E C M A

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

Secure Information Processing versus the Concept of Product Evaluation

---

ECMA TR/64

December 1993

Free copies of this document are available from ECMA,
European Computer Manufacturers Association,
114 Rue du Rhône - CH-1204 Geneva (Switzerland)

Phone: +41 22 735 36 34 Fax: +41 22 786 52 31
X.400: C=ch, A=arcom, P=ecma, O=genevanet,
OU1=ecma, S=helpdesk
Internet: helpdesk@ecma.ch

E C M A

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

Secure Information Processing versus the Concept of Product Evaluation

---

ECMA TR/64

December 1993

Brief History

In September 1990 the European Commission announced the "Harmonized IT Security Evaluation Criteria" ITSEC. The governments of France, Germany, Great Britain and the Netherlands had agreed on a common set of criteria for IT security evaluations. The European Commission proposed these criteria for usage within the European Community.

The ITSEC deviated substantially from the US TCSEC, (Trusted Computer System Evaluation Criteria) commonly known as Orange Book, the de-facto standard since 1983.

This created a problem for all world-wide operating computer manufacturers who were faced with two problems:

- to which set of criteria they should develop their products, and
- if a product was developed to one set of criteria, would a customer in a country outside the influence of this set accept the product and its evaluation.

Users of IT products were confused because they did not know, which set of criteria would meet their requirements.

The European Computer Manufacturers Association, ECMA, was alerted by its members, mostly world-wide operating companies. The ECMA General Assembly therefore decided already in December 1990 to establish an ad hoc group on Security. This group started its work in March 1991. Later in 1991 the group became ECMA/TC36 and then TC36/TG1.

The group decided to address the problem twofold:

- First, to write an ECMA Technical Report which positions security evaluations in the context of secure information processing in order to highlight the fact that an evaluated product or system can only guarantee security, when the total system, its environment and its operation are secure.
- Second, to develop an ECMA Standard for a functionality class which defines a minimum set of requirements for commercial application. This class was called "Commercially Oriented Functionality Class" or COFC. It distinguishes itself from the Orange Book and respective ITSEC functionalities, which are more tuned towards military and government requirements for confidentiality of classified information. Assurance criteria, as addressed on the Orange Book and ITSEC, have not been taken into account.

Both, the Technical Report and the Standard are intended to be a contribution to the ongoing harmonisation process. They highlight commercial requirements, which call for an appropriate evaluation process, ranging from vendor self-testing to accredited third party testing, and a minimal set of functional requirements, which satisfy commercial needs.

Adopted as an ECMA Technical Report by the General Assembly of December 1993.

Table of contents

1 Scope

This paper examines the value of security evaluation criteria and the accompanying evaluation process in a commercial environment. It argues this question must be approached systematically within the context of a full complement of security measures so as to maximize the value from associated investments. It then focuses on the potential benefit specific to evaluations and makes recommendations as to the processes for creating an IT security program with special emphasis on security evaluations.

Annex A is a review of the history and current status of formal evaluation programs. Readers unfamiliar with this topic may wish to read this first.

2 References

ECMA-138	Security in Open Systems - Data Elements and Service Definitions (1989)
ECMA-205	Commercially oriented functionality class for security evaluation (COFC) (1993)
ECMA-TR/46	Secutiry in Open Systems - A Security Framework (1988)
ECMA-apa	Auhentication and Priviliege Attribute Security Application with Related Key Distribution Functions (in preparation)
/Lipner 91/	Steven B. Lipner, "Criteria, Evaluation and the International Environment: where have we been, where are we going?". Proceedings of the IFIP TC11 Seventh International Conference on Information Security: IFIP/SEC'91 Brighton, UK, 45-17 May 1991. Edited by David T. Lindsay. Wyn L. Price. lSBN: 0 444 89219 2.
/GIS 91/	Information Technology Security Evaluation Criteria - Harmonized Criteria of France, Germany, the Netherlands, the United Kingdom. Provisional. Version 1.2 German Information Security Agency, Bonn, 1991.
/DOD 85/	Department of Defense: Trusted Computer Systems Evaluation Criteria. DOD 5200.28-STD, USA, 1985.
/Neumann 91/	Peter G. Neumann and Contributors: Risks to the Public. ACM Software Engineering Notes. Vol. 46, Jan. 1991.
/Le Roux 90/	Yves Le Roux, "Technical Criteria for Security Evaluation of Information Technology Products", Digital Equipment Corporation 1990
/ECTEL. EUROBIT/	Conformity Testing for IT Products, Second Edition 1992.

3 Acronyms and abbreviations

DoD	Department of Defense (USA)
COFC	Commercially Oriented Functionality Class
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
IEC	International Electrical Committee
ISO	International Standards Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	IT Security Evaluation Methodology Manual
JTC1	Joint Technical Committee 1
NIST	National Institute for Standardization and Technology (USA)
NSA	National Security Agency (USA)

TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TR	Technical Report
SC27	ISO/IEC JTC1 SC (Sub Committee) 27 "IT Security"
WG3	ISO/IEC JTC1/SC27 WG (Working Group) 3 "IT Security Evaluation Criteria"

4 Introduction

We assume the bank will keep our money in a safe, use armoured vehicles for transport, only permit authorized people to complete a transaction, and audit all transactions. Furthermore, we require banks to adhere to accepted banking practices and open their books to independent review. Doing this well can give one bank a competitive edge over its rivals. Information is the currency in a commercial enterprise, and information management is critical to its competitive position. How to protect information and the potential role of formally evaluated systems is the subject of this paper.

In the past 30 years we've seen computer technology revolutionize how we manage information -- and it's not over yet. Businesses can have access to the data they need: it is current, malleable, and easily disseminated. Technology is reducing the cost to process data and introducing.new methodologies to manipulate data, e.g. workgroup applications. Staying on top of these changes and adopting the right match of technology to the business need is high on most managers' agendas.

