TECHNICAL REPORT

ISO/IEC TR 15443-2

First edition
2005-09-01

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

Part 2: Assurance methods

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

Partie 2: Méthodes d'assurance

Reference number
ISO/IEC TR 15443-2:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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

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

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

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 15443-2, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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

— *Part 1: Overview and framework*

— *Part 2: Assurance methods*

The following part is under preparation:

— *Part 3: Analysis of assurance methods*

Introduction

The objective of this part of ISO/IEC TR 15443 is to describe a variety of assurance methods and approaches that may be applicable to ICT security, as proposed or used by various types of organizations whether they are generally acknowledged, de-facto approved or standardized, and to relate them to the assurance model of ISO/IEC TR 15443-1. The emphasis is to identify qualitative properties of the assurance methods that contribute to assurance, and where possible, to define assurance ratings. This material is catering to an ICT Security professional for the understanding of how to obtain assurance in a given life cycle stage of product or service.

This part of ISO/IEC TR 15443 gives for each item of the collection its aim, description and reference. Each item of collection of assurance methods is then placed within the framework defined in ISO/IEC TR 15443-1.

The assurance methods listed in this part of ISO/IEC TR 15443 are considered to comprise generally known items at the time of its writing. New methods may appear, and enhancements or other modification to the existing ones may occur.

Developers, evaluators, quality managers and acquirers may select assurance methods from this part of ISO/IEC TR 15443 for assurance of the ICT security software and systems, defining assurance requirements, evaluating products, measuring security aspects and other purposes. In complement, they may also use assurance methods which are not included here. This part of ISO/IEC TR 15443 is applicable to the assurance of security aspects, although many of the methods may also be applicable for the assurance of other critical aspects of software and systems.

This part of ISO/IEC TR 15443 is intended to be used together with ISO/IEC TR 15443-1.

This part of ISO/IEC TR 15443 will analyze assurance methods that may not be unique to ICT security; however, guidance given in this part of ISO/IEC TR 15443 will be limited to ICT security requirements. Similarly, additional terms and concepts defined in other International standardization 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 ICT security and is not intended for general quality management and assessment, or ICT conformity.

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

Part 2: Assurance methods

1 Scope

1.1 Purpose

This part of ISO/IEC TR 15443 provides a collection of assurance methods including those not unique to ICT security as long as they contribute to overall ICT security. It gives an overview as to their aim and describes their features, reference and standardization aspects.

In principle, the resultant ICT security assurance is the assurance of the product, system or service in operation. The resultant assurance is therefore the sum of the assurance increments obtained by each of the assurance methods applied to the product, system or service during its life cycle stages. The large number of available assurance methods makes guidance necessary as to which method to apply to a given ICT field to gain recognized assurance.

Each item of the collection presented in this part of ISO/IEC TR 15443 is classified in an overview fashion using the basic assurance concepts and terms developed in ISO/IEC TR 15443-1.

Using this categorization, this part of ISO/IEC TR 15443 guides the ICT professional in the selection, and possible combination, of the assurance method(s) suitable for a given ICT security product, system, or service and its specific environment.

1.2 Field of Application

This part of ISO/IEC TR 15443 gives guidance in a summary and overview fashion. It is suitable to obtain from the presented collection a reduced set of applicable methods to choose from, by way of exclusion of inappropriate methods.

The summaries are informative to provide the basics to facilitate the understanding of the analysis without requiring the source standards.

Intended users of this part of ISO/IEC TR 15443 include the following:

1. acquirer (an individual or organization that acquires or procures a system, software product or software service from a supplier);

2. evaluator (an individual or organization that performs an evaluation; an evaluator may, for example, be a testing laboratory, the quality department of a software development organization, a government organization or a user);

3. developer (an individual or organization that performs development activities, including requirements analysis, design, and testing through acceptance during the software life cycle process);

4. maintainer (an individual or organization that performs maintenance activities);

5. supplier (an individual or organization that enters into a contract with the acquirer for the supply of a system, software product or software service under the terms of the contract) when validating software quality at qualification test;

6. user (an individual or organization that uses the software product to perform a specific function) when evaluating quality of software product at acceptance test;

7. security officer or department (an individual or organization that perform a systematic examination of the software product or software services) when evaluating software quality at qualification test.

1.3 Limitations

This part of ISO/IEC TR 15443 gives guidance in an overview fashion only. ISO/IEC TR 15443-3 provides guidance to refine this choice for better resolution of assurance requirements enabling a review of their comparable and synergetic properties.

The regulatory infrastructure to support verification of an assurance approach and the personnel to perform verification is outside the scope of this part of ISO/IEC TR 15443.

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, *Quality management systems — Fundamentals and vocabulary*

ISO 9001, *Quality management systems — Requirements*

ISO/IEC 9126-1, *Software engineering — Product quality — Part 1: Quality model*

ISO/IEC 12207, *Information technology — Software life cycle processes*

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

ISO/IEC TR 13335-2, *Information technology — Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*

ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT Security*

ISO/IEC TR 13335-4, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

ISO/IEC TR 13335-5, *Information technology — Guidelines for the management of IT Security — Part 5: Management guidance on network security*

ISO/IEC 14598-1, *Information technology — Software product evaluation — Part 1: General overview*

ISO/IEC 15939, *Software engineering — Software measurement process*

ISO/IEC 15288, *Systems engineering — System life cycle processes*

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

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

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

ISO/IEC 15504-1, *Information technology — Process assessment — Part 1: Concepts and vocabulary*

ISO/IEC 15504-2, *Information technology — Process assessment — Part 2: Performing and assessment*

ISO/IEC 15504-3, *Information technology — Process assessment — Part 3: Guidance on performing an assessment*

ISO/IEC 15504-4, *Information technology — Process assessment — Part 4: Guidance on use for process improvement and process capability determination*

ISO/IEC TR 15504-5, *Information technology — Software Process Assessment — Part 5: An assessment model and indicator guidance*

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

ISO/IEC 21827, *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)*

ISO/IEC 90003, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

3 Terms, definitions and abbreviated terms

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

4 Overview and Presentation of Methods

Part 1 of this technical report provides a framework for the categorization of existing assurance methods. This clause lists and presents the available assurance methods that are of interest and directly related to the field of ICT security. It classifies these methods according to the framework:

— according to the different assurance phases - describing its lifecycle aspect: Design, Implementation, Integration, Verification, Deployment, Transition, or Operation;

— according to the different assurance approach: Product, Process or Environment.

As stated in Part 1 of this technical report an assurance method may comprise a combination of assurance approach and assurance phase.

For additional user guidance the overview table in sub-clause 5.4 presents this categorization along with a mention of:

— the ICT security relevance of the individual methods and

— the actuality of the individual methods.

5 Assurance Life Cycle Phase and Legend

The overview table in sub-clause 5.4 lists the later presented methods classified according to their Life Cycle Phase. The subclause title of each individual listing repeats this classification.

The different Life Cycle Phases of interest are graphically represented by four columns of the table. For this purpose and approaching the concepts of ISO/IEC 15288 and ISO 9000, the Technical Life Cycle Processes are grouped into four stages, one for each column and abbreviated by one letter as follows:

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

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

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

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

Note 1: A given assurance method may cover one life cycle phase only remotely. In this case, this phase is not flagged in the graphical presentation.

Note 2: The life cycle processes D-I-T-O are those applicable to a specific ICT system and its components, i.e., hardware, software. The development and improvement of the life cycle processes are a second dimension which may be graphically represented but presently is not shown. In ICT security this dimension is particularly important for the security management methods applied to ICT systems in the operations phase, such as ISO/IEC 17799 and BS 7799-2. This second dimension essentially comprises process assessment and documentation, development, measurement, improvement and certification. This second dimension is orthogonal to the D-I-T-O dimension.

5.1 Assurance Approach and Legend

The overview table in sub-clause 5.4 lists the later presented methods categorized according to their assurance approach. The subclause title of each individual listing repeats this categorization.

The respective assurance approach categories of the methods are represented symbolically (refer to Table 1):

— 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** ■.

Table 1 — Assurance methods in the framework - Legend

Clause	Assurance --Phase→ --Approach↓	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**

Note 1: As methods may feature a combination of approaches, the symbols may be cumulated; e.g., a method offering both process and environmental assurance will be the letter on a dark field with a dark frame.

Note 2: A given assurance method may cover one approach more or less extensively. This visual overview presentation is not suited to represent the extent of coverage of the various assurance approaches by a given method.

Note 3: A given assurance method may cover one approach only remotely. In this case, this approach is not flagged in the graphical presentation.

5.2 Actuality and Legend

As of the great number of methods the user of This part of ISO/IEC TR 15443 is given some direction as to their status. The overview table in sub-clause 5.4 reflects this status as follows:

— the methods presently in relatively wide-spread use and active maintenance are represented in the overview table of sub-clause 5.4 in **bold characters**.

— the methods becoming obsolete, superseded, merged or otherwise loosing actuality are represented in the overview table of sub-clause 5.4 in regular slim characters.

Note: This legend is not repeated in the subclause title of the individual listing.

5.3 Security Relevance and Legend

As of the great number of methods the user of This part of ISO/IEC TR 15443 is given some direction as to their ICT security relevance. The overview table in sub-clause 5.4 and the applicable subclause title reflect this status as follows:

— Methods which are specifically oriented towards ICT security have been awarded a "lock" sign (🔒).

5.4 Overview Table

Table 2 presents an overview of the considered assurance methods, together with their classification according to the framework developed in Part 1 of this Technical Report, as explained above.

