on a contract and are therefore considered to be deliverables as they are either delivered to the client or performed for the client as the case may be. Furthermore, this includes any deliverable whether provided as a service, shareware, freeware, sample, or by other means and whether supplied directly or indirectly (warranty, guaranty, pedigree, etc.) or assumed by the

consumer (pedigree, warranty, etc). These have measurable security attributes that can be verified to meet their security policy. For example, the deliverable may refer to a Threat and Risk Assessment (TRA) service performed by an organisation or it may refer to the certification of personnel qualified to perform evaluations using the ISO 15408 criteria. Personnel performing a security service or task are also considered to be deliverables. For example, those being trained to become evaluators, have a contract with the training organisation and are measured or graded on their abilities to acquire the knowledge and perform specific activities. Similarly, security consultants performing a service or task are also under contract.

Some assurance deliverables do not always appear as line items although they provide varying levels of confidence to Assurance Authorities and therefore must be factored into the security assessment. For instance, warranties and guarantees are specific services provided by the vendor either as stand-alone or as an additional feature bundled with the deliverable supplied. Warranty services serve to correct or mitigate the deliverable's operation (deployment, performance, or delivery) if it does not satisfy its security policy. A pedigree is an environmental factor associated with the vendor or deliverable, which although somewhat vague, cannot be discounted due to a recognized history of special performance such as consistent and repeated performance to meet its security policy or to meet the vendor claims.

Note: This definition of deliverable is similar to the term TOE defined in ISO/IEC 15408-1 except that deliverable has a broader application.

5.4 Assurance requirements

In terms of IT security, adequate assurance signifies that specific predefined security assurance requirements have been satisfied by performing appropriate assurance processes and activities, i.e. as prescribed by a chosen assurance method. Assurance requirements are determined from the security requirements and other driving factors.

Security assurance requirements are determined by analysing the security requirements for the deliverable, influencers, security requirements (policies), business drivers and the target environment for the deliverable. Influencers are any considerations that need to be addressed as they might affect the deliverable assurance requirements. The influence can have any origin and may not even be tangible such as politics, culture, local laws, and mandated requirements. A Risk Assessment is performed to provide an in-depth look at the asset sensitivity, vulnerabilities, and threats to determine the residual risk and recommendations for existing and proposed safeguards. The recommendations implemented are factored into the original security requirements to revise the security assurance requirements.

General guidance on security management and for performing a risk analysis can be found in ISO/IEC 13335 and ISO/IEC 17799. ISO/IEC 15408 Parts 1-3 contains information on security functional and assurance requirements for IT products and systems specific to traditional IT security evaluations.

Assurance requirements are unique to each environment due to the myriad of business and security requirements of each environment. Therefore, the same deliverable may not be suitable to other environments without modifications as different assurance requirements will usually need to be satisfied.

5.5 Assurance methods applicability to IT security

This clause expands on the assurance definition in clause 3.4. It discusses different aspects of assurance in order to demonstrate how the different aspects of assurance might be applied to IT security.

From the assurance definition in clause 3.4, it is seen that the application of appropriate assurance activities is what establishes confidence that the deliverable satisfies its security objectives. The confidence is realised by reviewing the assurance evidence gained through assessment processes and activities during development, deployment and operation, and through experience in actual usage of the deliverable. Any activities that can reduce the uncertainty by producing evidence attesting to the correctness, effectiveness, and quality of the deliverable's attributes is useful in determining security assurance. Recognising that some types of evidence more clearly establish the claims they support than other types, the key is creating a comprehensive assurance argument that firmly establishes the type and amount of assurance gained from the applied assurance methods. There are many existing assurance methods with only a small number specific to IT security. However, non-IT security assurance methods may also contain certain assurance properties relevant to IT security assurance. Due to the small number of security specific assurance methods available, it is important to recognise the value of all assurance methods since many non-security assurance methods are used throughout the IT industry. Assurance evidence is frequently in the form of documentation developed during the normal course of IT engineering

activities. Anything that can be used to construct an assurance argument and thereby reduce the uncertainty (risk) associated with a particular deliverable is of considerable importance.

The intent here is to communicate the value of non-IT security assurance methods and not downplay the value of IT security specific assurance methods. The latter is clearly preferable; however, some assurance can be obtained from many sources and should not be discounted simply because it does not come from a recognised security assurance method. Having said this, it is very important to recognise the source of the evidence and take that into account when developing the assurance argument. Furthermore, one must be familiar with their security and assurance requirements and understand the value of the evidence and its source to ensure that it satisfies their needs.

For example, while ISO 9000 is a quality assurance standard originally made for manufacturing organisations, it also contains process assurance properties applicable to software, and as such to IT security software products and systems. By contrast, the SSE-CMM is a security assurance method although not a traditional assurance method. This method produces assurance evidence by assessing the organisation's security engineering processes and not the deliverable directly.

