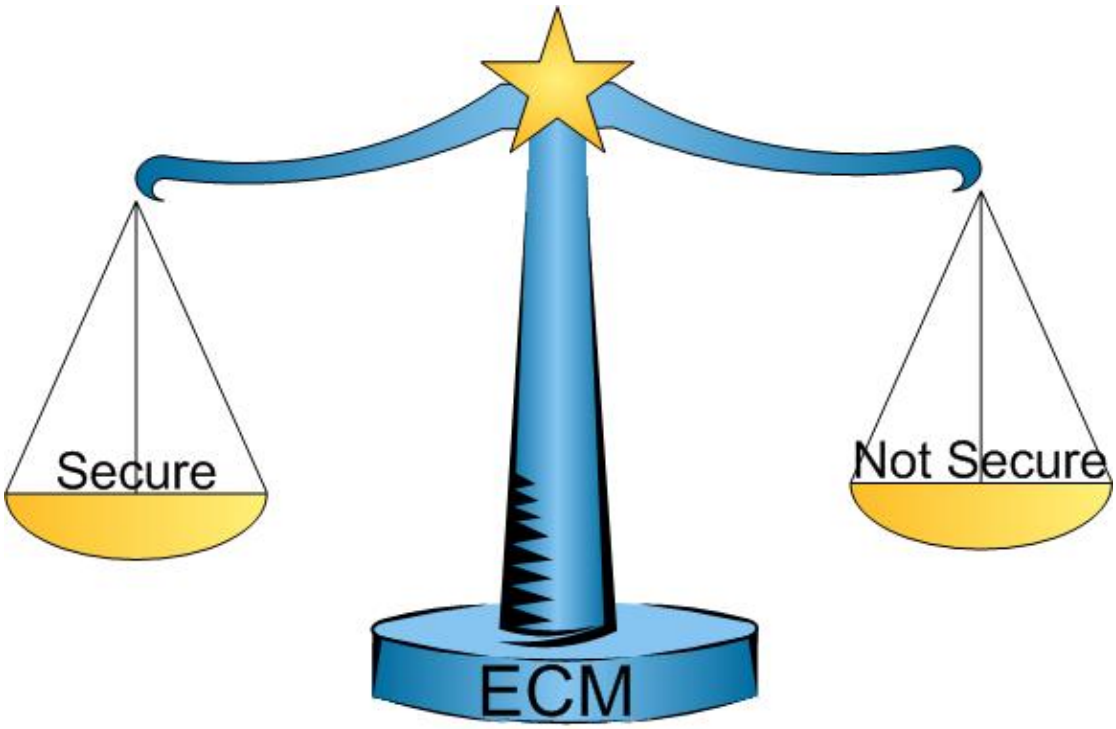
On the Evaluation of Information System Security

The Enhanced Classification Methodology



Chun Yip Leung

Master Thesis
Informatics & Economics
Faculty of Economics
Erasmus University Rotterdam

Erasmus Universiteit Rotterdam

On the Evaluation of Information System Security

The Enhanced Classification Methodology

Chun Yip Leung

Master thesis for completion of a degree in
Informatics & Economics at the
Erasmus University Rotterdam

Supervised by Dr. Ir. Jan van den Berg
Coached by Diederik Klijn and Wilco van Ginkel

Supported by Ubizen the Netherlands

Table of contents

ACKNOWLEDGEMENT VII

EXECUTIVE SUMMARY VIII

LIST OF ABBREVIATIONS X

1. INTRODUCTION 1

1.1 THE NEW ECONOMY 1
1.2 INFORMATION SECURITY 2
1.3 THE ENHANCED CLASSIFICATION MODEL 3
1.4 RESEARCH PROCESS 3
1.5 OUTLINE 4

2. INFORMATION SYSTEMS AND SECURITY 5

2.1 THE INFORMATION SYSTEM 5
2.2 INFORMATION SECURITY 8
2.3 INFORMATION SYSTEM SECURITY AND ITS THREATS 11
2.3.1 The need for security 11
2.3.2 Where to put security 13
2.4 EVALUATION CRITERIA 15
2.5 SUMMARY 18