Table 2 — Assurance methods in the framework - Overview

Clause	Assurance --Phase→ --Approach↓	Design/ Implemen-tation	Integration/ Verification	Deployment/ Transition	Operation
6.1	**ISO/IEC 15408 – Evaluation criteria for IT security**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.2	TCSEC – Trusted Computer System Evaluation Criteria	⇒D⇒	⇒I⇒		⇒O⇒
6.3	ITSEC/ITSEM – Information Technology Security Evaluation Criteria and Methodology	⇒D⇒	⇒I⇒		⇒O⇒
6.4	CTCPEC – Canadian Trusted Product Evaluation Criteria	⇒D⇒	⇒I⇒		
6.5	**KISEC/KISEM – Korea Information Security Evaluation Criteria and Methodology**	⇒D⇒	⇒I⇒		⇒O⇒
6.6	**RAMP – Rating Maintenance Phase**	⇒D⇒	⇒I⇒		⇒O⇒
6.7	**ERM – Evaluation Rating Maintenance (in general)**	⇒D⇒	⇒I⇒		⇒O⇒
6.8	**TTAP – Trust Technology Assessment Program**	⇒D⇒	⇒I⇒		
6.9	**TPEP – Trusted Product Evaluation Program**	⇒D⇒	⇒I⇒		
6.10	**Rational Unified Process® (RUP®)**	⇒D⇒	⇒I⇒	⇒T⇒	
6.11	**ISO/IEC 15288 – System Life Cycle Processes**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.12	**ISO/IEC 12207 – Software Life Cycle Processes**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.13	**V–Model**	⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒
6.14	**ISO/IEC 14598 – Software product evaluation**	⇒D⇒			⇒O⇒
6.15	**X/Open Baseline Security Services**	⇒D⇒			
6.16	**SCT – Strict Conformance Testing**		⇒I⇒		
6.17	**ISO/IEC 21827 – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)**	D	I	T	O
6.18	**TCMM – Trusted Capability Maturity Model**	D	I		
6.19	**CMMI – Capability Maturity Model ® Integration**	D	I	T	O
6.20	**ISO/IEC 15504 – Software Process Assessment**	D	I	T	O
6.21	**CMM – Capability Maturity Model® (for Software)**	D	I		

Table 2 *(continued)*

Clause	Assurance --Phase→ --Approach↓	Design/ Implemen-tation	Integration/ Verification	Deployment/ Transition	Operation
6.22	SE-CMM® – Systems Engineering Capability Maturity Model ®	D	I		
6.23	TSDM – Trusted Software Development Methodology	D	I		
6.24	SdoC – Supplier's declaration of Conformity	D			
6.25	SA-CMM® – Software Acquisition Capability Maturity Model®			T	
6.26	ISO 9000 Series – Quality Management	D	I	T	O
6.27	ISO 13407 – Human Centered Design (HCD)	D			
6.28	Developer's Pedigree (in general)	D			
6.29	ISO/IEC 17025 – Accreditation Assurance	D	I		
6.30	ISO/IEC TR 13335 – Guidelines for the management of IT Security (GMITS) 🔒		I	T	O
6.31	BS 7799-2 – Information security management systems – Specification with guidance for use 🔒				O
6.32	ISO/IEC 17799 – Code of practice for information security management 🔒				O
6.33	FR – Flaw Remediation (in general)				O
6.34	IT Baseline Protection Manual 🔒				⇒O⇒
6.35	Penetration Testing 🔒				⇒O⇒
6.36	Personnel Certification (non security related)				O
6.37	Personnel Certification (security related) 🔒	D	I	T	O

5.5 Presentation Methodology

Clause 6 is intended to provide a review of identified assurance methods. Because many assurance methods contribute to different assurance approaches and assurance, each assurance method shall be presented here with its own way of description and views. No comparing is provided at this stage.

In the subclauses Clause 6 there will be a structured synopsis for each assurance method identified in this technical framework.

The **title** of the method is the a self explanatory name, if possible the full and official name of the assurance method for proper reference, as well as a Mnemonic for its reference when appropriate.

Each synopsis is broken down into:

- **Aim:** Brief characteristic purpose of the method.
- **Description:** Short description of the method.
- **Sources:** Address/Reference to committees and/or organizations involved, documents the describing method and/or standardisation thereof.

6 Assurance Methods

6.1 ISO/IEC 15408 – Evaluation criteria for IT security

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.1.1 Aim

To provide a harmonized framework and detailed evaluation criteria for ICT security evaluation, suitable for both government and general use.

6.1.2 Description

The Common Criteria were developed on behalf of a number of governmental information security agencies as a way of independently assessing the security characteristics of ICT products and systems. The criteria were developed in conjunction with JTC 1 Subcommittee 27, Security Techniques, and published as International Standard ISO/IEC 15408.

The Common Criteria separate consideration of security functionality from security assurance and specify detailed techniques and functions that can aid in the development of confidence that a security product or system meets its security objectives. The specific assurance techniques and functions are defined in ISO/IEC 15408-3, and are primarily, but not exclusively, aimed towards assurance obtained through independent assessment or verification. It is intended that consistent application of the evaluation criteria can be verified through national certification schemes.

Within ISO/IEC 15408-3, assurance techniques are divided into different areas of applicability, called classes. Within each class, different techniques are identified, called families. Each family then identifies one or more levels of rigor by which the technique can be applied, these are called components. Each component specifies the precise actions and evidence elements required.

A number of packages of assurance components that work together in a complementary manner are defined within ISO/IEC 15408-3. These are called Evaluation Assurance Levels (Earls).

A supporting methodology for application of these criteria, the Common Evaluation Methodology, is being developed by the Common Evaluation Methodology Working Group, part of the Common Criteria project.

6.1.3 Sources

Refer to Clause 2: ISO/IEC 15408-1, ; ISO/IEC 15408-2, ; ISO/IEC 15408-3,

Note: ISO/IEC 15408 is a product of the committee:
ISO/IEC JTC 1/SC 27/WG 3 Information technology - Security techniques - Security evaluation criteria

6.2 TCSEC – Trusted Computer System Evaluation Criteria

⇒D⇒	⇒I⇒		⇒O⇒

6.2.1 Aim

To grade or rate the security offered by a computer system product.

6.2.2 Description

The Trusted Computer System Evaluation Criteria (TCSEC) is a collection of criteria that was previously used to grade or rate the security offered by a computer system product. No new evaluations are being conducted using the TCSEC although there are some still ongoing at this time. The TCSEC is sometimes referred to as "the Orange Book" because of its orange cover.

A product is "compliant" with the TCSEC if it has been evaluated by the Trusted Product Evaluation Program (TPEP) or Trust Technology Assessment Program (TTAP) to comply with the requirements of a rated class of TCSEC and if an independent assessment showed the product to have the features and assurances of that class.

A class is the specific collection of requirements in the Trusted Computer System Evaluation Criteria (TCSEC) to which an evaluated system conforms. There are seven classes in the TCSEC A1, B3, B2, B1, C2, C1, and D, in decreasing order of features and assurances. Thus, a system evaluated at class B3 has more security features and/or a higher confidence that the security features work as intended than a system evaluated at class B1. The requirements for a higher class are always a superset of the lower class. Thus a B2 system meets every C2 functional requirement and has a higher level of assurance.

A division is a set of classes (see Question 11) from the Trusted Computer System Evaluation Criteria (TCSEC) (see TCSEC Criteria Concepts FAQ, Question 1). There are 4 divisions A, B, C, and D in decreasing order of assurance and features. Thus, a system evaluated at a class in division B has more security features and/or a higher confidence that the features work as intended than a system evaluated at a class in division C. Although the Computer Security Subsystem Interpretation (CSSI) of the TCSEC specifies criteria for various D ratings, these are not reflected in the TCSEC itself, which has no requirements for D division systems. An unrated system is, by default, division D.

The Requirements for the different classes are:

Class D: Minimal Protection - is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

Class C1: Discretionary Security Protection - The Trusted Computing Base (TCB) of a class C1 system nominally satisfies the discretionary security requirements by providing separation of users and data. It incorporates some form of credible controls capable of enforcing access limitations on an individual basis, i.e., ostensibly suitable for allowing users to be able to protect project or private information and to keep other users from accidentally reading or destroying their data. The class C1 environment is expected to be one of cooperating users processing data at the same level of sensitivity.

Class C2: Controlled Access Protection - Systems in this class enforce a more finely grained discretionary access control than C1 systems, making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

Class B1: Labeled Security Protection - Class B1 systems require all the features required for class C2. In addition, an informal statement of the security policy model, data labeling (e.g., secret or proprietary), and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information.

Class B2: Structured Protection - In clas B2 systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in class B1 systems be extended to all subjects and objects in the automated data processing system. In addition, covert channels are addressed. The TCB must be carefully structured into protection-critical and non- protection-critical elements. The TCB interface is well-defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for system administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class B3: Security Domains - The clas B3 TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant system engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Class A1: Verified Design - Systems in clas A1 are functionally equivalent to those in class B3 in that no additional architectural features or policy requirements are added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature, starting with a formal model of the security policy and a formal top-level specification (FTLS) of the design. An FTLS is a top level specification of the system written in a formal mathematical language to allow theorems (showing the correspondence of the system specification to its formal requirements) to be hypothesized and formally proven. In keeping with the extensive design and development analysis of the TCB required of systems in class A1, more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported.

6.2.3 Sources

Refer to Bibliography [45] Trusted Computer System Evaluation Criteria (TCSEC), 1985.

Note: The TCSEC, its interpretations, and guidelines all have different color covers and are sometimes known as the "Rainbow Series". The TCSEC is a standard internal to and product of:
Department of Defense, Washington, D.C., USA.

6.3 ITSEC/ITSEM – Information Technology Security Evaluation Criteria and Methodology

⇒D⇒	⇒I⇒		⇒O⇒

6.3.1 Aim

To provide a framework of evaluation criteria and evaluation methodology for IT security evaluation for the European market.

6.3.2 Description

The evaluation criteria ”Information Technology Security Evaluation Criteria (ITSEC)” and the evaluation manual ”Information Technology Security Evaluation Manual (ITSEM)” are among the predecessor documents of the Common Criteria and of the Common Evaluation Methodology. They have been developed in the early 1990s by the four European nations France, Germany, the Netherlands and the United Kingdom.

The ITSEC assurance is based on the approach introduced in the TCSEC. However, the separation between functional and assurance requirements in the ITSEC allows a greater flexibility. The assurance requirements are themselves again split into the two aspects of effectiveness and correctness. Assessment of effectiveness involves consideration of the following aspects of the Target of Evaluation (TOE):

— the suitability of the Toe's security enforcing functions to counter the threats to the security of the TOE identified in the security target;

— the ability of the Toe's security enforcing functions and mechanisms to bind together in a way that is mutually supportive and provides an integrated and effective whole

— the ability of the Toe's security mechanisms to withstand direct attack;

— whether known security vulnerabilities in the construction of the TOE could in practice compromise the security of the TOE;

— that the TOE cannot be configured or used in a manner which is insecure but which an administrator or end-user of the TOE would reasonably believe to be secure;

— whether known security vulnerabilities in the operation of the TOE could in practice compromise the security of the TOE.

The focus of the assurance effectiveness requirements is more on those aspects where the evaluator has to use the own knowledge and experience to assess whether the security approach in the evaluated IT product or system is reasonable.

The focus of the assurance correctness requirements in the ITSEC is more on the aspects which shall confirm that the developer information concerning the IT security of the evaluated product or system is correct.

The ITSEC distinguishes between correctness requirements for the construction and the operation of the TOE. The construction criteria cover the Development Process with different specification layers beginning with a high level description of the requirements which can be instantiated to an Architectural Design which can again be instantiated to a Detailed Design and to the implementation representation. Construction aspects of the Development Environment covered by the ITSEC are Configuration Control, Programming Languages and Compilers, and Developers Security.

The operation requirements are further subdivided into the aspects of Operational Documentation with User Documentation and Administration Documentation and the Operational Environment with Delivery and Configuration, and Start-up and Operation.

The correctness requirements in the ITSEC are presented in the form of six hierarchically ordered assurance levels E1 to E6. From level to level additional requirements ensure a more rigorous evaluation of the IT product and system. The assurance effectiveness requirements are not included in the assurance levels. However, the information obtained from the correctness assessment which is to be used to perform a vulnerability analysis is defined.