But new technologies introduce new risks: the same capabilities that gives us current, malleable, and easily disseminated information expose that data to new forms of attack. We've come to rely on data being shared for update and access, on networks for inter-and intra-company connections, on PCs, and on dial-up lines. The typical enterprise has an IT environment composed of many computers.

These computers range in size and location. It is no longer safe to assume that the "mission critical" applications are confined to the data centre, nor that they run over a single vendor's equipment. Networks are pervasive, providing connectivity not only within workgroups and across the enterprise, but also to external data sources, suppliers, and customers.

Electronic information is a company asset and protecting it must be woven into the enterprise's asset-protection plan. In the 60's, we could lock computers in specially built rooms; this approach is woefully inadequate today.

We've all experienced the horrors of the system being down. Not only have we come to depend upon the availability of our systems, but we must also guard against unauthorized or inadvertent modification (information integrity) or disclosure (confidentiality) of the data. Thus we arrive at the three tenants of Security: **Confidentiality**, **Integrity** and **Availability** ... or CIA.

5 Approaching Security: System perspective, Balance, Feedback

5.1 System perspective

Information is subject to a number of threats from a number of sources. "Acts of God" and acts of war or civil unrest have dealt the dramatic blows. Employees make mistakes and miscalculations a few commit fraud, abuse authority, or vandalize property. Outsiders may target an enterprise for vandalism, fraud, or espionage.

By their very nature, accidents can hit anywhere, any time. Intelligent malicious attacks will seek out the path of least resistance -- it is often via a dial-up line, but may be by sifting through the wastebaskets. Effective protection involves adopting a structured management approach to security where policy and investment decisions take all risks into consideration. Since this approach involves many facets of the business, it is important that those in charge of security have enough authority to enforce the policies. In practice, this means a security organization reporting to top management. Identifying the **Security Organization** is the first step in managing security.

Before defining the IT security strategy, it is necessary for the Security Organization to address security from a global viewpoint. Answering such questions as listed result in defining the **Corporate Security Policy**.

- What are the assets?
- What is the value of the assets?

- Who is allowed access or knowledge of the assets?
- How vulnerable are the assets?
- Which threats have to be anticipated?
- What is the impact of failure?
- Which organizational measures are necessary to protect the assets?
- What regulations, rules, processes are needed to ensure security?

This policy is a set of rules and practices regulating how assets are managed, protected, and distributed. It typically covers people, buildings, material, equipment, and information; it includes such things as personnel policy, business planning, facility planning, IT strategy, and operational procedures.

The Corporate Security Policy is the starting point for the IT security strategy. It is important that top management issues the Corporate Security Policy in order to demonstrate its commitment. This is critical since such policy implies changing behaviours at every level, and a failure in IT security can have serious financial repercussions.

The following steps then lead to a strategy for managing IT security -- a clear demonstration that managing IT security is much more about good business management than about technology.

- Publish the corporate IT security policy.
- Analyse business needs and risks. This is achieved through a process of needs identification, threat assessment, vulnerability assessment, and risk analysis.
- Assess impact on current or expected situation.
- Develop security policies, standards, countermeasures, and contingency plans. This step constitutes the IT security program and involves choosing a set of safeguards that balances with ones risk acceptance decisions.
- Implement IT security program, not forgetting user training.
- Ensure compliance.

5.2 Balance

Security is not about achieving 100 percent. Getting the balance right is the key to good security management; it is a game of trade-offs. There are three main factors to consider when making an investment in a security measure:

- Cost
- Productivity (fullness of functionality and ease-of-use)
- Security (features and assurance)

The paradox is that you want all three, but any two pull against the third! You can have a cheap solution at maximum security (unplug all the machines) but you won't be pleased with the functionality; maximum security at full functionality would be prohibitively expensive; while ignoring security minimises initial investment, but maximises your risks.

Another paradox is that people think of IT security as managing technology, hence tend to focus on the technical aspects. They may even invest in technical solutions at the cost of other aspects; for example, requiring (hence investing in) formal security evaluations of products at the cost of sufficient investment in user training.

Investment is limited in every enterprise. Only people understand the business dynamics and can judge which investments will yield the greatest benefit. This analysis is best approached as a team: involving users as well as management, often aided by external consultants.

Today there is an investment imbalance, with more going into the scrutiny, methodology, and assurance of product security compared with that spent in managing the security of operations. We should insist that any innovations in security evaluations amend this balance.

5.3 Feedback

Achieving and maintaining balance depends on listening to experience and incorporating its lessons into our guidelines, policies, and procedures. IT security evaluation criteria and any associated evaluation process fall into this category. The quality of any guideline, policy, or procedure is directly proportional to how much real experience, from a variety of sources, it incorporates and how adaptive it is to changing conditions. The rest of this paper will look at the value of IT security Evaluation Criteria and associated evaluation processes as mechanisms for encapsulating and passing on such experience.

6 Security Evaluations: the practice

Annex A describes the concepts behind formal evaluations as exemplified by TCSEC and ITSEC. The next paragraphs examine the practice, looking at the following limitations:

- Ambiguity
- Time delay
- Maintenance and re-evaluations
- Secretive/closed process
- Non-productive nature of the investment
- Real use
- Cost

Any development manager who has taken a system through a formal evaluation can attest to seemingly endless disputes around the interpretation of the requirements: To what granularity must one take the definition of an "object" for requiring access controls and auditing; e.g. is inter-process communication an object? Why does a mechanism that passed as C2 in one evaluation, fail in a later one? What the original authors regarded as clearly stated requirements have proven ambiguous in practice, especially as applied by evaluators now far removed from their origin. TCSEC addresses this in a number of subsequent "interpretations". It is not guaranteed (in fact unlikely) that a system that passed in one year would be judged the same in a subsequent evaluation. Vendors term this phenomenon as "criteria creep."