Certain assurance methods specifically focus on defining consistent and complete sets of security features, which often reflect a standardised threat scenario or good practices. Different assurance methods may have some components or aspects of assurance in common.

All these factors will have an impact on the assurance framework, and in particular on the definition of metrics. The relationship between assurance methods will take account of these factors.

5.6 Assurance schemes

A specific assurance method that may be implemented in a way that emphasises the context within which the method is executed is called an assurance scheme. Recognised facilities and assessors might ensure a higher degree of assurance gained by using the respective assurance method. Such an assurance scheme may also provide a basis for acceptance of results or verdicts achieved by the assurance method in a broader audience.

5.7 Quantifying assurance risk and mechanism strength

Assurance does not "add" any safeguards or services to the deliverable. Thus it is sometimes difficult for non-security personnel to understand what benefit they are receiving from the investment of resources in assurance. For example, with respect to an IT security product, it has been argued that assurance contributes to the "strength" of a security mechanism; however, the assurance actually contributes to the confidence that one has in the mechanism strength by reducing the uncertainty (or probability) of a threat occurrence causing a security breach. For example, Two-Factor authentication is often mistaken as having more assurance than a simple password mechanism, where in reality it is only a stronger authentication mechanism. Two-Factor authentication is a stronger mechanism since it verifies two user attributes versus one attribute in a password mechanism. This in itself does not offer assurance since it is the assurance activities in the development of the mechanism that contributes to the assurance of the mechanism.

It is important to understand that assurance does not automatically imply good security: only that it meets its security objectives (security policy). In other words, the assurance provides confidence that the deliverable enforces its security objectives without examining if the security objectives appropriately address the risks and threats. For example, while a high assurance IT product can be trusted to meet its security objectives, it depends on the nature of these objectives whether or not the product behaves in a secure manner. In contrast, a low assurance product with more appropriate objectives may actually be more secure.

5.8 Assurance reduces security risk

Assurance contributes to a reduction of risk, in-so-much-as assurance reduces the uncertainty associated with vulnerabilities of the deliverable, and thus the potential vulnerability is reduced leading to a reduction in the overall risk associated with the deliverable. As discussed in the previous clause, assurance does not add any additional controls to counter risks related to security, rather the assurance activities attempt to substantiate that the deliverable satisfies its security objectives. This involves the production of assurance relevant evidence and rationale to provide the confidence that the controls implemented will reduce the anticipated risk.

5.9 Quantifying assurance

Direct qualification or valuation of the contribution of assurance or increased assurance to the organization is not easy to achieve. However, increased assurance of a security control does reduce the uncertainty associated with the risk that the control is implemented to address. Thus the value of the assurance in this case can be inferred from a reduction in the uncertainty associated with the risk. Relating assurance to the uncertainty of a risk, or its constituent parts, facilitates assurance measurements, as the uncertainty risk occurrence is easier to quantify than assurance. Assurance measurements could be made indirectly by measuring the probability of the risk occurrence and then adjusted, as it is inversely proportional to assurance.

5.10 Stakeholders

Assurance may be sought by the stakeholders of a deliverable who are the ones having assets at risk through the deliverable. Therefore, the determination of an acceptable assurance method and level of assurance may be required/and or influenced by the stakeholders some of whom are listed below:

- a) standard bodies;
- b) national and international laws and regulations;
- c) specific communities (such as government or the banking industry);
- d) authorised units within an organisation;
- e) policy (security, personnel, procurement, marketing, certificate policy, etc.) owners;
- f) system owners;
- g) system accreditors;
- h) end users; and
- i) the general public.

5.11 Assurance authority

The Assurance Authority is a person (or body) responsible for decisions pertaining to the deliverable at a specific stage of its lifecycle. Given that there are several stages within a deliverable's lifecycle and several stakeholders, there will be several Assurance Authorities, each with their vested interest and specific responsibilities. For example, during the development phase, the Assurance Authority may be a security engineer in the vendor organisation responsible for ensuring the appropriate assurance is built in to the IT product. Simultaneously, the client organisation may have their own Assurance Authority responsible for ensuring their assurance requirements are addressed by the vendor organisation. Still, another Assurance Authority may exist in the evaluation organisation responsible for ensuring the product satisfies the assurance scheme. Here we see three Assurance Authorities each responsible for a particular stage of the deliverable and from different perspectives. Furthermore, an Assurance Authority may be responsible for multiple stages. Such would be the case if the client Assurance Authority in the example above, would also be responsible for accepting the certification report submitted by the Certifier.

Assurance Authorities are applicable to all types of security deliverables regardless if it is a product, system, service, process, personnel, etc. The Assurance Authority is responsible for the assurance decisions surrounding the deliverable with respect to the organisation's objectives.

Depending on the organisation and their responsibilities, the Assurance Authority will have any number of responsibilities. Some of their tasks may include selecting the appropriate assurance method and identifying the required amount and type of assurance required to satisfy their specific requirements. The assurance authority also has the responsibility of liaising with other assurance organisations such as the assurance assessment organisation with concerns regarding the IT security evaluation scheme if for example ISO 15408 and its corresponding scheme were being used.