The ITSEC outline additionally the relationship of the evaluation levels to the TCSEC classes.

The ITSEM builds on the ITSEC describing how a TOE should be evaluated according to these criteria. The specific objective of the ITSEM is to ensure that there exists a harmonized set of evaluation methods which complements the ITSEC.

The ITSEM was not based on a predecessor document. It presented as such for the first time much background information for the application of the assurance methods outlined in the ITSEC and indirectly also for the assurance methods used in the TCSEC and the CTCPEC.

6.3.3 Sources

Refer to Bibliography
[40] Information Technology Security Evaluation Criteria (ITSEC), version 1.2,
[41] Information Technology Security Evaluation Manual (ITSEM), version 1.0

Note: ITSEC/ITSEM is a product of:
the European Commission, Directorate General Information Society, Information and Communications Unit, BU 24 0/41, Rue de la Loi 200, B-1049 Brussels.
The Directorate General Information Society may be reached by URL http://europa.eu.int/pol/infso/index_en.htm.

6.4 CTCPEC – Canadian Trusted Product Evaluation Criteria

⇒D⇒	⇒I⇒		

6.4.1 Aim

To provide a metric used for the evaluation of the functionality and assurance of the security services provided by a software or hardware product or system.

6.4.2 Description

The Canadian Trusted Product Evaluation Criteria (CTCPEC) were developed with three objectives in mind:

1. to provide a comparative scale for the evaluation of commercial products;
2. to provide a basis for the development of specifications for trusted computer products; and
3. to provide a method for specifying trusted products in procurements.

Two types of requirements are delineated for trusted processing:

1. specific security service requirements; and
2. assurance requirements.

The CTCPEC specifies functionality and assurance requirements in two distinct groups to allow for the unique security services among products. The functionality group consists of confidentiality, integrity, availability, and accountability criteria while the assurance group consists of the assurance criteria.

Some of the assurance requirements enable an evaluation to determine if the required features are present and functioning as intended. These criteria are to be applied to the set of components comprising a trusted product and are not necessarily to be applied to each product component individually. Hence, some components of a product may be completely untrusted, while others may be individually evaluated to a lower or higher evaluation class than the trusted product considered as a whole. In trusted products at the high end of the range, the strength of the isolation and mediation mechanisms is such that many of the product components can be completely untrusted.

The assurance requirements can be applied across the entire spectrum of electronic data processing products or application processing environments without special interpretation.

6.4.3 Sources

Refer to Bibliography [31] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0.

Note: CTCPEC is an internal standard and product of:
Communications Security Establishment (CSE), P.O. Box 9703, Terminal, Ottawa, Ontario K1G 3Z4, Canada.
CSE) may be reached by URL http://www.cse-cst.gc.ca.

6.5 KISEC/KISEM – Korea Information Security Evaluation Criteria and Methodology

⇒D⇒	⇒I⇒		⇒O⇒

6.5.1 Aim

To provide a framework of security evaluation criteria and security evaluation methodology for firewalls and intrusion detection systems in Korea.

6.5.2 Description

The evaluation criteria ”Korea Information Security Evaluation Criteria (KISEC)” and the evaluation methodology ”Korea Information Security Evaluation Methodology (KISEM)” were developed in 1998 with three objectives:

— to provide a hierarchical rating scale for the evaluation of security functions of firewalls and intrusion detection systems;

— to provide a method for specifying trusted firewalls and intrusion detection systems in procurements;

— to cumulate know-how related to ICT security evaluation by operating its own evaluation criteria and methodology.

The KISEC defines functional and assurance requirements for the each of seven evaluation levels (K1 to K7). Each level has a set of functional and assurance requirements in KISEC to which evaluated firewalls and intrusion detection systems should conform. KISEC has some different functional requirements depending on product type such as firewalls and intrusion detection systems. However assurance requirements are commonly used for both firewalls and intrusion detection systems. The functional requirements consist of identification & authentication, integrity, security audit, security management, etc. Assurance requirements consist of development, configuration management, testing, operation environment, guidance documents, and vulnerability analysis.

The specific level is determined according to the implemented security functions and the confidence of assurance requirements in the firewalls or intrusion detection systems. Depending on the security functional requirements and assurance requirements, the evaluation level is divided into seven levels. K1 represents the lowest level and K7 represents the highest.

The followings are the characteristics of each evaluation level:

— Level K1 must satisfy the minimum level of security functions such as identification & authentication for system administrator and security management, etc. Also, there must be security target and functional specifications;

— Level K2 must satisfy the requirements of the level K1 and be able to create and maintain audit records on security related activities. Also, architectural design document must be required. Vulnerability and misuse analysis of firewall or intrusion detection system must be carried out;

— Level K3 must satisfy the requirements of the level K2 and be able to check whether there has been any modification to the stored data inside firewall or intrusion detection system and transmitted data. Also, detailed design and configuration management documents are required;

— Level K4 must satisfy all the requirements of the level K3 and provide the identification & authentication function that protects firewall or intrusion detection system from replay attacks. Also, source code and/or hardware design documents are submitted;

— Level K5 must satisfy all the requirements of the level K4 and provide mutual authentication function. Also, formal model of firewall or intrusion detection system security policy is required. Functional specifications, architectural design documents, and detailed design documents must be written in semi-formal;

— Level K6 must satisfy the requirements of the level K5. At this level, consistency among detailed design documents, source code, and/or hardware design documents must be verified;

— Level K7 must satisfy all the requirements of level K6. At this level, functional specifications and architectural design documents must be written in the formal so it is synchronized with formal model of system security policy.

The KISEM builds on the KISEC describing how firewalls and intrusion detection systems should be evaluated according to these criteria. The specific objective of the KISEM is to ensure that there exists a harmonized set of evaluation methods that complements the KISEC.

6.5.3 Sources

Refer to Bibliography:
[50] Korea Information Security Evaluation Criteria (KISEC),
[51] Korea Information Security Evaluation Methodology (KISEM).

Note: KISEC/KISEM is a product of:
Korea Information Security Agency, 78, Karak dong, Songpa-Gu, Seoul 138-160, Korea
The Korea Information Security Agency may be reached by URL http://www.kisa.or.kr/.

6.6 RAMP – Rating Maintenance Phase

⇒D⇒	⇒I⇒		⇒O⇒

6.6.1 Aim

To provide a mechanism to extend the previous TCSEC rating to new versions.

6.6.2 Description

The Rating Maintenance Phase (RAMP) Program was established to provide a mechanism to extend the previous TCSEC rating to a new version of a previously evaluated computer system product. RAMP seeks to reduce evaluation time and effort required to maintain a rating by using the personnel involved in the maintenance of the product to manage the change process and perform Security Analysis. Thus, the burden of proof for RAMP efforts lies with those responsible for system maintenance (i.e., the vendor or TEF) instead of with an evaluation team.

Requirements exist in the Common Criteria for Information Technology Security Evaluation (CCITSE) for maintenance of existing EAL levels. A RAMP-like program is currently being developed to address these requirements.

6.6.3 Sources

Refer to Bibliography [32] Rating Maintenance Phase Program (RAMP), Doc Vers. 2, 1995.

Note: RAMP is a product of:
National Computer Security Center (NCSC), 9800 Savage Road, Fort George G. Meade, Maryland 20755-6000, USA.

6.7 ERM – Evaluation Rating Maintenance (in general)

⇒D⇒	⇒I⇒		⇒O⇒

6.7.1 Aim

To extend obtained assurance beyond its lifecycle and/or time period, especially after modification.

6.7.2 Description

Once assurance for a system has been obtained, there will still be assurance required when the system is modified. Schemes exist to preserve the assurance of a system through minor modification, and so maintain the assessment (i.e. the ”certificate” or ”rating”).

Evaluation Rating Maintenance is the phase of the assessment that follows the evaluation phase. Understood under this term are a series of rating maintenance actions that assess the compliance with applicable requirements of updated versions of the product and allow those versions to be listed. During ERM, the vendor performs the majority of the work to determine that changes to the product maintain the previously attained rating.

In a ERM scheme there are various entities involved with respective responsibilities (vendor, user, certification bodies). With respect to the assurance framework this means that the assurance method called ”evaluation rating maintenance” has a strong dependency on both the design/development and operation assurance phases.

Evaluation Rating Maintenance schemes exist in various forms and typically consist of the following components.

— **Applicable Requirements: T**he requirements under which the product is to be evaluated.

— **ERM Audit:** The review of the RAMP evidence, based on a suitable representative sample, to ensure that only approved changes are implemented, and that security analysis is performed satisfactorily. In addition to the required RAMP audits performed by the VSAs, aperiodic RAMP Audits may be performed by a security analysis team.

— **ERM Plan:** The vendor document that describes the mechanisms, procedures, and tools used to meet the RAMP Requirements. The procedures in the ratings maintenance plan are followed throughout the rating maintenance phase. The ratings maintenance plan is proposed by the vendor and approved as part of the evaluation process. The ratings maintenance plan may change during the course of RAMP for a product, particularly in the identification of designated personnel.

— **Security Analysis:** The examination of whether a proposed change, or set of changes, upholds the security features and assurances of the original product and any subsequent releases of the product that have been previously maintained under RAMP, in compliance with the applicable requirements.

The operators of the ERM scheme are typically:

— **Security Analysis Team:** Individuals (e.g., VSAs, additional evaluators) responsible for performing the security analysis and presentation and defense of the RAMP evidence before the technical review board.

— **Technical Review Board** provides a source of senior technical review of the technical findings, conclusions, and recommendations of individual evaluation teams. The technical review board serves as a check point for the quality, uniformity, and consistency of evaluations.

In the US, ERM has been formalized as RAMP and applied to TPEP and ISO/IEC 21827 (SSE-CMM) ratings. In the UK, a ERM has been formalized as Certificate Maintenance Scheme and is based on ITSEC ratings.

The ISO/IEC 15408 evaluation criteria recognize ERM but leave evaluation maintenance to the national bodies overseeing the evaluation scheme.

6.7.3 Sources

For the US Evaluation Maintenance Program refer to subclause 6.6.

For the UK Evaluation Maintenance Program refer to Bibliography:
[44] UK Certificate Maintenance Scheme, Issue 1.0.

Note: The Certificate Maintenance Scheme is a product of:
Senior Executive, UK IT Security Evaluation and Certification Scheme, Certification Body, PO Box 152, Cheltenham Glos GL52 5UF

6.8 TTAP – Trust Technology Assessment Program

⇒D⇒	⇒I⇒		

6.8.1 Aim

To establish, approve, and oversee commercial evaluation facilities.

6.8.2 Description

The Trust Technology Assessment Program (TTAP) is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. TTAP will establish, approve, and oversee commercial evaluation facilities. The program focuses initially on products with features and assurances characterized by the Common Criteria for Information Technology Security Evaluation (CCITSE).