The evaluation process performed by a third party imposes a layering of paperwork, checking, bureaucracy, and mistrust on the vendor's development. All this adds time to the development process; time resulting in delay. The TCSEC experience is that by the conclusion of the process, the vendor is likely shipping a version succeeding the one under evaluation. The requirement for a distinct certification process of the evaluation results (by yet a different authority) can only result in extra delay in publishing the official evaluation report.

Software maintenance poses another problem. If the concerned components are security relevant, each software change requires some re-evaluation. Re-evaluation is expensive, especially if the expertise of the initial evaluation team is no longer available. Today's experience is that evaluated products are not usually maintained; thereby compounding the problem of obsolescence observed in the previous paragraph.

TCSEC was subject to extensive public review during development. But the "interpretation process" is often triggered by proprietary aspects of the vendor's product and conducted behind closed doors. The resulting total set of interpretations is not visible outside NSA. Review comments have also sited secrecy concerns with the draft ITSEM. It's not enough for requirements to be unambiguous, they must also be exposed to the scrutiny of public review.

The nature of the evaluation investment is highly non-productive. In practice the product development team must invest heavily in the training of and documentation for the evaluation team on their product. Multi-purpose commercial operating systems are large and complex. This is a nontrivial investment; one that does enhance the product functionality. More hours are spent in discussion and debate. Admittedly this sometimes results in correction of faults, but more often is further justification of the implementation. Also there is no guarantee the expertise will be maintained by the evaluator and certainly acts as an inhibitor to changing evaluation teams. (With ITSEC a vendor can choose the evaluation facility.) The process of certifying of the evaluation results can only be viewed an example of "checkers checking on the checkers" rather than contributing to product functionality.

Few (if any!) commercial sites use products as they were evaluated. Not only do their requirements for functionality push them to use other than the evaluated versions, but applications servicing multiple users (e.g. databases or Office systems) may need to override the operating system controls. Furthermore, TCSEC evaluations exclude general networking facilities, as does the ECMA draft for an ITSEC commercial functionality class. (And for very good reason: attempts to define network criteria have proven too restrictive on vendor implementation and customer deployment. We suspect their heterogeneous, dynamic nature will never lend itself to a point-in-time, static evaluation).

The experience of all the above is that security evaluations are expensive and do not keep pace with product development nor real user environments. Vendor cost (with reports running from 10-40% of the development cost, or millions of dollars on every evaluation) must be passed on in the price, and the value-for-money equation suffers as a consequence.

On the positive side, there is now general C2 awareness. "C2 systems are the workhorses of commercial computing. They incorporate user identification and authentication mechanisms, auditing, discretionary access controls, and controls over storage residues ... They are thus well-suited to the vast majority of commercial multi-user applications." (ref. Lipner 91).

The evaluation process has therefore not only to check if the criteria are met, but also to judge the development process against good programming practices. Security functions are today engineered into products, rather than added on as an afterthought. Hence the mechanisms no longer stand alone, but are integrated in their design. Unfortunately, all this at great cost.

7 The Value of Formal Evaluations in the Commercial Market

IT security evaluation criteria attempt to capture the characteristics that enable secure management of the associated systems. Today the TCSEC "C2" rating is widely recognised as a baseline for commercial systems. "C2" has changed the mind set of software developers.

Almost all major vendors offer systems aimed at satisfying these criteria, even when they do not undertake formal evaluations. One could argue that the very success of C2 as a baseline has drawn attention to its shortcomings and given impetus to defining a commercial functionality class under ITSEC.

The C2 experience also demonstrates that when a standard is widely recognised as providing value, it makes good business sense to follow it -- even without coercion. It then seems to follow that improving the accepted baseline would improve the security potential of our operations. Such an undertaking has two components:

- Improving the criteria themselves -- most effectively by incorporating feedback from both users and vendors, always mindful of the cost : benefit balance.
- Getting wide acceptance for any new classifications of security criteria -- in today's global market, this must mean world-wide recognition.

International standards bodies are working on this task; it's not easy. In ECMA/TC36 our recommendation is to bound the scope of the task, demonstrate improved value, then build from there. The first step is to get world-wide recognition for an updated definition of security for commercial multi-user operating systems. ECMA/TC36 is making a contribution towards this goal.

Achieving this objective would result in benefits for consumers and vendors alike. It would give consumers an updated and hopefully more reliable benchmark for comparing vendor offerings. Vendors would get a well-defined set of user requirements applicable across a large market segment -- extremely valuable information.

One caution: today we lack adequate consumer involvement. Very much needed is a public forum where users and vendors come together to share experience, test the balance, and set priorities. Establishing an effective feedback mechanism would be a greater contribution to secure information processing than a hundred formal evaluations!

The evaluation controversy has not been so much with regards to the criteria, but with the process for verifying adherence. The consumer benefit is in having security features built into products; hence vendors would like to see their associated investment directed towards engineering these features. Instead, if formal evaluation is undertaken, a disproportionate amount of the cost (surely reflected in the price) is spent in proving adherence to a third party, predicated upon an operating environment that may never occur outside the laboratory. It's difficult to argue value-for-money.

Therefore another advantage of well-defined criteria is that conformance testing should be a straight forward exercise, one where the vendor plays a greater role. On the other hand, when criteria are ill-defined and ambiguous, any evaluation process (including one by a third party) will be arbitrary ... and potentially very costly.