3. EVALUATION METHODS 19

3.1 EVALUATION METHODS FOR INFORMATION SYSTEM SECURITY 19
3.1.1 Technical evaluation methods 19
3.1.2 Managerial evaluation method 21
3.2 TRUSTED COMPUTER SYSTEMS EVALUATION CRITERIA (TCSEC) 22
3.3 INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA (ITSEC) 24
3.4 COMMON CRITERIA (CC) 26
3.5 SUMMARY 27

4. THE ENHANCED CLASSIFICATION METHODOLOGY 28

4.1 INTENTION AND FOUNDATION 28
4.1.1 Information system oriented 28
4.1.2 End-user point of view 29
4.1.3 ECM foundation 29
4.1.3.1 Protection profile 29
4.1.3.2 Requirements 30
4.1.4 Conclusion 30

4.2 METHODOLOGY 31
4.3 PREPARATION STAGE 33
4.3.1 Functional requirements 34
4.3.1.1 Coherence of the CC classes 34
4.3.1.2 Security services 38
4.3.2 Assurance Requirements 39
4.3.3 Additional requirements 39
4.4 IDENTIFICATION STAGE 40
4.4.1 Context assessment 40
4.4.1.1 Intended use 40
4.4.1.2 Information system requirements 41
4.4.1.3 Context needs 41
4.4.2 Requirements classification 42
4.4.3 Sub-protection profiles 43
4.4.4 Protection profiles 44
4.4.4.1 Predefined requirements 44
4.4.4.2 Protection profile documentation 45
4.4.4.3 Reusability 47
4.5 THE ANALYSIS STAGE 49
4.5.1 Information system and what is provided 50
4.5.2 Security target format 51
4.6 THE EVALUATION STAGE 53
4.6.1 Functional requirements evaluation 54
4.6.2 Assurance requirements evaluation 54
4.6.3 Evaluation outcome 55
4.7 SUMMARY 56

5. THE ENHANCED CLASSIFICATION METHODOLOGY TEST CASE 57

5.1 FRAMING THE TEST CASE 57
5.2 PREPARATION STAGE 59
5.3 IDENTIFICATION STAGE 61
5.4 ANALYSIS STAGE 68
5.5 EVALUATION STAGE 69
5.6 CONCLUSION 73

6. CONCLUSION AND POSSIBLE FURTHER RESEARCH 76

6.1 GOALS REVISITED 76
6.2 CONCLUSION 77
6.3 POSSIBLE FURTHER RESEARCH 79

APPENDIX 80

REFERENCES 90

List of figures

Chapter 2:
Figure 1: Information system model 6
Figure 2: Information security levels.....11
Figure 3: Attackers requirements by ICAT [Icat, 2003].....12
Figure 4: Vulnerabilities accounted by ICAT [Icat, 2003].....14
Figure 5: Security management life-cycle [Simo, 1970].....16
Figure 6: Evaluation methods division [Leav, 1964] 16

Chapter 3:
Figure 7: Evaluation of the criteria [Comm, 2003] 21
Figure 8: Information security management 21
Figure 9: Bell-Lapadula model.....23

Chapter 4:
Figure 10: Common Criteria methodology 31
Figure 11: General description of the ECM 32
Figure 12: Preparation stage.....34
Figure 13: Common Criteria hierarchical structure example 35
Figure 14: Common Criteria's functional requirements coherence.....36
Figure 15: Identification stage.....40
Figure 16: Protection profile 45
Figure 17: Protection profile overview.....45
Figure 18: Common Criteria protection profile format 47
Figure 19: Analysis stage 50
Figure 20: Security target format.....52
Figure 21: Evaluation stage 53

Chapter 5:
Figure 22: Architectural design of the test case.....58
Figure 23: Web application sequence diagram.....63
Figure 24: Aggregation of components 74

List of tables

Chapter 2:
Table 1: Mapping attacks to information system 15

Chapter 4:
Table 2: Functional requirements in relation to security services 38
Table 3: Requirements classification.....42
Table 4: Protection profile.....44
Table 5: Protection profile reusability 48
Table 6: Protection profile templates.....49
Table 7: Pragmatic assurance extension.....55