To conduct evaluations under TTAP, an organization must be accredited as a TTAP Evaluation Facility (TEF). First, a prospective TEF applies to the TTAP Oversight Board for provisional status. If accepted, the prospective TEF is granted authorization to proceed with a trial evaluation and is placed on the provisional TEF list. Second, the provisional TEF contracts with a vendor and conducts a trial evaluation of a trusted product. Following the trial evaluation, the provisional status is lifted, and the TEF may conduct evaluations under TTAP.

The TTAP Oversight Board will monitor the TEFs to ensure quality and consistency across evaluations. Vendors of information technology products desiring a security evaluation will contract with a TEF and pay a fee for their product's evaluation. Upon completion of the evaluation, the product will be added to NSA's Evaluated Products List.

6.8.3 Sources

Refer to Bibliography [28] Trust Technology Assessment Program (TTAP).

Note: TTAP is a standard internal to US Government and a product of:
TTAP Oversight Board c/o National Security Agency, 9800 Savage Road, Suite 6740, Ft. Meade, Md 20755-7640

6.9 TPEP – Trusted Product Evaluation Program

⇒D⇒	⇒I⇒		

6.9.1 Aim

To encourage the widespread availability of trusted computer products.

6.9.2 Description

Under the Trusted Product Evaluation Program (TPEP), vendors approach NSA with their commercial-off-the-shelf (COTS) computer security product requesting an evaluation that targets a particular level of trust rating. Evaluators working under TPEP use the TCSEC and its interpretations to assess how well the product meets the requirements for the targeted rating. The results of the TPEP evaluations are published quarterly in the Evaluated Products List (EPL) as Chapter 4 of the Information Systems Security Products and Services Catalog.

The ultimate goal of TPEP is to encourage the widespread availability of trusted computer products to data owners and users who wish to protect their sensitive and/or classified information. Additional goals are:

— To ensure the availability of useful trusted products that meet the end user's operational needs.

— To provide trusted products to be used when constructing an implemented trusted system.

— To provide specific guidance on the utility of trusted products.

— To provide specific guidance on the interoperability of the security features and the level of assurance associated with specific features for individual evaluated products.

— To foster an open and cooperative business relationship with the computer and the National and Defense Information Infrastructures.

6.9.3 Sources

Refer to Bibliography [46] Trusted Product Evaluation Program (TPEP).

Note: TPEP has been replaced by the Trust Technology Assessment Program. No new evaluations are being conducted using the Trusted Computer System Evaluation Criteria (TCSEC). Refer to TCSEC.
TPEP is a standard internal to US Government and a product of:
National Security Agency, 9800 Savage Road, Suite 6740, Ft. Meade, Md 20755-7640

6.10 Rational Unified Process® (RUP®)

6.10.1 Aim

To provide a completely populated software engineering life cycle framework, including environment, processes, activities, techniques and tools.

6.10.2 Description

The Rational Unified Process® or RUP® is a commercial off-the-shelf software engineering process framework developed and maintained by Rational® Software. The framework is continuously updated and improved to reflect recent experiences and evolving best practices.

Unlike e.g., ISO 12207, an "empty" framework RUP is populated with guidance, processes, methods, techniques, templates, tools and examples, out of which a concrete process framework can be instantiated, managed and improved.

Like the software products it produces, RUP itself is designed and documented using the Unified Modeling Language (UML). An underlying object model of RUP is the Unified Software Process Model (USPM).

From a Project Management standpoint RUP provides a structured approach to assigning tasks and responsibilities within a development organization. It emphasizes addressing high-risk areas very early and allows to refine the requirements as the project evolves to help high-quality software that meets user requirements within a predictable schedule and budget.

RUP activities effectively use the Unified Modeling Language (UML) to create and maintain models, and emphasizes the development and maintenance of models — semantically rich representations of the software system under development — which are supported by computerized tools. These tools automate large parts of the process such as visual modelling, programming, testing and configuration management.

RUP is a configurable process framework to fit small development teams as well as large development organizations. Its process architecture provides commonality across a family of processes and is supported by a Development Kit to support the configuration of the RUP to suit the needs of a given organization.

RUP incorporates best practices, in particular the six fundamental best practices:

— Develop software interactively

— Manage requirements

— Use component-based architectures

— Visually model software

— Verify software quality

— Control changes to software

From a process management and improvement standpoint RUP matches CMM and 15504 requirements at the project level. When correctly implemented it corresponds to CMM organizational levels 2 or 3. It is suited for higher Process Maturity because the software process is well defined, and management has good insight into technical progress on all projects.

6.10.3 Sources

Refer to Bibliography [52] Philippe Kruchten, The Rational Unified Process — An Introduction

Note: RUP® is a product of:
Rational, a wholly owned subsidiary of IBM Corporation, Software Group, Route 100, Somers, NY 10589, USA.
Rational may be reached by URL http://www.rational.com/rup/.

6.11 ISO/IEC 15288 – System Life Cycle Processes

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.11.1 Aim

To provide life cycle models, processes and activities for the entire life cycle of any kind of complex technical systems.

6.11.2 Description

ISO/IEC 15288-System Life Cycle Processes is the first ISO standard to deal with system life-cycle processes of generally complex systems comprising hardware, human interfaces and software. At present, this ISO/IEC standard is at FDIS stage, Finial Draft International Standard, with a scheduled publication date of October 2002.

This standard encompasses the life cycle of man-made systems, spanning the time from the conception of the ideas through to the retirement of the system. It provides the processes for acquiring and supplying system products and services that are configured from one or more of the following types of system components: hardware, software, and human interfaces. This framework also provides lists of activities and provision for the assessment and improvement of the life cycle and its processes.

The processes in this international standard form a comprehensive set from which an organization may construct life cycle models appropriate to the product, service types, and markets in which they are active. An organization, depending upon its purpose, may select and apply an appropriate subset to fulfill that purpose via a tailoring provision.

The most relevant processes from a quality point of view are: the quality management process; the integration, verification and validation processes; and the project planning, assessment and control processes.

This international standard may be used in several ways:

— An organization might use the standard to establish an environment of desired processes that can be supported by an infrastructure of trained personnel, utilizing specific methods, procedures, techniques and tools. This environment would be employed by the organization to manage its projects and to facilitate progress through the life cycle stages.

— A project, within an organization, might use this standard to select, structure, employ and perform the elements of the established environment to provide products and services.

— The standard might also be used, via contract or agreement, within the supplier/acquirer relationship, to select, agree on, and perform the processes and activities called out in the standard. Additionally, this mode may also be used to assess conformance of the acquirer's and suppliers performances with the agreement.

The Standard is supported by a Guide (ISO/IEC 19760), a technical report intended to:

— be used as a companion document to ISO/IEC 15288 - System Life Cycle Processes

— give guidelines for the implementation of the International Standard.

The Guide is intended to be applicable to large and small systems, to systems requiring large and small project teams, and to new and legacy systems. The Guide includes: 1) links to other ISO documents that are necessary for supporting the implementation of the International Standard as well as for assessing its effectiveness of implementation and 2) factors that should be considered when implementing the International Standard.

The Guide should is useful to those who

— implement ISO/IEC 15288, in an organization

— use ISO/IEC 15288, for a specific system, or

— write organization or domain specific standards based on ISO/IEC 15288, .

Specific applications can be tailored as appropriate to the system size, project staffing or system type. Tailoring guidance is provided in both Annex A of the International Standard and Clause 4 of the Technical Report. The Guide does not and is not intended to provide the rationale for the requirements of the International Standard.

6.11.3 Sources

Refer to Clause 2: ISO/IEC 15288.

Refer to Bibliography: ISO/IEC TR 19760 Systems engineering — Guide for ISO/IEC 15288

Note: ISO/IEC 15288 is a product of the committee:
ISO/IEC JTC 1/SC 7/WG 7 Information technology - Software and system engineering - Life cycle management

6.12 ISO/IEC 12207 – Software Life Cycle Processes

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.12.1 Aim

To provide life cycle models, processes and activities for the entire life cycle of software systems.

6.12.2 Description

The importance of software as an integral and necessary part of many products and systems requires a common international framework for specifying the best practices for software processes, activities and tasks.

The ISO/IEC 12207 groups the activities that may be performed during the life cycle of software into:

— primary processes (acquisition process, supply process, development process, operation process, maintenance process)

— supporting processes (documentation process, configuration management process, quality assurance process, verification process, validation process, joint review process, audit process, problem resolution process)

— organizational processes (management process, infrastructure process, improvement process, training process).

Each of the processes details the included activities and tasks defining specific responsibilities; outputs of activities/tasks are also identified.

It must be noted that this standard does not imply any specific life cycle model.

The processes of ISO/IEC 12207 form a comprehensive set. An organization, depending on its purpose, can select an appropriate subset to fulfill that purpose. In addition all activities may be selected and tailored proportional to the scope, size, complexity and criticality of the software product and of the organization itself.

The most relevant processes from a quality point of view are the: Quality assurance process, verification process, validation process, joint review process, audit process and problem resolution process. Moreover the standard highlights process internal evaluations conducted during all day-to-day activities.

The audience for this standard is:

— organizations acquiring a system that contains software or a stand-alone software product

— software products suppliers

— organizations involved in operation and maintenance of software.

— The Guide to 12207 is a Technical Report designed to elaborate on factors which should be considered when applying ISO/IEC 12207 in the context of the various ways in which ISO/IEC 12207 can be applied.

— Three fundamental life cycle models are discussed and examples of tailoring are provided.

— The guidance is not intended to provide the rationale for the requirements of ISO/IEC 12207.

6.12.3 Sources

Refer to Clause 2: ISO/IEC 12207, .

Refer to Bibliography: ISO/IEC TR 15271 Information technology — Guide for ISO/IEC 12207

Note: ISO/IEC 12207 is a product of the committee:
ISO/IEC JTC 1/SC 7/WG 7 Information technology - Software and system engineering - Life cycle management

6.13 V–Model

⇒D⇒	⇒I⇒	⇒T⇒	⇒O⇒

6.13.1 Aim

To lay down in a uniform and binding form what has to be done, how the tasks are to be performed and what tools are to be used in developing software systems.

6.13.2 Description

The V Model is a series of General Directives (250, 251, and 252) that describe a Lifecycle Process Model consisting of procedures, methods to be applied, and the functional requirements for tools to be used in developing software systems. It was originally developed for the German Federal Armed Forces. The V-Model is an internationally recognised development standard.

The V-Model defines what steps are to be taken and which methods are to be applied for the development tasks and which functional characteristics the tools to be used must have. The V-Model encompasses a Lifecycle Process Model, Allocation of Methods, and Functional Tool Requirements.

The Lifecycle Process Model is structured in three parts:

— Part 1: Regulations.
This part contains binding regulations concerning the steps to be performed (activities) and results (products).

— Part 2: Supplements with regard to Authorities.
This part exists once for the field of German Federal Armed Forces and once for the field of the civilian Federal Administration. It contains instructions to apply the Lifecycle Process Model in the respective field.

— Part 3: Collection of Manuals.
This part contains a set of manuals dealing with special topics, such as ICT security or use of object-oriented languages.