Ideally the vendor should be able to verify adherence to well-defined criteria as part of the development process. This could be documented and communicated in a "first party evaluation." Competitive pressures and existing consumer safeguards against supplier claims are powerful motivations for honesty. (The legal profession is well-poised in the event of a false product claim resulting in a security breach.) Much of formal evaluation work is actually concerned with quality assurance. There is evidence that third parties can play an important role in quality assurance.

However, multiple quality control programs fragments a vendor's focus on quality. Hence our recommendation is to look to an existing quality program, where ISO 9000 seems to be the leading international contender, to fulfil the need

in security evaluations. This might take the form of periodical audits of the first-party evaluation documentation, but need not review all the documentation for all the products -- better to achieve 90% of the value at 10% of the cost. The current draft of ITSEM seems not to take such a pragmatic approach and would lead to the costs outweighing the benefits.

Well-defined, commercial-oriented security criteria define a security baseline for products. But products are only components of any system; product security is only a component of any IT security plan. Furthermore, since operating environments differ, vendors must offer a range of valid settings for most security functions. Adjusting these parameters can only be accomplished by the customer, who alone can judge the actual threats in the environment. Systems with improperly set security parameters pose a security risk.

Security criteria can also only approximate a minimum standard. Any enterprise, based upon its risk assessment, may choose to implement greater security measures, from stricter operating procedures to additional technology. When cost justified, it may even undertake a system accreditation. Our thesis is that the most neglected and greatest opportunity (i.e. the greatest return on the associated investment) is in improving operating procedures. The contribution of using evaluated products is rather limited compared to the potential misuse by authorized users, possibly exacerbated by improperly configured or administered systems. It is well known that most security violations stem from insiders operating within the bounds of their privileges, yet evaluations can only effectively check on unauthorized/external attacks.

8 Conclusions

At their best, security evaluation criteria coupled with a cost-sensitive evaluation process is a means of passing on collective experience with IT security. Grouping security criteria into an internationally recognised commercial classification, would provide a useful baseline and benchmark for comparisons.

For evaluations to be cost effective, criteria must be unambiguous thereby facilitating effective first-party testing with optional third-party review of the results, preferably as part of an integrated quality program. Associated costs must be monitored and justified. Also required is a responsive and open (public) process for proposing changes to the criteria or evaluation process so they can keep pace with a changing technology and business environment. The goal of product evaluations must become more modest than in either TCSEC or ITSEC. It has to be viewed as a service contributing to, not guaranteeing, security.

Deploying products containing well-designed and engineered security features does not ensure secure information processing. To focus investment on product evaluations disproportionately to other aspects of operations constitutes an example of (mis)applying technology to what is essentially a management problem. In the extreme, this could result in lulling an enterprise into a false sense of security; thereby increasing its security risks.

Security must be approached from a systematic enterprise-wide perspective. An enterprise must seek to achieve a balance of manageable risk and safeguards, justified by examining the business objectives. It must adopt monitoring procedures that mirror this holistic approach and feedback recommendations for change to its IT security policy.

Annex A

The Concept of Security Evaluations - A Tutorial

A.1 Introduction

An enterprise with a need to protect its information, has to address many areas, that influence security. It starts from a Corporate Security Policy and ends with the implementation and follow-up of an IT security Programme. The central point of the IT security Programme is the installed IT equipment and its surrounding organisation. Protection mechanisms have to cover the whole system and its stored information.

A system is comprised of many parts: hardware units, software packages, communication links etc. Many of them can be seen as products, often bought as IT products from different vendors. Security has always to be the security of a complete system. To ensure total system security the customer may decide for a complete system evaluation. However, prior to a total system evaluation it is advisable to use as many evaluated parts as possible. Some are already available of the shelf. An operating system, could be a typical example. If the operating system is evaluated, it has only to be checked that the evaluation has covered the requested security functions and was done with the necessary level of assurance. The usage of evaluated products within a system does, however, not necessarily mean that the whole system is secure. It is only a step towards system security.

Some users, primarily in the defense industries, have turned to formal security evaluations of IT products to increase their confidence in the security of their IT operations. Historically these evaluations concentrated on ensuring confidentiality, i.e. the prevention of unauthorized disclosure of information. The work in this area was pioneered by the US Department of Defense in a publication called the Trusted Computer System Evaluation Criteria, or TCSEC, in 1983, better known as the "Orange Book".

But the TCSEC process was found deficient in a number of areas:

- In its emphasis on confidentiality, many felt the TCSEC neglected other aspects of security, namely integrity and availability.
- The "levels of security" in the TCSEC bundle provisions for functionality with the degree of confidence in the implementation. For example, there is no provision for a product requiring only minimum functionality, but perhaps a very high level of assurance in its implementation.
- The TCSEC are product oriented and not well suited for system evaluation.
- The evaluation body is the US National Computer Security Center and only US vendors can qualify for evaluations.

These deficiencies gave rise to a number of other security evaluation standards and processes being adopted by other countries.

The proliferation of standards and processes was recognised as a deterrent to meeting the requirements of a single European market. Representatives of France, the Federal Republic of Germany, the Netherlands, and the United Kingdom agreed to work on a project to harmonise their respective criteria as a basis for forming a single European standard. This project is called the European IT Security Evaluation Criteria, or ITSEC.

The most recent development is that the US, Canada, and Europe are investigating whether they can harmonise their respective efforts. Contributions have been made to ISO/IEC JTC1/SC27 WG3.

The following explains the basic concepts behind TCSEC and ITSEC and their associated evaluation processes. It also discusses the path to world-wide harmonization.