Within certain organisations, in particular within government and military organisations, assurance may be regulated, limiting the choices and at the same time, the risk to the Assurance Authority. Organisations may designate different roles as the Assurance Authority and the duties may differ according to their unique operating models; however, the assurance authority will still be responsible for the required duties. In small organisations, an employee would typically have other duties in addition to being the Assurance Authority where larger organizations

may have a dedicated employee assume the role of the Assurance Authority. Larger organisations would usually designate a senior employee as the Assurance Authority to be accountable for the implementation of an assurance method and acceptance of the assurance results.

Depending on the organisation, the person responsible for final acceptance of the assurance results may also be accountable for the operation of the deliverable (i.e. putting the system into operation or accepting the service delivered). Therefore, the Assurance Authority will often have to determine an appropriate balance between the extent and depth to which assurance is performed, and thereby the cost and time frame of the related assessment activities.

6 Selecting security assurance

Selecting a security assurance method and the appropriate amount of assurance is a decision that should be based on the organisational security assurance policy, business requirements, and type of deliverable (i.e. product, process, environment, system, service or personnel).. For example, some assurance methods are only applicable to processes (i.e. SSE-CMM) and products (i.e. ISO/IEC 15408).

The selected assurance method should be compatible with the organisation's environment and be capable of examining the desired attributes and life cycle stages of the deliverable. The assurance method selection must take into account the available resources (time, personnel, budget, etc.) to ensure that the resources expended are reasonable for the type and amount of assurance obtained. For example, adding a fifty thousand dollar safeguard to a low assurance deliverable would be unreasonable. Similarly, there is no need to select an evaluation assurance method (i.e. TCSEC, ITSEC, CTCPEC, ISO/IEC 15408) when a shorter assurance method would be acceptable (assuming that an evaluation assurance method is not mandated) and save months off the schedule¹. For organisations (i.e. government departments) that are required to choose vendors who have developed evaluated IT security products, and use IT security evaluated products to gain assurance, there may be little requirement for decision thus eliminating most or all of the expense of resources for consideration of options.

For example, a private organisation could use the SSE-CMM assurance method to establish assurance of their corporate website to prevent unauthorised persons from accessing the private part. This would require an assessment of the processes surrounding the development, deployment, and operation of the website including the processes to implement the security and operational policies. Based on the findings, an assurance argument would be produced along with a SSE-CMM maturity level of the organisation. This assurance method should suffice, as the Assurance Authority only needed to address their internal security assurance policy. A second example is of a government department that used the ISO/IEC 15408 assurance method to establish high assurance because it was required to use this particular assurance method and approach to meet specific government security requirements. This example demonstrates the latitude that the Assurance Authority has depending on the organisation and their security assurance policies. No statement is made regarding which assurance method is better or provides more assurance. Where existing policy or regulation does not prescribe a particular assurance method and assurance level, the selection of an assurance method and assurance level has to be selected in fulfilment of the assurance requirements which correspond to the security requirements as a function of the security objectives. However, it is possible that security risk management may indicate situations where greater assurance is required, in-so-much-as if security risk management is having to address high levels of uncertainty, then increased assurance can contribute to a reduction in overall uncertainty, and thus a net reduction in security risk. In these situations increased assurance is indicated.

Note that even when an assurance method is mandated, there may be some options available, such as:

- a) what to assure;
- b) how much assurance;
- c) which evaluation lab to use; and
- d) which certification and accreditation services to use.

¹ These are simplistic examples to demonstrate a point and not to imply actual dollar amounts or time frames with respect to a particular assurance method.

There are many different assurance approaches and methods available with few assurance methods being widely accepted or regulated. Guidance is therefore required to assist stakeholder(s) in selecting and applying an assurance method.

6.1 Assurance requirements specification

Prior to choosing and/or performing assurance methods, the assurance requirements have to be specified. Various methods are available to arrive at these specifications. Generally a TRA and organisational security assurance requirements will aid in the selection of the assurance method. Requirements may also include regional and business aspects such as when a customer requires a specific assurance approach such as ISO/IEC 15408 to satisfy internal or procurement requirements.

To address organisation or market requirements, the assurance requirements specification may include recognition and acceptance of the assurance method or assurance scheme, mutual recognition, and minimal assurance level.

Examples of assurance requirements include constraints on the rigour of the development process and/or requirements to search for and analyse the impact of potential security vulnerabilities.

When the deliverable contains security mechanisms such as a password or hash function, the assurance requirements may specify a minimum strength level consistent with the security objectives be claimed.

Assurance specifications should address all organisational requirements and contain all mutually supportive assurance components such as correctness assurance and effectiveness assurance. Furthermore, acceptable assurance approaches and methods need to be detailed as well as specifying the Assurance Authorities, their responsibilities, and communication channels.