The V-Model's is intended as Basis for contracts, for instruction and for communications between the involved parties. By means of the description of the documents and the provision of a glossary, it serves as the basis for mutual understanding and reduces frictional losses between customer, user, contractor, and developer.

The provisions of the V-Model are organizationally impartial. They are restricted exclusively to the technical development process. Therefore, the V-Model is not only suitable as the development standard in public administration but also in industry.

The use of the V-Model is free of license fees. It is non-proprietary and not copy-protected.

The V-Model contains rules which are necessary for the generation of critical software. The currently valid security criteria (ITSEC) have been fulfilled with respect to their regulations governing the development process by the application of the V-Model. A certification of the software so developed is hence considerably facilitated.

The V Model, Methods Standard, and Tool Standard present complete coverage of the functional areas software development, quality assurance, configuration management, and project management), provide concrete support, is sophisticated, yet flexible and balanced, has a wide spectrum, and is publicly controlled under the supervision of a Change Control Board. Improvements as well as corrective changes are handled through the Control Board.

The influence of the users necessary for the maintenance and modification processes of the V-Model is ensured by a change control board which meets roughly once a year with representatives from industry and authorities. The change control board is obliged, according to its orders of procedure, to process carefully all received change requests to the V-Model.

6.13.3 Sources

Refer to Bibliography: [42] V-Model — Development Standard for IT Systems, VM 1997

Note: The V-Model is a product of:
BWB IT I 5, Postfach 7360, D-56057 Koblenz, Germany

6.14 ISO/IEC 14598 – Software product evaluation

⇒D⇒			⇒O⇒

6.14.1 Aim

To provide a method for measurement, assessment and evaluation of software product quality

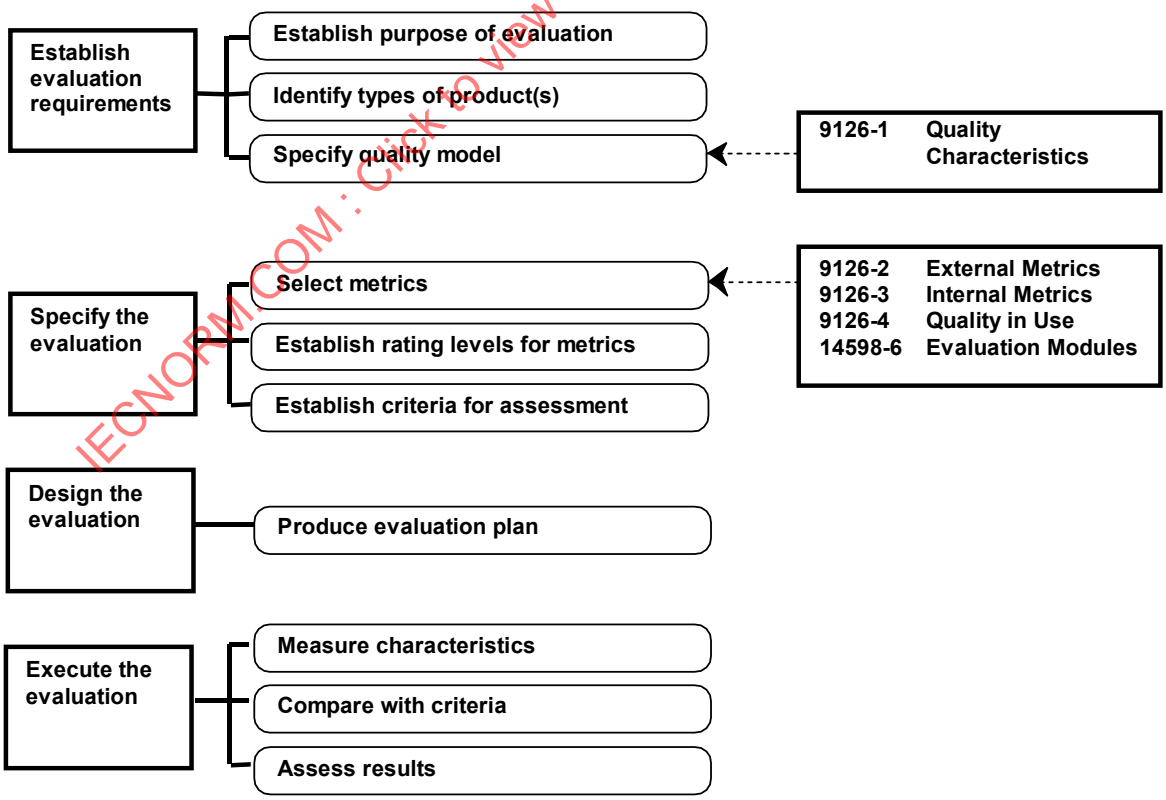
6.14.2 Description

ISO/IEC 14598 is based on the general quality model of ISO/IEC 9126. It therefore provides a framework for evaluating the quality of all types of software product and states the requirements for methods of software product measurement and evaluation.

ISO/IEC 14598 is intended for use by developers, acquirers and independent evaluators, particularly those responsible for software product evaluation. The evaluation results produced from the application of ISO/IEC 14598 can be used by managers and developers/maintainers to measure compliance to requirements and to make improvements where necessary. The evaluation results can also be used by analysts to establish the relationships between the internal and external metrics. Process improvement personnel can use the evaluation results to determine how processes can be improved through study and examination of the project's product quality information.

The ISO/IEC 14598 series of standards give methods for measurement, assessment and evaluation of software product quality. They describe neither methods for evaluating software production processes nor methods for cost prediction. Software product quality measurements may, of course, be used for both these purposes.

The ISO/IEC 14598 evaluation process flow chart is as follows:



6.14.3 Sources

Refer to Clause 2: ISO/IEC 9126-1, ; ISO/IEC 14598-1,

Refer to Bibliography:

ISO/IEC TR 9126-2 Software engineering — Product quality — Part 2: External metrics
ISO/IEC TR 9126-3 Software engineering — Product quality — Part 3: Internal metrics
ISO/IEC TR 9126-4 Software engineering — Product quality — Part 4: Quality in use metrics

ISO/IEC 14598-2 Software engineering — Product evaluation — Part 2: Planning and management

ISO/IEC 14598-3 Software engineering — Product evaluation — Part 3: Process for developers
ISO/IEC 14598-4 Software engineering — Product evaluation — Part 4: Process for acquirers
ISO/IEC 14598-5 Information technology — Software product evaluation — Part 5: Process for evaluators
ISO/IEC 14598-6 Software engineering — Product evaluation — Part 6: Documentation of evaluation modules

Note: ISO/IEC 14598 is a product of the committee:
ISO/IEC JTC 1/SC 7/WG 6 Information technology - Software and system engineering - Evaluation and metrics

6.15 X/Open Baseline Security Services

⇒D⇒			

6.15.1 Aim

To provide assurance through conformance to X/Open standards certified by third parties.

6.15.2 Description

X/Open branding is a different type of assurance as it provides assurance by conformance testing, vendor warranty, and trade mark (implying third party controls). This approach provides assurance that the system will enforce the vendor's claims by providing documented evidence and third party enforcement of standards.

X/Open is a consortium of companies creating open standards to provide an open systems environment called the Common Applications Environment (CAE). This environment provides for interoperability and portability of applications and systems. Products, systems, and applications which conform to the X/Open standards carry the X/Open trade mark to signify compliance to their standard.

X/Open branding is the procedure by which a vendor certifies that its product complies with one or more of X/Open's standards. The certification will contain a conformance statement of the actual system details and testing evidence to support the vendor's claims. Testing of the vendor's product may be performed by the vendor or a third party; however, the test lab must be approved by X/Open.

X/Open's answer to security is the X/Open Baseline Security Services (XBSS) specification developed to provide buyers of X/Open-branded systems with assurance that such systems provide a defined minimum level of security functionality. The XBSS is essentially a Protection Profile containing mostly security functional requirements and only a few assurance requirements. This profile defines a minimum level of security functionality that products must provide. It also defines specific default settings in cases where the requirement is to provide selectable security options. To be registered as conformant to this Profile Definition a system must provide this level of security or greater.

Any system that meets the defined security level can be branded as conformant. Details of the actual system/operating system must be recorded in the Conformance Statement. It does require that products support the mandatory security functionality and default parameter settings as defined in the X/Open XBSS Specification.

X/Open differs from the other three candidate AA methodologies as it does not focus on developmental assurance. The XBSS specification contains mainly functional requirements and the bulk of the assurance is provided by conformance testing, the vendor's warranty, and by the X/Open trade mark.

6.15.3 Sources

Refer to Bibliography:
[39] X/Open Baseline Security Services (XBSS),
[30] Practical Guide to the Open Brand,.

Note: X/Open Branding is a product of:
The Open Group, 44 Montgomery, Street, Suite 960, San Francisco, CA 94104-4704, USA.
The Open Group may be reached by URL http://www.opengroup.org/

6.16 SCT – Strict Conformance Testing

	⇒I⇒		

6.16.1 Aim

To test security functionality

6.16.2 Description

Strict (Security) Conformance Testing defines a method of testing of secure systems against a publicly available specification - most commonly, a standard. Test suites are designed in a systematic way to stress test implementations. The starting point for deriving tests is an abstract security target (AST) which is incorporated into a base security standard. This offers a means of structuring test suites and providing tractability from security requirements through security functions and supporting mechanisms to the tests of those mechanisms. The tests are written at an abstract level corresponding to the level of abstraction of the base standard. The test suite can then be parameterised for a particular implementation. This offers the advantage of allowing a certain amount of pre-evaluation of the abstract security target and the corresponding test suite. It ensures a base level of coverage and reduces the amount of work required in preparing evidence for evaluation where the subject is an implementation of a standard.

SCT is functionality testing rather than robustness testing.

6.16.3 Sources

Refer to Bibliography: [20] SCT. Strict Conformance Testing.

Note: SCT is a product of:
National Physical Laboratory, Teddington, Middlesex, TW11 0LW, UK.
The National Physical Laboratory may be reached by URL http://www.npl.co.uk/

6.17 ISO/IEC 21827 – Systems Security Engineering – Capability Maturity Model (SSE-CMM®)

D	I	T	O

6.17.1 Aim

To improve the organization's systems security engineering processes and to produce a deliverable with capability assurance.

6.17.2 Description

ISO/IEC 21827 *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)* primarily focuses on the process areas (PAs) required for systems security engineering, which are referred to as Engineering PAs. ISO/IEC 21827 also includes PAs that are required to support projects performed within the systems security engineering area, referred to as Project PAs, and PAs that are required within the organization as a whole to support the systems security engineering PAs, referred to as Organization PAs.

The emphasis of ISO/IEC 21827 is on the systems security engineering PAs and their activities. The PAs of the SSE-CMM can be tuned to the needs of the organization, and the scope of application of ISO/IEC 21827 can be a specific project, an organizational department, or the organization in its entirety.