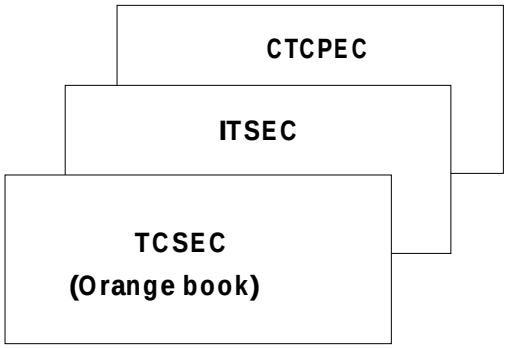

Figure A.1 - IT security criteria

A.2 Availability, Integrity, Confidentiality

Often people believe that "security" means "confidentiality", i.e. the prevention of unauthorized disclosure of information. This assumption stems from security issues of about a decade ago, where indeed the main issue was to keep information secret. It was of prime importance in national defense matters.

Meanwhile commercial enterprises as well as governmental institutions use data processing, fully integrated in the business process and connected to transmission lines and networks. The increased complexity tends to make systems more vulnerable. To meet all security requirements, "Integrity" and "Availability" are of equal importance as "Confidentiality", sometimes even of higher importance, if we only think of information services, where the information is not confidential, but instant availability and integrity are vital.

An evaluation of products and systems should therefore include integrity (the prevention of unauthorized modification of information) and availability (the prevention of unauthorized withholding of information or resources).

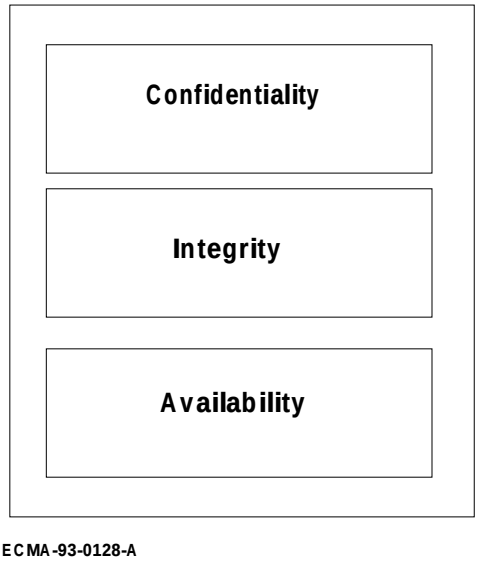

Figure A.2 - IT security

A.3 Security Target

Before starting a security evaluation, the evaluation requestor (sponsor) has to define which threats the system or product shall withstand. This investigation has to take the environment (real or assumed) into account, as well as the security objectives and the level of assurance. Both derived from the security policy. All this together allows to define the security target. The security target is product dependent. The purpose of the security target is to provide a baseline

against which the TOE (Target of Evaluation) can be evaluated. Security target and TOE are ITSEC terms. The Orange Book does not need the term security target since, it is implicit to its classes (see 8.1).

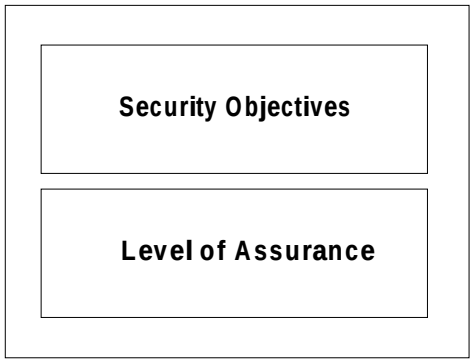

Figure A.3 - Security target

A.4 Protection Profile

The protection profile is a new term presently under discussion. A protection profile is an abstract specification of the security aspects of a needed IT product. It is product independent, describing a range of products that could meet this same need. Required functionality and assurance are bound together in a protection profile, with a rationale describing the anticipated threats and expected mode of use. The protection profile specifies requirements on the design, implementation, and use of IT security-capable products.

Protection profiles are developed by users, the government, or vendors. There may be many profiles, reflecting different needs, and a single profile may apply to many products.

The various profiles can be put in a registry. A nicely filled registry would allow vendors to develop products to certain profiles. It would allow a user to select a profile that meets his need and use it as Security Target for an evaluation of his product or system.

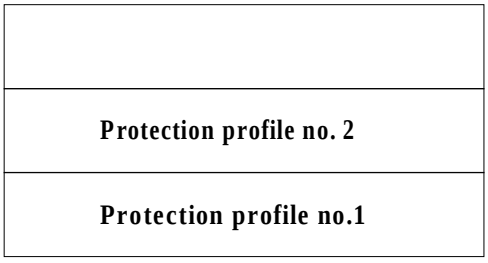

Figure A.4 - Registry of Protection Profiles

A.5 Functional Criteria

Each enterprise or institution should have a Corporate Security Policy. This policy is a set of rules and practices that regulate, how assets, including sensitive information, are managed, protected, and distributed within the organisation. From the Corporate Security Policy one can derive those instructions, rules and practices, that regulate the secure processing of sensitive information and the use of hardware and software resources of an IT system. This leads to security objectives and security enforcing functions, that the IT system should provide.

The list of figure A.5 shows, how the Security Objectives and needed Security Enforcing Functions are developed.

Figure A.5 - IT Security Policy

Most commonly used groupings (generic headings) of Security Enforcing Functions are listed in figure A.6.

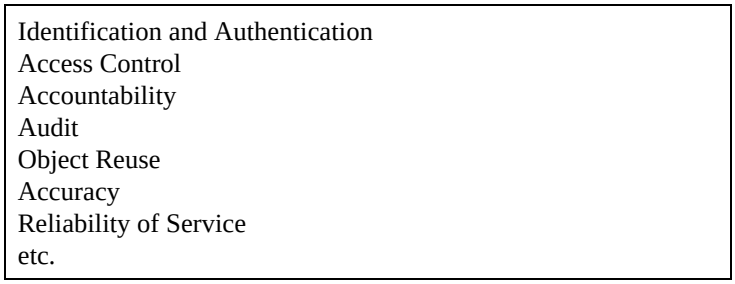

Figure A.6 - Examples of Security Enforcing Functions

A functional requirement does not normally specify a certain mechanism for implementation. Only in rare cases this might be necessary. On the other hand, a level of strength of evaluation must be specified. This is done by specifying a level of defined Assurance Criteria.