6.2 Economical aspects

Assurance generally is resource intensive causing cost and delays. Furthermore, assurance is geared to prevent losses rather than providing revenue or profit. Therefore its return on investment is not measurable but hypothetical similar to insured losses. Even when a supplier amortises assurance over a number of IT security products, it may take several years to recoup the investment depending on the assurance method and desired assurance level. The benefit an organisation receives from the investment of resources in assurance will not be obvious to people not familiar with security issues and therefore it may require extensive justification and must be well presented to gain management approval.

Different forms of assurance target different audiences. For example, the assurance provided by a warranty is of little value to the user when the system is down, but it is of value to the manager in defraying the cost of a delay. In a similar manner, the assurance provided by a guarantee of technical support if the system fails is of little value while the system is functioning, but will be of value to operations if the system malfunctions.

All forms of assurance provide different benefits to different parts of the organisation, not assessing these different benefits devalues the assurance being obtained.

What assurance actually does is reduce uncertainty, at least with respect to vulnerabilities associated with the IT security product or service. Uncertainty is associated with all factors used in the assessment of security risk. Thus reduction of uncertainty facilitates focussing on the aspects that are truly of greatest risk to the organisation. This represents a measurable benefit to the organisation and a beneficial investment of resources.

6.3 Organisational policies

It is important to recognise the security environment, and in particular to understand that the assurance requirements reflect the organisation's culture and business requirements. An understanding of the organisational requirements is necessary to decide whether a particular assurance method is acceptable and/or how much assurance is sufficient. The organisation policy should specify the following:

- a) how assurance requirements are to be determined;
- b) the circumstances under which a deliverable should be certified against a particular standard;
- c) standards against which deliverables are to be certified;

- d) the degree of assurance required in certification processes in nominated circumstances;
- e) responsibilities for an assurance authority; and
- j) the circumstances where accreditation of deliverables is necessary.

For example, a government organisation may decide to specify and control the assurance process to for their specific environments. They may develop all aspects of the process such as the assurance methods, criteria (a standard), guidance on using the standard, performing assessment, and even the level of assurance required. However, the assurance authority for the accreditation will still have to make the final decision of acceptable assurance and be held accountable for resources and schedule. By contrast, a private organisation may choose to select a de-facto assurance method for their in-house development if their Assurance Authority is not required to satisfy external influences. The organisational policies are essential to specify what is required and also referenced when verifying if the security safeguards and assurance are appropriate to the organisation.

6.4 Security Assurance Model

To address the composition of multiple assurance methods for a specific deliverable, it is best to construct a security assurance model to show how the different types of assurance are intended to work together to contribute to the total assurance associated with the deliverable. The security assurance model for a deliverable can then be composed of different constituent assurance models each corresponding to a specific assurance approach (i.e. evaluation assurance, process assurance, development assurance). In this way, the deliverable assurance model by being a compound of several distinct assurance models, will address how these assurance models are combined regardless of the assurance phase to which they have been applied. Further, it may be that some security assurance associated with the deliverable is not directly intended for the next recipient of the deliverable, but is in fact intended for the final recipient. The model can show this clearly, and help to ensure that the final recipient receives a clear picture of the associated security assurance.

Each assurance model can then specify the type and quantity of assurance for a specific life cycle stage of the deliverable to facilitate comparison. The deliverable assurance model would glue the distinct models together by describing the trade-offs and providing the rationalisation to describe the resultant assurance for the deliverable.

6.5 Technical aspects

Many assurance methods are available to choose from and offer potential for optimisation in terms of resources and time frame. The assurance method should be selected from the following list as is appropriate for the deliverable or its attribute(s) to be assessed:

- a) assurance methods applicable exclusively to specific IT deliverables such as IT security hardware or software products, systems, networks, personnel, services, etc;
- b) assurance methods specific to a life cycle process; or
- c) assurance methods based on experience and actual usage.

Applying an assurance method to assess the assurance of a deliverable may yield different types or quantities (levels) of assurance due to:

- a) deficiencies or characteristics of the deliverable;
- b) the size and complexity of the deliverable;
- c) differences in the applied assurance methods;
- d) applying an assurance method with a limited rigour or effort;
- e) the nature of the security objectives being met;
- f) the specific environment;
- g) the specific IT life cycle stage; or
- h) the combination with other methods.

Incremental assurance of a deliverable may be gained from:

- a) increased knowledge of its pre-existing IT security capability; and/or

- b) improved capability of its IT security mechanisms.

Each assurance method has its own application as well as pros and cons, depending on individual security requirements. It is necessary to understand how each assurance method establishes assurance in order to decide if a particular assurance method will satisfy the assurance requirements.

For example, when a system is deployed, consisting of a set of products (whose level of assurance may or may not be known or accepted due to the assurance method used) the recognisable level of assurance is usually determined by the system certification prior to operation.

Technical considerations impact the decision, as some assurance methods may be better for simple versus complex deliverables. For example, it is usually easier to verify a deliverable with minimal security functionality (i.e. thousands of lines of code) and achieve a high assurance result than a deliverable with extensive security functionality composed of millions of lines of code.