ISO/IEC 21827 is applicable to and can be used by any organization that is involved in or has an interest in Information and Communications Technology (ICT) Security. Organizations can range from those who develop products and/or integrate products, both security and non-security products, to organization that use security products or provide security services. Thus ISO/IEC 21827 can be used by organizations to improve their system security engineering processes to develop ICT Security products or deliver ICT Security services (such as a threat and risk assessment) with higher quality and within schedule.

The SSE-CMM is a unique model as it details security engineering requirements for engineering security systems and providing engineering security services in addition to the security requirements, which the development environment must meet. Furthermore, it contains PAs for a wide range of development areas such as defining security requirements, system testing, threat and vulnerability analysis. This is different from the Trusted Capability Maturity Model (TCMM), which only specifies requirements, which the organization's development environment must satisfy.

ISO/IEC 21827 contains PAs, Base Practices (BP), Generic Practices (GP), and capability levels to describe the organization's processes and to measure how well an organization performs the PAs. The PAs consist of a group of related BPs which focus on specific process activities within an organization while the GPs are related to the overall process maturity throughout the organization. The PAs, BPs, and GPs can be thought of as requirements and the capability levels indicate compliance to ISO/IEC 21827; however, these requirements cover the what but not the how a process achieves the end result to not interfere with the organizations operating model. A capability level is assigned to each PA to indicate the level of compliance to ISO/IEC 21827, which ranges from level 0 "Not Performed" to Level 5 "Continuously Improving". A rating profile is presented as a graphical representation of the PAs performed with their associated capability levels, or as the maturity level attained by the organization as a whole. The capability level and rating profiles are determined by the Appraisal Team performing an appraisal of the organizations compliance to ISO/IEC 21827, according to the SSE-CMM Appraisal Methodology (SSAM).

A capability level demonstrates that an organization has achieved a minimum capability level for all of the applicable PAs (a group of related practices). The GPs are specific requirements which apply to all PAs related to the overall process maturity and institutionalisation of individual PAs throughout the organization. Each successive level indicates an improvement of the organization's overall process maturity and ability to implement the PAs throughout the organization.

The rating profile depicts the organization's capability level per individual PA indicating the organization's strengths and weaknesses. The rating profile is used to indicate where an organization must apply their efforts to improve their processes and achieve the next higher capability level. Although this was originally not intended, a rating profile can become a procurement tool to require an organization to achieve different capability levels for specific PAs rather than one capability level for all PAs. For example, a procurement profile might specify a capability level of 2 for PAs 1 - 5 and a capability level 3 for PAs 6 - 10.

The SSE-CMM of ISO/IEC 21827 is a continuous model, which is more flexible for industry organizations in that only the applicable PAs can be selected; however, it is more difficult to compare ratings of different organizations if a staged model like TCMM was used.

An organization should attain a minimum capability level of 2 for the PAs required to satisfy good security since Level 1 is inadequate as the processes are adhoc and may not be complete. In terms of the SSE-CMM model, this means that the organization is planning and tracking the performance of their base practices and correcting them when errors occur in the work products. This indicates that their processes are repeatable and consistent allowing to produce a predictable and consistent product, which is an important assurance factor.

6.17.3 Sources

Refer to Clause 2: ISO/IEC 21827,

Refer to Bibliography:
[24] System Security Engineering Capability Maturity Model, Model Description (SSE-CMM Model), Version 2.0 ,
[25] System Security Engineering Capability Maturity Model, Appraisal Methodology (SSE-CMM Method), Version 2.0.

Note 1: ISO/IEC 21827 is a product of the committee:
ISO/IEC JTC 1/SC 27/WG 3 Information technology - Security techniques - Security evaluation criteria

Note 2: The base document of ISO/IEC 21827 was provided and is maintained by
The International Systems Security Engineering Association (ISSEA)
13873 Park Center Road, Suite 200, Herndon, VA 20171, USA and
1327 Upper Dwyer Hill Road, Carp, Ontario, K0A 1L0, Canada
ISSEA also may be reached by URL http://www.issea.org.

6.18 TCMM – Trusted Capability Maturity Model

D	I		

6.18.1 Aim

To improve the organization's software security assurance and software development processes.

6.18.2 Description

The Trusted Capability Maturity Model (TCMM) is a developmental security software assurance standard based on the fundamental principles and structure of the CMM developed by SEI. Although the TCMM is a specialty CMM, it was created by merging the Trusted Software Development Methodology (TSDM) and the SEI CMM resulting in many revised Key Process Areas (KPA) and a new KPA called Trusted Software Development containing new practices which did not fit under any of the existing KPAs. The TCMM focuses only on the development environment and targets the management and organizational activities of an organization which differs considerably from ISO/IEC 21827 (SSE-CMM). The TCMM is applicable only to processes and systems. Any processes related to the TOE development are out of scope.

The TCMM contains Key Process Areas, Generic Practices, and capability levels to describe the organization's processes and measure how well an organization performs the KPAs similar to the SSE-CMM model of ISO/IEC 21827. A capability level is awarded to an organization to indicate the level of compliance which ranges from level 1 Initial to Level 5 Optimizing. Level 1 contains few KPAs and the organization is said to have ad hoc processes.

Being a staged model, the TCMM capability levels form a series of stages with each level (except for level 1) containing a unique set of related KPAs. Unlike a continuous model, organizations must meet all KPAs to achieve compliance to a capability level; however, these stages help the organization focus on improving their processes and provide a clear path of improvement to the next level. These stages facilitate procurement and comparisons since the KPAs per stage do not change. Being a staged model it is similar to the CC; however, the TCMM is limited to the development environment security where the CC focuses on TOEs.

6.18.3 Sources

Refer to Bibliography:
[26] Trusted Capability Maturity Model, Version 2.0,
further to [27], [48].

Note: TCMM was jointly developed by the National Security Agency (NSA) and the Software Engineering Institute (SEI). The TCMM was never published as NSA subsequently decided to support only one of the two initiatives it had sponsored.

6.19 CMMI – Capability Maturity Model ® Integration

D	I	T	O

6.19.1 Aim

To provide guidance for improving the organization's processes and its ability to manage the development, acquisition, and maintenance of products and services.

6.19.2 Description

The purpose of Capability Maturity Model ® Integration (CMMI SM) is to provide guidance for improving the organization's processes and its ability to manage the development, acquisition, and maintenance of products and services. CMM ® Integration SM places proven practices into a structure that helps the organization assess its organizational maturity and process area capability, establish priorities for improvement, and guide the implementation of these improvements.

The CMMI Product Suite springs from a framework that generates multiple integrated models, courses, and an appraisal method. As new material is added to the framework, more integrated models and supporting materials will become available that cover additional disciplines.

Presently the following models are available:

— CMMI-SE/SW for the systems engineering and software engineering integrated model

— CMMI-SE/SW/IPPD for the systems engineering, software engineering, and integrated product and process development model

— CMMI-SE/SW/IPPD/SS for the systems engineering, software engineering, integrated product and process development, and supplier sourcing model.

The CMMI effort is intended to support process and product improvement and to reduce redundancy and eliminate inconsistency when using separate stand-alone models. The goal is to improve efficiency, return on investment, and effectiveness by using models that integrate disciplines such as systems engineering and software engineering that are inseparable in a systems development endeavor.

The concept of the CMMI Project was to improve the usability of the CMM ® technology in a wider set of disciplines beyond its initial success for software engineering alone.

The concept called for use of common terminology, common components, and rules for constructing Capability Maturity Models that would be available with a reduction in the amount of training and process improvement effort needed by users of multiple disciplines. As the concept developed, it was advisable to restrict the initial scope of the CMMI Project to a few of the most needed disciplines until the concept was proven. The selection of software engineering, systems engineering, and integrated product development CMMs was made by industry and government participants for the initial proof-of-concept phase. The CMMI Product Suite was designed with the capability to expand in both disciplines and life-cycle coverage. Work has begun on an expansion for acquisition, and coverage of additional disciplines such as security systems engineering is possible. Expansion decisions will be made based on the success of the initial release, user community needs and support, and availability of participants for development.

The CMMI models cover the same life cycles as the source models (Software CMM; Integrated Product Development CMM; and EIA/IS 731, the Systems Engineering Capability Model).

The CMMI framework is designed to accommodate additional disciplines, and it is the intent to add disciplines as needed by our user community. The process for adding new disciplines is now depicted in the Concept of Operations (CONOPS) document for CMMI.

The CMMI A-Spec requires that the CMMI Product Suite be consistent and compatible with ISO/IEC 15504, and that the framework readily accommodate additional disciplines but does not identify any specific ones. To date, supplier sourcing discipline has been added.

6.19.3 Sources

Refer to Bibliography:
[35] Capability Maturity Model ® Integration for the systems engineering and software engineering integrated model, CMMI-SE/SW Version 1.1 ,
[36] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development, Version 1.1, Staged Representation,
[37] CMMISM for Systems Engineering/Software Engineering/Integrated Product and Process Development/Supplier Sourcing, Version 1.1, Staged Representation

Note : CMMI is a product of:
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890).
The Software Engineering Institute may be reached by URL http://www.sei.cmu.edu

6.20 ISO/IEC 15504 – Software Process Assessment

D	I	T	O

6.20.1 Aim

To provide a framework of concepts and processes for the assessment of software life cycle processes according to ISO/IEC 12207. This framework is compatible with process measurement according to ISO/IEC 15939.

6.20.2 Description

ISO/IEC 15504 is compatible with CMM. ISO/IEC 15504 uses the process dimension and the capability dimension. The base practices are split into organization, management, engineering, customer-supplier and support. ISO/IEC 15504 specifies a capability rating of the organization running the development process:

L0	incomplete process
L1	performed process
L2	managed process
L3	established process
L4	predictable process
L5	optimizing process.

The rating is based on the assessment of a specific process instance. All types of assessment are supported. ISO/IEC 15504 is applicable to self assessment and independent assessment, to continuous assessment and to discrete assessment.

ISO/IEC 15504 level 3 rating maps to successful ISO 9000 certification.

6.20.3 Sources

Refer to Clause 2: ISO/IEC 15504-1, ISO/IEC 15504-2, ISO/IEC 15504-3, ISO/IEC 15504-4, ISO/IEC TR 15504-5,

Note: ISO/IEC 15504 is a product of the committee:
ISO/IEC JTC 1/SC 7/WG 10 Information technology - Software and system engineering - Process assessment

6.21 CMM – Capability Maturity Model® (for Software)

D	I		

6.21.1 Aim

To judge the maturity of the software processes and to increase the maturity of these processes of an organization.

6.21.2 Description

The Capability Maturity Model for Software describes the principles and practices underlying software process maturity and is intended to help software organizations improve the maturity of their software processes in terms of an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes.

The CMM is organized into five maturity levels:

Level 1 - Initial. The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.

Level 2 - Repeatable. Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.

Level 3 - Defined. The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.

Level 4 - Managed. Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.

Level 5 - Optimizing. Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

Predictability, effectiveness, and control of an organization's software processes are believed to improve as the organization moves up these five levels. While not rigorous, the empirical evidence to date supports this belief.