A.6 Assurance Criteria

Assurance Criteria help the evaluator to check the correct implementation of the security enforcing functions and their effectiveness.

The Orange Book (TCSEC) defines assurance criteria which are hierarchically designed and described in classes C1 to A1, while ITSEC defines equivalent assurance criteria as levels E1 to E6. The ITSEC levels are independent of any security enforcing functions. The Orange Book connects certain functions with the levels of assurance.

TCSEC	ITSEC	Required input for evaluation (example)
C1	E1	Informal description of the security architecture
C2	E2	E1 + Informal description of the detailed design. Library of test programs. Configuration control.
B1	E3	E2 + Detail design and source code.
B2	E4	E3 + Formally specified model of security. Semiformal description of architecture and detailed design
B3	E5	E4 + Vulnerability analysis based upon the source code
A1	E6	E5 + Formal description of the security architecture.

Fig. A.7 - Assurance Criteria

A.7 Predefined Functionality Classes

Only a small number of organisations and enterprises will consider a security evaluation for their total IT installation, since the high cost and long lead time of an evaluation have to be economically justified. But it is very likely that vendors will try to meet customer requirements and provide evaluated products.

In this case, the actual environment and its threats are not known. An assumption has to be made. The IT product can then be evaluated against this assumption. One can even go one step further and develop a set of security requirements for an assumed environment and independent of a product or system.

ECMA/TC36 and other standardisation bodies are presently working on such pre-defined functionality classes for specific areas. For example a need exists for an Commercial Functionality Class which meets the requirements of the commercial world. Once the class is defined or even standardised, vendors can evaluate their products to this class. A customer, buying this product, has assurance that it meets the defined requirements.

A.8 The Evolution of Security Evaluation Criteria

A.8.1 The Orange Book (TCSEC)

The "Trusted Computer System Evaluation Criteria" book, called "The Orange Book", because of the colour of its cover, was first published 1983 by the Department of Defense of the USA. Since then it was the base for security evaluations performed by the NSA (National Security Agency), and controlled by the DoD.

The need for evaluated products came first from the military side. The prime emphasis was to ensure that sufficient confidentiality was provided.

The Orange Book is based on a hierarchy of Functionality Classes, called C1, C2, B1, B2, B3, A1. Each class bundles defined functionalities with assurance criteria. C1 is the lowest class. C2 is C1 plus additional functions and a higher level of assurance. B1 is C2 plus additional functions and a higher level of assurance and so on. During the period since 1983, several hundred products were evaluated according to Orange Book Criteria.

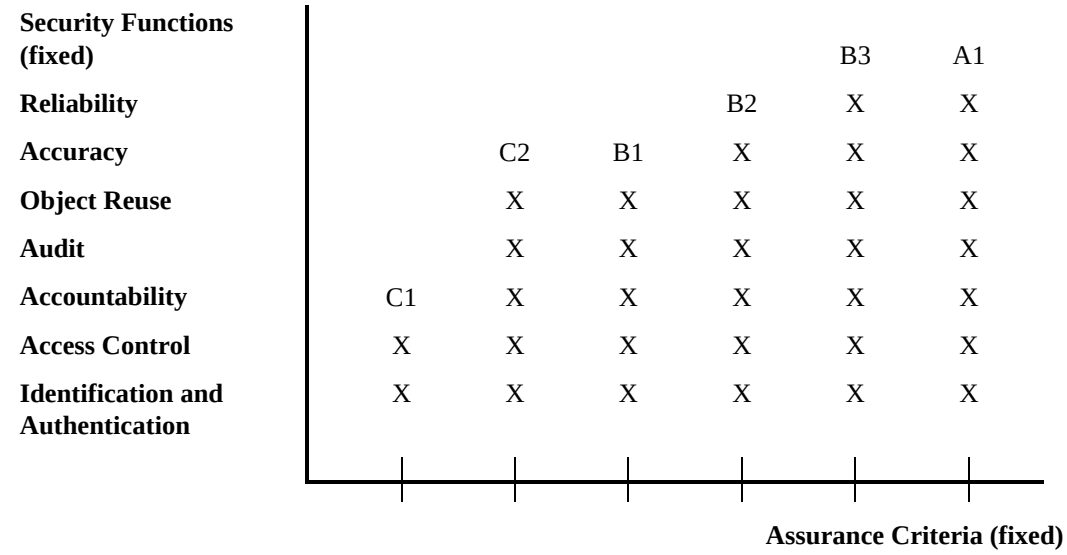

Figure A.8 - Orange Book Classes

A.8.2 The European Criteria (ITSEC)

France, Germany, the Netherlands, and the UK had developed sets of criteria for usage within their countries. Envisioning the Common European Market, they decided to harmonise their criteria. This initiative was picked up by the Commission of the European Countries for harmonization within Europe. The first document of harmonised criteria, called ITSEC (Information Technology Security Evaluation Criteria) was published in May 1990 as draft. After public discussion, a new version 1.2 is available since June 1991. This version is now being tested in a 2-year trial period, as part of the European INFOSEC program. A final version 2.0 is expected to be published at the end of 1993, taking the results of the 2-year trial period into account.

ITSEC took major elements from the Orange Book, but is unfortunately not harmonised with the Orange Book. In addition to the Orange Book it was extended to include Integrity and Availability and is applicable to products and systems. Its design is open to define functionalities. This was achieved by a strict separation of functional criteria and assurance criteria. Pre-defined Functionality Classes may be chosen for an evaluation.