The type and level of assurance possible from a particular assurance method is determined by the assurance method's features, i.e. the particular life cycle stages assessed, and the security element assessed.

6.6 Optimisation considerations

Deciding on the assurance methods and amount of assurance required is not an exact science and requires the assurance authority to determine the correct mix of assurance methods and the appropriate assurance to satisfy the organisation's requirements. To that end, the IT system and assurance method attributes must be taken into account.

If several assurance methods are applied, more weight may be given to the assurance results derived from the last assurance method applied just prior to final acceptance of the deliverable. Therefore, the assurance authority for the last assurance method must weigh the current assurance results and may have to make a judgement call if any previous assurance results are not satisfactory. Furthermore, as authority for the last assurance activity, they will ultimately be accountable for the operation of the deliverable.

Assurance may be derived incrementally through the vendor of an IT security product, systems integrator or service provider in some form of guarantee or warranty of performance of the product or service.

With respect to deliverables with adequate assurance it should be noted that in particular the integration of one or more deliverables into their final target environment generally has a negative impact on the resulting security assurance level. Consequently, additional assurance may be required.

7 Framework

7.1 Assurance approach

Assurance methods can be categorised into three high-level assurance approaches:

- a) assessment of the deliverable, i.e., through evaluation and testing;
- b) assessment of the processes used to develop or produce the deliverable; and
- c) assessment of the environment, such as personnel and facilities.

Assessment of a deliverable involves an examination of the deliverable (product, system, service, etc.). In this case, these assurance methods examine the deliverable and its associated security design documentation independent of the development processes.

Assessment of a process involves an examination of the organisational processes used in the production and operation of the deliverable throughout its life cycle (development, deployment, delivery, testing, maintenance, disposal, etc.). Assurance is gained through the inference that the processes implemented by people affect the quality of the development and implementation of the deliverable and therefore yield security assurance when applied to IT security deliverables.

Assessment of the environment involves an examination of the environmental factors that contribute to the quality of the processes and the production of the deliverable (It does not examine a deliverable or process directly). These factors include personnel and physical facilities (development, production, delivery, operation, etc.).

Note: By contrast, assurance approaches such as evaluation assurance obtained from applying evaluation criteria such as ISO/IEC 15408 assess the TOE directly over a subset of its life cycle and offer a unique blend of assurance.

Examples: ISO/IEC 15408 examines the TOE directly and produces evaluation assurance which is an agreed upon set of development, assessment, and testing assurances whereas ISO 9001 focuses on examining the manufacturing processes.

7.2 Assurance Methods

This Technical Report covers a broad range of existing methods to obtain assurance. This includes official national or international standards, de-facto standards, and other accepted methods which have or utilize a specified and systematic method.

An example of a de-facto standard is the SSE-CMM Appraisal Method (SSAM), which is a well-documented assurance method; however, it is not a national or international standard. An example of another de-facto standard is the Trusted Product Evaluation Process (TPEP) assurance method. Although, the TPEP is an acceptable standard used successfully by some governments for the evaluation of IT security products, it is an undocumented proprietary evaluation method.

Assurance methods produce specific types of assurance depending on their technical and life cycle focus, which facilitates categorizing them according to assurance approaches. Table 1 lists some of the more widely known assurance methods according to their focus and approach. Later parts of this Technical Report will contain a more comprehensive listing of assurance methods and address technical details and comparisons.

Assurance Approach	Assurance Focus	Assurance Method Examples (includes the respective criteria or model)
Process	Quality and Development process	<ul style="list-style-type: none"> • ISO 9000 • ISO/IEC 15504 • HCD • SSAM (SSE-CMM)
Deliverable, Process, Environment	Branding – Recognition of company to produce quality deliverables (based on historical relationship or data)	<ul style="list-style-type: none"> • Developer's Pedigree
Deliverable	Insurance (supported by manufacturer's promise to correct flaw in deliverable)	<ul style="list-style-type: none"> • Warranty Assurance
Deliverable	Self Declaration	<ul style="list-style-type: none"> • Supplier's declaration
Environment	Personnel expertise and knowledge	<ul style="list-style-type: none"> • Professional certification & licencing • Secure facilities
Deliverable	Direct Assessment of deliverable	<ul style="list-style-type: none"> • CEM (ISO/IEC 18045) • ITSEM (ITSEC) • TPEP (TCSEC) • TPEP (CTCPEC) • Rating Maintenance (RAMP) • Rating Maintenance (RM) • Certification and Accreditation Assurance • ISO 14598 Software product evaluation
Deliverable, Process, Environment	Security Management	<ul style="list-style-type: none"> • BSI Code of practice for information security management (ISO/IEC 17799) • Information security management systems - specification and guidance for use (BS 7799.2) • GISA/BSI Base Line Protection Manual • ISO/IEC 13335

Table 1: Examples for assurance methods

7.3 Assurance and life cycle aspects

As human error, equipment failures, new vulnerabilities, and threats can occur in any life cycle stage of the deliverable, appropriate assurance is required at each of the deliverable life cycle stages (i.e. concept, development, integration, deployment, operation, and disposal). Therefore, the assurance methods must be appropriate for the specific stage.