Except for Level 1, each maturity level is decomposed into several key process areas that indicate the areas an organization should focus on to improve its software process.

The key process areas at Level 2 focus on the software project's concerns related to establishing basic project management controls. They are Requirements Management, Software Project Planning, Software Project Tracking and Oversight, Software Subcontract Management, Software Quality Assurance, and Software Configuration Management.

The key process areas at Level 3 address both project and organizational issues, as the organization establishes an infrastructure that institutionalizes effective software engineering and management processes across all projects. They are Organization Process Focus, Organization Process Definition, Training Program, Integrated Software Management, Software Product Engineering, Intergroup Coordination, and Peer Reviews.

The key process areas at Level 4 focus on establishing a quantitative understanding of both the software process and the software work products being built. They are Quantitative Process Management and Software Quality Management. The key process areas at Level 5 cover the issues that both the organization and the projects must address to implement continual, measurable software process improvement. They are Defect Prevention, Technology Change Management, and Process Change Management.

Each key process area is described in terms of the key practices that contribute to satisfying its goals. The key practices describe the infrastructure and activities that contribute most to the effective implementation and institutionalization of the key process area.

6.21.3 Sources

Refer to Bibliography: [34] Capability Maturity Model for Software.

Note: CMM is a product of:
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.
The Software Engineering Institute may be reached by URL http://www.sei.cmu.edu

6.22 SE-CMM® – Systems Engineering Capability Maturity Model ®

D	I		

6.22.1 Aim

To improve the system engineering process.

6.22.2 Description

The Systems Engineering Capability Maturity Model ® (SE-CMM ®) describes the essential elements of an organization's systems engineering process that must exist to ensure good systems engineering.

In addition, the SE-CMM provides a reference for comparing actual systems engineering practices against these essential elements. The effort to develop the SE-CMM was instituted in August, 1993, in response to industry requests for assistance in coordinating and publishing a model analogous to the CMM for the systems engineering community. The development effort was a collaboration among several organizations, including the SEI.

Current effort in this area is now part of CMMI.

6.22.3 Sources

Refer to Bibliography:
[21] A Systems Engineering Capability Maturity Model (SE-CMM Model), Version 1.1,
[22] System Security Engineering Capability Maturity Model, Appraisal Methodology (SSE-CMM Method), Version 2.0.

Note: SE-CMM® is a product of:
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890.
The Software Engineering Institute may be reached by URL http://www.sei.cmu.edu

6.23 TSDM – Trusted Software Development Methodology

D	I		

6.23.1 Aim

To provide assurance through the assignment of trust levels to Management Policy, Environment Controls and Management as well as Software Engineering.

6.23.2 Description

The Trusted Software Development Methodology (TSDM) was developed by the Strategic Defense Initiative Office (SDIO) in the mid 1980's to increase software assurance by strengthening the development process.

Due to the estimated size (millions of lines of code) of the proposed SDIO projects, typical software error densities would have rendered the systems inoperative. Analysis suggested that improvements to the development process could reduce the software error rate.

Each characteristic of the software development process was examined to identify potential weaknesses. The result of the analysis was the formulation of 25 Trust Principles.

TSDM defines trust principles as outlined in the July 2, 1993 TSM Report. It contains a rationale for each trust principle; a set of compliance requirements for the trust principle as well as identification of applicable trust classes. In addition, the document identifies a list of associated requirements that describe activities similar to those addressed in the trust principle and provides a list of useful references for the trust principle.

The 25 TSDM trust principles that can be grouped into the following four areas and are related to the general software development process:

— Management Policy (trust principles 1-6);

— Environment Controls (trust principles 7-10);

— Environment Management (trust principles 11-14);

— Software Engineering (trust principles 15-25).

Each of the trust principles are measured by five TSDM Levels:

— T1 (minimal trust);

— T2 (moderate trust);

— T3 (preferred);

— T4 (malicious attack);

— T5 (ideal).

TSDM proposes measurement of software/information assurance (IA). A specific program's Software Development Plan (SDP) requires acceptable TSDM practices being carried out. This is because, the SDP will capture TSDM compliance methods as well as preliminary software engineering team risk analysis results.

Capability Evaluation. Additionally, it is important to understand how TSDM compliance will be identified and tracked using software engineering analysis standards such as the Software Engineering Institutes (SEI) Capability Maturity Model (CMM). Knowledge is required to be able to estimate of the cost associated with providing TSDM training on a program to the software engineering team members. Finally, knowledge of software reuse and metrics collection is necessary.

Note: To integrate the CMM and TSDM a team of people from the National Security Agency and the Software Engineering Institute was formed. The resulting Trusted Capability Maturity Model (TCMM) is the basis for conducting Trusted Software Capability evaluation. Refer to subclause 6.18

6.23.3 Sources

Refer to Bibliography:
[29] Trusted Software Methodology (volumes 1 and 2)
[47] A Trusted Software Development Methodology.

6.24 SdoC – Supplier's declaration of Conformity

D			

6.24.1 Aim

To declare and substantiate conformity of a product, process or service to normative documents under the responsibility of the supplier.

6.24.2 Description

This approach formalizes the developer's commitment to his product with a Suppliers Declaration of Conformity (SDoC). For ICT security systems this declaration would include statements on the system's security compliance. The required structure and content of security functionality as well as the assurance aspect should be defined in a guideline for vendor's and end users.

There are existing SDoC schemes for many aspects of ICT products and SDoCs are already mandatory for Electromagnetic Compatibility (EMC) and Low Voltage Directive (LVD) product compliance in Europe. However, in other cases, like ISO9000, Software Quality, Ergonomics, Environmental Protections, GS marking, etc. the SDoC is voluntary.

The declaration of aspects of security compliance has not yet been considered. However, most supplier's perform an enormous amount of work in specification, design, testing/assurance, and documentation for the security functionality which is not seen by the end user; while others perform only minimum testing. Adequate statements by suppliers on security would increase the transparency and comparability for the end user in selecting trustworthy products.

Furthermore, the ICT security compliance statements in the SDoC would further increase the focus of the suppliers and end users on ICT security. Commercial entities are more than ever driven by "time to market" and this would be a further step to promote security aspects in ICT products on a cost effective and voluntary base.

The related ISO/IEC Standard specifies general criteria for a framework of supporting documentation to strengthen, facilitate and promote confidence in a supplier's declaration of conformity, as defined in ISO/IEC 17050.

6.24.3 Sources

Refer to Bibliography:
ISO/IEC 17024 Conformity assessment — General requirements for bodies operating certification of persons,
ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories,
ISO/IEC 17050-1 Conformity assessment — Supplier's declaration of conformity — Part 1: General requirements

Note: The SdoC a product of the committee:
ISO/CASCO WG 24 Committee on conformity assessment -- Supplier's declaration of conformity and its supporting documentation

6.25 SA-CMM® – Software Acquisition Capability Maturity Model®

		T	

6.25.1 Aim

To benchmark and improve the software acquisition process.

6.25.2 Description

The Software Acquisition Capability Maturity Model® (SA-CMM®) is a model for benchmarking and improving the software acquisition process. The model follows the same architecture as the Capability Maturity Model for Software (SW-CMM), but with a unique emphasis on acquisition issues and the needs of individuals and groups who are planning and managing software acquisition efforts. Each maturity level indicates an acquisition process capability and has several Key Process Areas (KPAs). Each KPA has goals and common features and organizational practices intended to institutionalize common practice. In a collaborative effort among the Department of Defense (DOD), other federal agencies, the SEI, and industry, a team of acquisition experts initially developed, pilot-tested, and planned the implementation of the SA-CMM. Since much work in software acquisition process modeling had been performed by the Army, Navy, Air Force, and other federal agencies recently, this effort combined the best of that work, refined it, and used the established SW-CMM as an architectural model.

SA-CMM® Key Process Areas

Level	Focus	Key Process Areas
5 Optimising	Continuous process improvement	Acquisition Innovation Management Continuous Process Improvement
4 Quantitative	Quantitative management	Quantitative Acquisition Management Quantitative Process Management
3 Defined	Process standardization	Training Program Acquisition Risk Management Contract Performance Management Project Performance Management User Requirements Process Definition and Maintenance
2 Repeatable	Basic project management	Transition to Support Evaluation Contract Tracking and Oversight Project Management Requirements Development and Mgt Solicitation. Software Acquisition Planning
1 Initial	Competent people and heroics	

6.25.3 Sources

Refer to Bibliography: [38] Software Acquisition Capability Maturity Model® (SA-CMM®), Version 1.03.

Note: SA-CMM® is a product of:
Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890).
The Software Engineering Institute may be reached by URL http://www.sei.cmu.edu/

6.26 ISO 9000 Series – Quality Management

D	I	T	O

6.26.1 Aim

To provide organizations with a quality management framework and to allow certification of its successful implementation.

6.26.2 Description

ISO 9000 is a quality assurance standard which contains 20 high level clauses for an organization to satisfy before obtaining ISO 9000 registration. Originally made for manufacturing organizations, it can be applied to software development organizations but requires a lot of interpretation to be applicable. For this reason, ISO 9000-3 guidance for the application of ISO 9001 to the development, supply, and maintenance of software was added to address the confusion and difficulty in applying ISO 9001 to software. ISO 9000-3 contains 22 clauses written specifically for software development and these map back to the actual ISO 9001 standard consisting of 20 clauses. Although the clauses are more specific to software, they are still of sufficient high level to require further interpretation to be applicable to an organization and they do not address information technology security. Note that ISO 9000-3 guidance is limited to software where ISO 9001 and the CC are applicable to hardware in addition to software products and systems.

Compliance to ISO 9000 is achieved by independent auditors inspecting the organization's quality manual and processes and interviewing personnel. An ISO 9000 certificate is only offered to a proper organization such as a company. This differs from ISO/IEC 21827 (SSE-CMM) which can be appraised for an individual group or project within a company or an organization.

ISO 9001 covers a wider scope than the CC requirements from conception to decommissioning of a product which means that an organization looking at being ISO 9001 registered as a way of saving evaluation time will have to implement a quality system covering more areas than required for a CC evaluation. This additional work to obtain ISO 9001 may not be justified.

It is important to note that ISO 9000-3 is guidance and that the organization must satisfy the ISO 9001 requirements to achieve registration.

6.26.3 Sources

Refer to Clause 2: ISO 9000, ISO 9001, ISO/IEC 90003 (revision of ISO 9000-3).

Note 1: ISO 9000 and ISO 9001 are products of the committee:
ISO TC 176 - Quality management and quality assurance
with its subcommittees
ISO TC 176/SC 1 - Quality management and quality assurance - Concepts and terminology
ISO TC 176/SC 2 - Quality management and quality assurance - Quality systems
ISO TC 176/SC 3 - Quality management and quality assurance - Supporting technologies

Note 2: ISO/IEC 90003 is a product of the committee:
ISO/IEC JTC 1/SC 7/WG 18 Information technology - Software and system engineering - Quality management

6.27 ISO 13407 – Human Centered Design (HCD)

D			

6.27.1 Aim

To obtain through human-centred design a more usable, trainable, and supportable product, to achieve reduced security risks associated with the operation of a system.