In ITSEC the assurance criteria are fixed on a scale starting from E1 to E6, while the security functions must be defined for each evaluation. E0 means inadequate assurance.

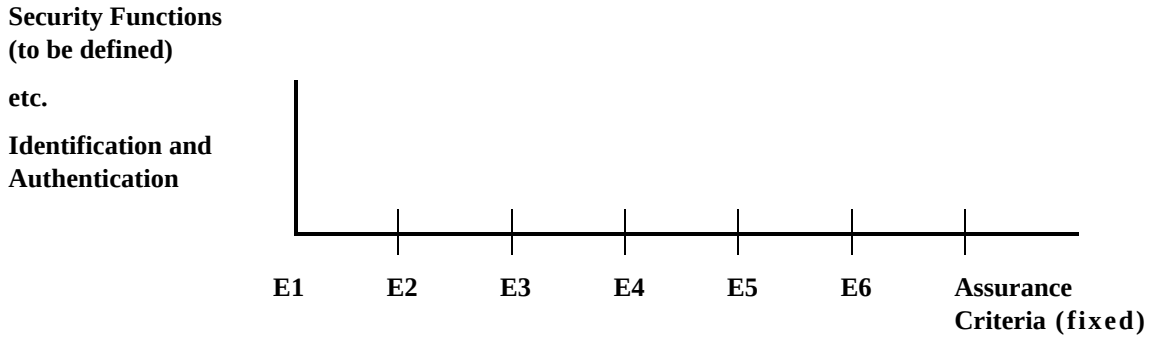

Figure A.9 - ITSEC Assurance Scale

This scheme allows to map the Orange Book classes into ITSEC pre-defined classes. Mapping and standardisation as pre-defined classes is presently under investigation.

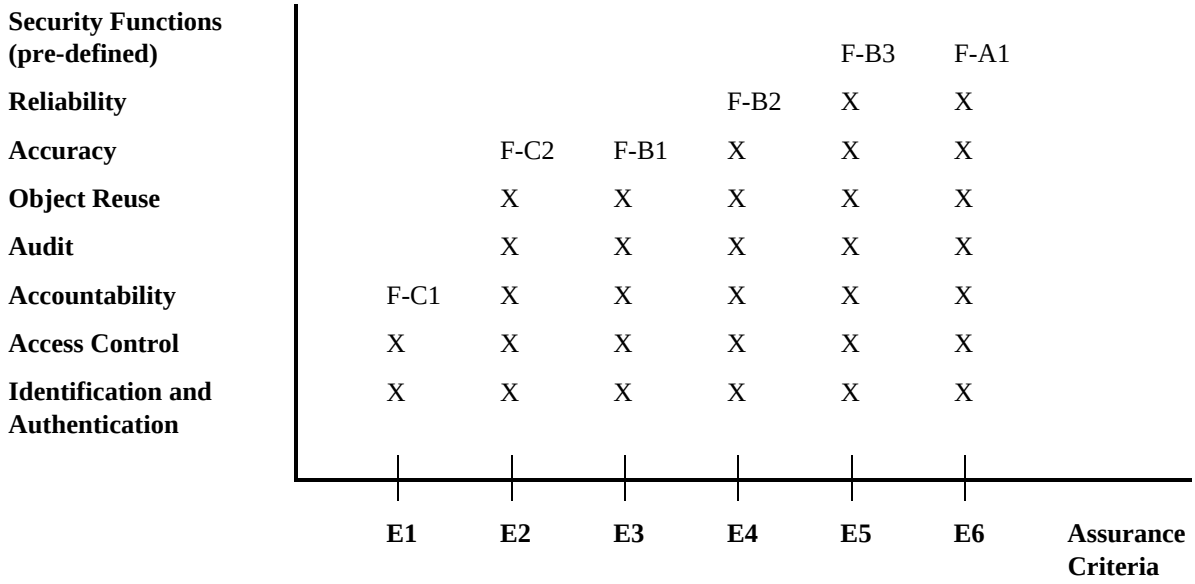

Figure A.10 - ITSEC Pre-defined Classes

A.8.3 The Federal Criteria (FC)

After public discussion of the different criteria during the year 1991 and 1992 it became clear, that the missing world wide harmonization caused confusion on the IT user side and fear on the IT vendor side to be forced into double or multiple evaluations of the same product not to talk about the uncertainty of development, to which criteria a product should conform. ECMA was one of the organisations emphasizing the problem. In the US, the commercial sector was until recently not addressed at all and the infrastructure for non military evaluation was missing. This caused NSA (National Security Agency) to reach an agreement with NIST (National Institute of Standardization and Technology), whereby NIST would cover the lower end of the assurance scale C1 to B1), while NSA would mainly address the higher end (B1 to A). NIST would include governmental as well as commercial requirements in their scope and build up an evaluation structure which is applicable to the private sector as well. The aspect of harmonization and worldwide mutual recognition was taken into account from the very beginning. The work on the Federal Criteria, as well as the harmonization and mutual recognition discussions are presently underway. ECMA is one of the discussion partners in this process.

A.9 Evaluation and Certification

A.9.1 Accreditation of test laboratories

Evaluations are performed following certain national regulations as to who is accredited to perform evaluations and who is allowed to certify an evaluation. In USA, most of the evaluations have been done by teams established by the NSA and paid by the US Government. In Europe, however, a national security agency or potentially another accreditation body would accredit a test facility (laboratory).