Functional deficiencies, change in requirements, and new vulnerabilities will affect assurance and require earlier life cycle stages to be entered again. Therefore, life cycle models must allow for a repetitive, overlapping or iterative relationship between the stages.

A sample life cycle model (Figure 1) is used to demonstrate relation of the assurance methods to a deliverable's life cycle stage. The sample life cycle model contains four basic stages general enough to be mapped to any specific life cycle model.

Assurance methods may be specific to a particular stage (i.e. System Accreditation) or apply to several life cycle stages of a deliverable as can be seen by examining ISO 9000, ISO/IEC 15408, and the SSE-CMM.

To achieve the resultant assurance, the assurance gained at each stage must be carried forward to the next stage where it will be factored into the assurance of that stage. This method of incrementing the assurance continues to the last stage of the life cycle model, which is the *operation stage* in the sample model shown in Figure 1.

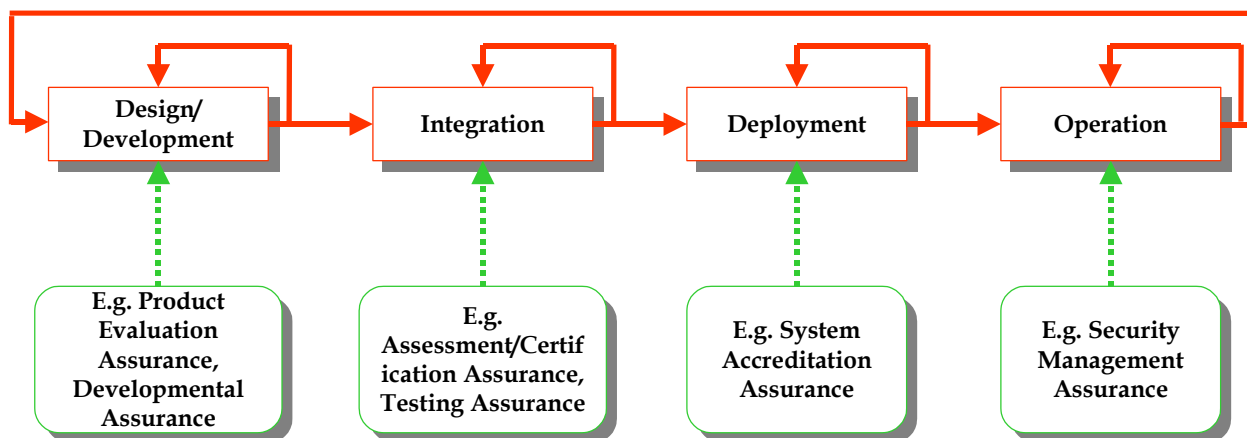


Figure 1: Assurance methods in relationship to a simplified model life cycle stages

NOTE: The life cycle model shown in Figure 1 is an example to demonstrate a model compatible with other life cycle models and frameworks to facilitate the analysis of assurance methods within this Technical Report. It is not intended to prescribe or recommend a particular life cycle model.

7.4 Correctness versus effectiveness assurance

Correctness assurance refers to the assessment of the deliverable to verify the correct implementation according to the design. In contrast, effectiveness refers to the suitability of the deliverable’s security functions to counter the perceived or identified threats. The next paragraph demonstrates that effectiveness and correctness assurance are both important assurance properties and neither can stand alone as they each address important aspects of the deliverable.

If the deliverable’s security functionality addresses the potential threats, but the functionality has not been analysed to establish its correct design and implementation, then one cannot have confidence that the deliverable will withstand an attack. In this example, it is seen that the effectiveness assurance has been established but the correctness assurance has not due to the lack of verified security functionality. Similarly, if analysis has found the design and implementation of the deliverable’s security functionality as correct; however, the design does not contain the appropriate functionality to address the probable threats, then one can not have confidence that the deliverable will withstand an attack by those threats. In this example, although the correctness assurance is there, it lacks effectiveness assurance due to the implementation of ineffective security functionality against the probable threats. In order to achieve comprehensive assurance, the deliverable must be assessed to ensure the correct design, implementation, and operation (correctness element) and the deliverable must provide the appropriate security functionality to counter the identified threats (effectiveness element).

7.5 Categorisation of assurance methods

Assurance methods can be classified according to the three assurance approach categories as described earlier in Section 7.1. Within each assurance approach, an assurance method may focus on a specific life cycle stage or several depending on the assurance method characteristics.

Depending on the type of assurance method, the assurance gained is based on the aspect assessed and the life cycle stage. For example, evaluation assurance methods produce assurance related to parts of the design, development, and operation stages; developmental assurance methods yield assurance related specifically to the development stage; and testing assurance produces assurance related specifically to testing aspects in several stages depending on the assurance method.