6.27.2 Description

ISO 13407 Human-centred design processes for interactive systems is the standard produced by ISO/TC 159/SC4/WG6 that explains the benefits achieved by making the interactive systems lifecycle more human centred, and the processes required to make a lifecycle human-centred. The human-centred lifecycle process model presented in this technical report is a structured and formalised definition of the human-centred processes described in ISO 13407. ISO 13407 is applicable to software processes assessment and improvement specialists and to those familiar with or involved in process modelling.

The model presented in this document uses the format common to process assessment models. These models describe the processes which ought to be performed by an organization to achieve defined technical goals. The processes in this model are described in the format defined in ISO 15504 *Software process assessment*. Although the primary use of a process assessment model is for the measurement of how well an organization carries out the processes covered by the model, such models can also be used as a description of what is required in order to design and develop effective organizational and project processes.

The usability maturity model UMM based on ISO 13407 describes seven processes each defined by a set of base practices. The base practices are defined. A set of work products are given for each process. A summary is provided of the ISO/IEC 15504 scale for the assessment of the maturity of processes. The uses of the model are outlined. A recording form is supplied and its use described. Mappings of the base practices to processes in SPICE, CMM and SE-CMM are provided. The process model is conformant to ISO/IEC 15504.

As far as systems and software developers are concerned the use of a human-centered approach gives a more usable, trainable, and supportable product and greater client satisfaction. Human-centered design may reduce the security risks associated with the operation of a system. Human-centered processes require more investment in the early stages of the lifecycle, but have been found not only to reduce in-service costs but also to reduce development costs. In particular human-centered processes reduce the risk of unexpected changes in requirements and reduce re-work and installation risks.

The goal of the human-centered approach is to remind the developer and owner of an interactive system that the system is intended for use rather than for delivery and purchase. Human-centered processes allow developers and owners to analyze how the system will behave when it is in operation and to measure its quality and assurance in use. Human-centered processes take account of context of use, the complete environment in which the interactive system will be used. Human-centered processes deal with the total system within which software and hardware are components. Human-centered systems empower users and motivate them to learn. The benefits can include increased productivity, enhanced quality of work, reductions in support and training and improved assurance in operation.

6.27.3 Sources

Refer to Clause 2: ISO/IEC 15504-1,

Refer to Bibliography: ISO 13407 Human-centred design processes for interactive systems

Note: ISO 13407 is a product of the committee:
ISO TC 159/SC 4/WG 6 Ergonomics - Ergonomics of human-system interaction - Human-centred design processes for interactive systems

6.28 Developer's Pedigree (in general)

D			

6.28.1 Aim

To use the prior experience and success rate as an indicator for the quality of security software

6.28.2 Description

Pedigree suggests a method to determine the acceptability of evidence based on the identity of the creator(s) of that evidence using the prior success rate (i.e. track record) that an individual/organization has in developing, maintaining, operating or auditing security products and systems. Pedigree may be based on an individual's identity or on the organization that produced the evidence. Furthermore pedigree may be categorized based on roles of the individual/organization into builders, evaluators, and approvers.

Pedigree may be formalized within the ICT security community. Whether formalized or not, this pedigree is a channel of information that is currently used, albeit on a more informal basis as "trust"; many products/systems are selected based on reputation of the developer or integrator.

An option given serious consideration in some quarters is that of developer's assurance. This involves the developer performing testing and assessment in-house and making some kind of statement of assurance based on the companies internal procedures. A developer's assurance mark cannot give the same level of assurance as independent third party testing but some parties feel that establishing a scheme to recognize trusted developers may meet many commercial requirements.

6.28.3 Sources

Refer to Bibliography: [43]

Note: The formalization of the concept of "Developers Pedigree" can be found in the process assurance methods such as CMM (subclause 6.21) and ISO/IEC 15504 (subclause 6.20), in Personnel Certification (subclauses 6.36 and 6.37) and in the Suppliers Declaration of Conformity (subclause 6.24).

6.29 ISO/IEC 17025 – Accreditation Assurance

D	I		

6.29.1 Aim

The aim of accreditation assurance is to guarantee the comparability of all evaluation procedures and results, to comply with relevant standards and to guarantee objectivity and neutrality.

6.29.2 Description

The guarantee the comparability of all evaluation procedures and results, to comply with relevant standards and to guarantee objectivity and neutrality: these principles form the basis for accreditation assurance. The accreditation assurance procedure requires evaluation facilities to furnish proof of compliance with the conditions and qualification requirements.

According to ISO/IEC 17025 the requirements for accreditation are as follows:

a) 1. Compliance with the relevant parts of ISO/IEC 17025 (including general evidence of competence for the overall field of ICT security),

b) 2. Proven technical competence for a specific field of evaluation (several fields of evaluation if applicable).

The accreditation procedure thus comprises a Basic Accreditation (compliance with the requirements further to Clause 1) and at least one licensing procedure (compliance with the requirements further to Clause 2).

An accreditation may be supplemented by licensing procedures for additional fields of evaluation.

Licensing Field 1	Licensing Field 2	Licensing Field n
Basic Accreditation in accordance with ISO/IEC 17025		

Accreditation Procedure

Evaluation facilities run by natural or legal persons under private law may be accredited by an Accreditation Agreement between the accreditation body and the operator. The precondition for this is that these evaluation facilities not be involved in development, manufacture or marketing of products to be evaluated. Thus, in principle, this does not preclude the possibility of accreditation of so-called vendor laboratories.

As basis of the accreditation process the European Standard ISO/IEC 17025 specifies general criteria for the technical competence of testing laboratories including calibration laboratories, irrespective of the sector involved. It is intended for the use of testing laboratories and their accreditation bodies as well as other bodies concerned with recognising the competence of testing laboratories. This set of criteria is supplemented when applied to a particular sector of ICT-security.

Note: The independent third party evaluation following the Common Criteria 15408 are conducted by accredited and licensed evaluation facilities following the requirements of ISO/IEC 17025.

6.29.3 Sources

Refer to Bibliography:
ISO/IEC 17024 Conformity assessment — General requirements for bodies operating certification of persons
ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories

Note: ISO 13407 is a product of the committee:
ISO/CASCO WG 24 Committee on conformity assessment - Assessment and accreditation

6.30 ISO/IEC 13335 – Management of information and communications technology security (MICTS)

	I	T	O

6.30.1 Aim

To give to management general guidance on assessing and managing security risk.

6.30.2 Description

ISO/IEC 13335 consists of a series of standards and technical reports for guidance, not solutions, on management aspects of information and communications technology (ICT) security. Those individuals within an organization that have responsibility for ICT security should be able to adapt the material in ISO/IEC 13335 to meet their specific needs. The main objectives of ISO/IEC 13335 are:

1) to define and describe the concepts associated with the management of ICT security,

2) to identify the relationships between the management of ICT security and management of ICT in general,

3) to present several models that can be used to explain ICT security, and

4) to provide general guidance on the management of ICT security.

MICTS describes the underlying concepts behind risk assessment and risk management, including the terminology and the overall process of assessing and managing risks.

MICTS was developed to manage information security problems holistically, addressing issues such as technical, physical, procedural and administrative controls. MICTS not only provides a basis to assist an organization in developing and enhancing its own information security architecture; it also aims to establish commonality between organizations.

MICTS provides a framework for managing ICT security. MICTS discusses high level concepts about ICT security management and introduces general requirements and techniques for risk analysis and management.

The risk management process defined in the future Part 2 of MICTS requires that suitable controls are implemented and suggests specific controls selected from standards such as ISO/IEC 17799 or the IT Baseline Protection Manual.

ISO/IEC 13335 MICTS is currently in the course of revision and partial conversion of the previous and current ISO/IEC 13335 GMITS (Guidelines for the management of IT Security) from a Technical Report into an International Standard. When this process is complete, it will consist of the following parts, under the general title *Information technology — Security techniques — Management of information and communications technology security*:

Part 1: Concepts and models for information and communications technology security management;

Part 2: Techniques for information and communications technology security risk management.

ISO/IEC 13335-1:2004 cancels and replaces ISO/IEC TR 13335-1:1996 and ISO/IEC TR 13335-2:1997. It also includes ISO/IEC TR 13335-5:2001.

ISO/IEC 13335-2 will cancel and replace ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000.

The following parts of ISO/IEC TR 13335 presently remain under the general title *Information technology — Guidelines for the management of IT Security*:

Part 3: Techniques for the management of IT security;

Part 4: Selection of safeguards;

Part 5: Management guidance on network security.

6.30.3 Sources

Refer to Clause 2: ISO/IEC 13335-1, ISO/IEC TR 13335-2, ISO/IEC TR 13335-3, ISO/IEC TR 13335-4, ISO/IEC TR 13335-5, ISO/IEC 17799.

Refer to Bibliography: [33] IT Baseline Protection Manual.

Note 1: ISO/IEC 13335 is a product of the committee:
ISO/IEC JTC 1/SC 27/WG 1 Information technology - Security techniques - Requirements, security services and guidelines

Note 2: At the time of the release of this Technical Report, ISO/IEC 13335 is in a major revision including a restructuring and name change. Previously entitled "Guidelines for the management of IT Security", new parts of ISO/IEC 13335 now are titled "Management of information and communications technology security", abbreviated "MICTS".

6.31 BS 7799-2 – Information security management systems – Specification with guidance for use

			O

6.31.1 Aim

To establish the requirements for setting up and managing an effective Information Security Management System (ISMS).

6.31.2 Description

BS 7799-2 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of an organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

An ISMS developed using BS 7799-2 takes in account an organization's overall business risks to define adequate and proportionate security controls to protect information assets and give confidence to customers and other interested parties. This should maintain and improve an organization's competitive edge, cash flow, profitability, legal compliance and commercial image.

An organization must identify and manage its many activities in order to function effectively. Any set of activities using resources can be considered to be a process that transforms inputs into outputs. Often the output from one process directly forms the input to the following process. The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

BS 7799-2 uses the process approach to encourage its users to emphasize the importance of:

a) understanding business information security requirements and the need to establish policy and objectives for information security;

b) implementing and operating controls in the context of managing an organization's overall business risk;

c) monitoring and reviewing the performance and effectiveness of the ISMS;

d) continual improvement based on objective measurement

The underlying process model used by BS 7799-2 is the "Plan-Do-Check-Act" (PDCA) model found in many other process standards.

6.31.3 Sources

Refer to Bibliography: [53] BS 7799-2:2002 Information security management systems — Specification with guidance for use.

Note 1: BS 7799-2 is a product of:
BSI (British Standards Institution), Customer Services, 389 Chiswick High Road, London W4 4AL, United Kingdom
BSI may be reached by URL www.bsi-global.com

Note 2: BS 7799-2 also was published as national standard AS/NZS 7799-2: 2003 in Australia and New Zealand, refer to (www.standards.com.au)