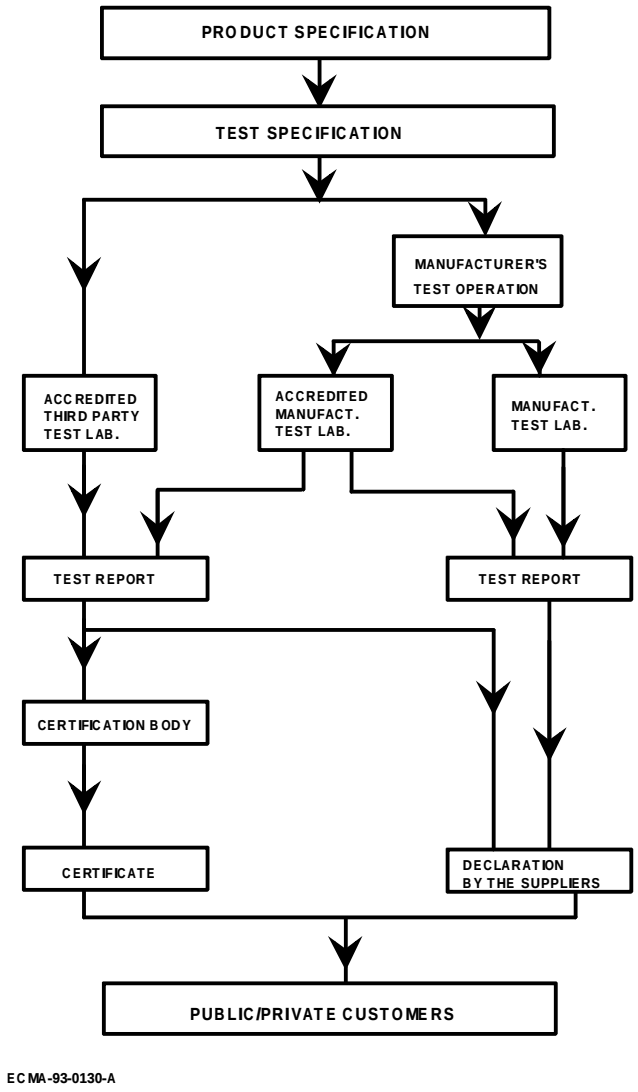

Figure A.11 - Alternatives to declare conformity - Reference:/ECTEL, EUROBIT/

A.9.2 Role of an Accredited Test Laboratory

There is no doubt that accredited testing facilities would deliver qualified test reports and, in case of third party testing, impartial test reports, however, the duration of an evaluation causes problems. An evaluation is of little value if the certificate comes years after the product goes to the market place. With today's fast cycle of change, the product might be obsolete by the time of certification.

To ease this problem, it is suggested to accredit vendor test laboratories. This would allow the testing of security functions almost parallel to the development process and ensures that the test report is available, when the product is ready for shipment to the customer. The test report from an accredited test laboratory can be followed by certification and a certificate. The test report from an unaccredited test laboratory could be followed by a declaration by the supplier.

A.10 Harmonization of Criteria

Besides Europe and the USA also Canada and Japan have published Security Evaluation Criteria. This confuses customers and could also create trade problems. ECMA has highlighted this problem already early 1991. Meanwhile all involved parties agree that harmonization and mutual recognition of evaluation results are a must.

Activities to achieve this goal are presently underway on the political level (EC/USA), (USA/Canada), (EC/Japan) and on the standardisation level (ISO/IEC/JTC1). ECMA/TC36 is actively supporting these efforts. The JTC1 subcommittee SC 27 WG3 tries to merge the different approaches and to find world-wide agreement for an international standard.

Standard ECMA-205, Commercially oriented functionality class (COFC), is intended as a contribution to the international standardisation process.

Another effort is worth noting. The CEC, Canada and USA have established an "Editorial board" to develop criteria called "Common criteria", which are a synthesis of the best concepts and components of existing criteria.

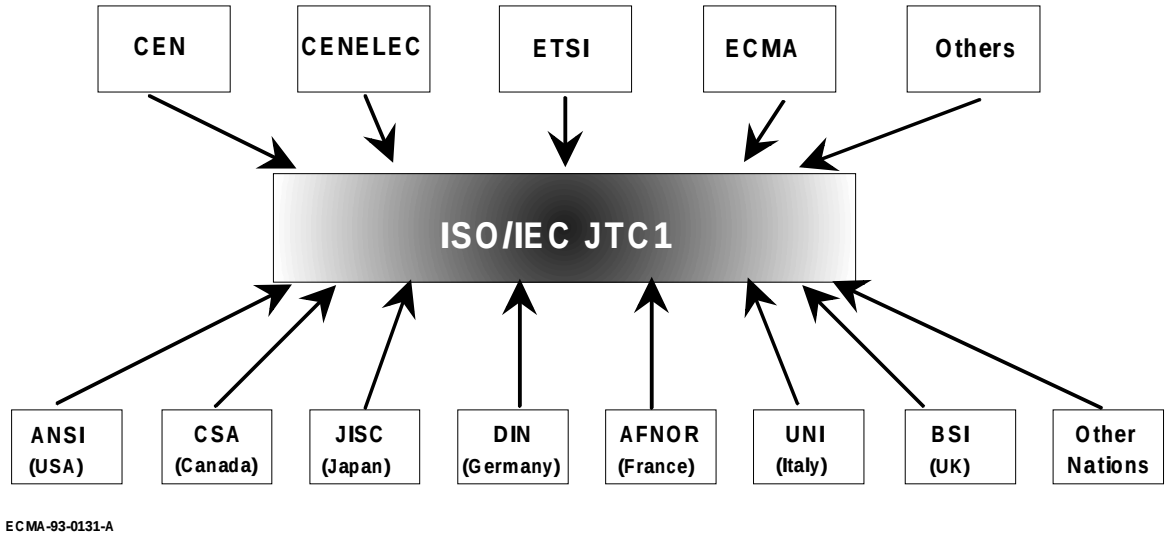

Figure A.12 - International Standardization