Figure 2 demonstrates that assurance approaches may apply to more than one assurance stage. Part 2 and Part 3 of this Technical Report elaborates on the assurance approaches and Part 2 provides specific examples of assurance methods.

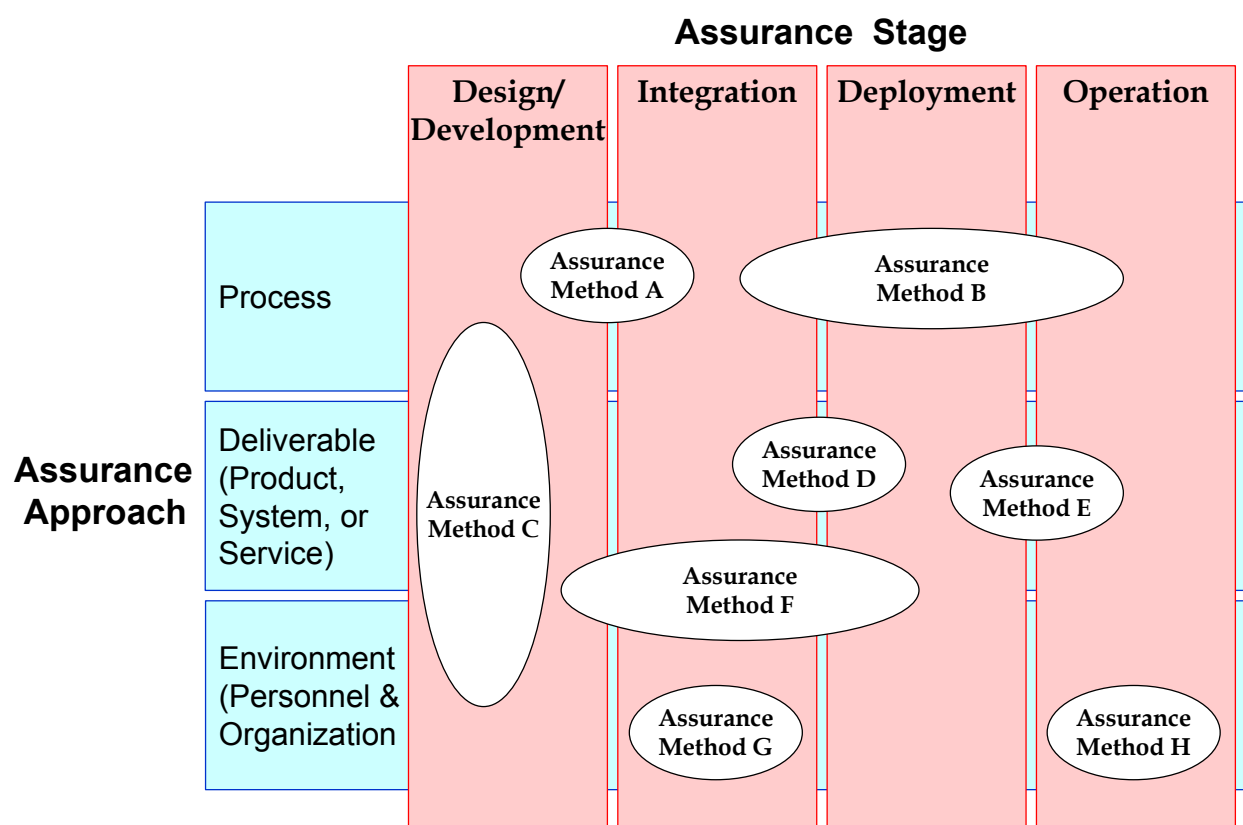


Figure 2: Categorisation of existing assurance methods

Assurance methods from different assurance approach categories yield different assurance due to their different focus. However, even within assurance approach categories, assurance methods will yield different assurance due to the deliverable's (IT component or service) aspect examined.

Assurance approaches yield different assurance due to the deliverable (IT component or service) aspect examined. Some approaches examine different stages of the deliverable life cycle while others examine the processes that produce the deliverable (indirect examination of the deliverable). Assurance approaches include facility, development, analysis, testing, flaw remediation, operational, warranties, personnel, etc. These assurance approaches can be further broken down; for example, testing assurance approach includes general testing and strict conformance testing assurance methods.

Using this framework, specific assurance methods of the same category may then be checked for redundant or synergetic properties. Assurance methods of different categories may be recognised for their complementary properties. Some methods may show coverage of several categories, entirely or partially, while others may only partially fill categories.

7.6 Composite assurance

The resultant assurance obtained for a deliverable is usually a blend or composition of different assurance methods applied at various stages throughout the deliverable's life cycle. The assurance may be indicated as a rating, type, or other measure as appropriate.

Composition of assurance is difficult to perform as very few assurance methods are standardized, and scales or measurement of assurance across assurance methods do not exist. At the moment, composition of assurance is only possible by forming an assurance argument and subjective reasoning by experienced IT security professionals. Moreover, the assurance authority ultimately determines the acceptable assurance.

Currently, composite assurance is the result of building the assurance incrementally, throughout the life cycle, by the application of various assurance methods. The following examples demonstrate possible assurance scenarios and the questions they openly create:

- 1) The assurance methods included one that examined the processes to produce the deliverable and another that examined the deliverable directly at different points in the same developmental life cycle stage.
- 2) Two assurance methods applied from the same assurance approach at different life cycle stages of the deliverable.
- 3) A complex IT system (for a specific operational environment) composed of numerous IT products and services, had various degrees of assurance established through evaluation, warranty, certification, and accreditation assurance methods.

Example 1 demonstrates the simplest problem where the composite assurance is determined by combining the different assurance from the respective methods.

Example 2 seems simpler since the assurance methods are of the same approach and even straight forward if the assurance methods are the same, it becomes more difficult as the question arises about the significance of the assurance approach occurring in a later life cycle stage of the deliverable.

Example 3 is even more difficult as several different assurance methods are applied at different life cycle stages and the accreditation assurance method forms the basis for the decision to go live with the system. Even though the system certification will address early assurance evidence, there may be no requirement for a particular assurance approach at that point. This suggests that there is more weight applied to assurance methods applied at later life cycle stages.

It is worth noting that many standards based approaches to process assurance are now moving towards adoption of the same underlying model of continuous process improvement. An example is the PDCA (Plan, Do, Check, Act) model used by both ISO 9001 for quality and BS 7799 for information Security Management.

It is the objective of this Technical Report to shed more light on whether or not an assurance approach applied in a later life cycle stage has more relevance or more assurance. Later parts of this Technical Report will address these and other questions.

7.7 Assurance rating

The analysis in Part 3 of this Technical Report focuses on assurance metrics as a way of categorising assurance methods and measuring the amount of assurance obtained by the application of an assurance method (i.e. developmental assurance levels). Establishing assurance metrics also facilitates describing the relationships between methods.

The following are some of the issues addressed in Part 3 of this Technical Report as they are related to the analysis and rating of assurance methods:

- a) Comparing different assurance methods;
- b) Quantifying assurance methods;
- c) Selection of the appropriate assurance methods;
- d) Relationship between different assurance methods;
- e) Determining which assurance methods can be combined;
- f) Determining when and how assurance methods can be combined;
- g) Determining if and how the order of assurance methods performed impact the overall assurance; and
- h) Determining the technical issues to ensure and enforce the validity of assurance results (and conditions) during the deliverable's life cycle (i.e. operations and maintenance) where one or more assurance approaches are used.

8 Bibliography

Aaron Cohen, *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. Common Criteria Project: Assurance Approaches Working Group (report: AAWG-97/037, annex A: AAWG-97/038), August 1997.

Abadi, Burrows, Lampson, Plotkin: *A calculus for access control in distributed systems*, Digital Equipment Corporation, Palo Alto, 1991.

British Standard BS 7799-2:2002 Information Security management systems – specification and guidance for use, British Standards Institution, 2002. Available from Internet: <<http://bsonline.techindex.co.uk>>.

CMM® (model): Capability Maturity Model for Software, Version 1.1, February 1993.

CMM® (method): Key Practices of the Capability Maturity Model, Version 1.1, February 1993.

Gasser, Goldstein, Kaufmann, Lampson: *The Digital distributed security architecture*, Proc. of National Computer Security Conference, USA, 1989.

Korea Information Security Evaluation Criteria, Ministry of Information and Communication, Republic of Korea, February 1998.

Korea Information Security Product Evaluation Program, Ministry of Information and Communication, Republic of Korea, February 1998.

The application of quality assurance procedures to security evaluation, NPL Report DITC 236/95, UK, July 1995.

SCT, *Strict Conformance Testing*, NPL Report, UK, March 1997.

SE-CMM® (model). *A Systems Engineering Capability Maturity Model*, Version 1.1. Carnegie Mellon University (CMU/SEI-95-MM-003), November 1995.

SE-CMM® (method). *A Description of the Systems Engineering Capability Maturity Model Appraisal Method*, Version 1.1. Carnegie Mellon University (CMU/SEI-96-HB-004), March 1996.

Strack/Lam: *Context-dependent access control in distributed systems*, Proc. of IFIP/SEC'93, Toronto 1993 (IFIP transactions A-37, North-Holland, 1993).

Trusted Capability Maturity Model, Version 2.0. National Security Agency (NSA), June 20, 1996.

UK Certificate Maintenance Scheme, Part II Impact Analysis And Evaluation Methodology, UKSP 16, Issue 1.0, UK IT Security Evaluation & Certification Scheme Certification Body", 31 July 1996.

X/Open CAE Specification Baseline Security Services (XBSS), Document Number C529, UK: X/Open Company, Ltd., December 1995.