Chapter 5:
Table 8: Functional requirements division in security services.....61
Table 9: Dependencies between security needs/threats and security requirements.....65
Table 10: Requirements classification.....66
Table 11: Protection profiles' functional requirements 67
Table 12: Information system functionalities 69
Table 13: Evaluation table.....70
Table 14: Recommendations 71
Table 15: Assurance overview 72
Table 16: Deviations of the test case 73

Acknowledgement

The final phase of my master study Informatics & Economics (Informatica & Economie) at the Erasmus University Rotterdam requires me to write a thesis in order to successfully conclude my study. This thesis is written at Ubizen BV (located in Mijdrecht, The Netherlands) over the course of almost one year. Many people contributed to the realization of this thesis. Without the help of those people, this thesis probably would not have existed. Therefore I would like to thank the following persons for their indispensable support (in no particular order):

- My supervisor, dr. ir. Jan van den Berg, even though with his busy schedule and despite some setbacks at the university, he managed to guide me through the entire course of writing this thesis.

- Ubizen, for giving me the opportunity to explore one of information technology's most interesting fields of study, namely information security. During my period at Ubizen I have learned a lot about information security and much more.

- All the people from Ubizen BV, thank you for giving me such a good time at Ubizen. Furthermore I would like to thank my two coaches in particular: Wilco van Ginkel (senior security consultant) and Diederik Klijn (security engineer), for their guidance of writing a thesis and just for the fun we had.

- André Mariën from Ubizen headquarters in Belgium, for freeing time for me and for giving invaluable input.

- The organization that was willing to let me conduct the ECM test case on their information systems.

- My family and friends, for not getting upset due to the lack of time (with whatever I was doing).

- Google, thanks for the great search engine, "To google" is most definitely included in my dictionary/vocabulary.

Sorry for all the persons that I forgot to mention or I did not mention directly. Your support and presence are truly appreciated, many thanks!

Chun Yip Leung
Mijdrecht, November 2003

Executive Summary

The Enhanced Classification Methodology (ECM) is a methodology designed to assess the security of information systems against a certain set of requirements (whether best practices or requirements of the customer).

Background: large amount of attacks
In the current economy, information and information systems have become an integral part of business processes. As with all business processes they need to be well secured against security breaches (in terms of: confidentiality, integrity, availability, and accountability). The damage of lacking security can be quite severe. As a recent research claimed, approximately half of the Dutch companies had an intrusion to their information system in 2002 [Tele, 2003]. An intrusion may lead to the following losses:

- Revenue; a research of the Yankee group claimed that denial of service (DoS) attacks of websites alone cost organizations over $1.2 billion in 2000 [Yank, 2003].
- Business continuity; an article of ABC news showed that a (distributed) DoS attack on eBay lead to an interruption of 22 hours in June 1999 [ABC, 2003].
- Trust; trust/image plays a very important role for many organizations in the current era. The attack on eBay mentioned in the previous example caused the company's stock to lose 26% of their value in only five days [ABC, 2003].

Problem: no suitable assessment methods available
There have been several methods developed to assess the security of computer products. The latest standardized assessment method (Common Criteria), however, cannot satisfy the needs of the users. The following points are considered as the main inadequacy:

- Product based
- Manufacturer oriented

Solution: The Enhanced Classification Methodology (ECM)
The ECM is an information system security evaluation methodology based on the Common Criteria, but without the inadequacies stressed above. The inadequacies can actually also be considered as the key-points of the ECM. The following section describes the key-points of the ECM in further details:

Information system based
The ECM is based on information systems rather than based on products like the Common Criteria. After all, often products are not used separately. An information system is a combination of products that works together. Therefore entire information systems need to be assessed and not merely single products.

End-user oriented
The Common Criteria is mainly manufacturer oriented. To conduct an evaluation by the Common Criteria, an accredited evaluation organization has to be consulted. This implies high costs, in terms of: money, time, and effort. To eliminate these costs, the ECM is designed to be performed by the end-user.

To achieve its goals, the ECM utilizes a systematic approach. Hereby focussing on the following two aspects:

- What is needed
- What is provided

The first aspect (what is needed) contains a context[1] analysis to determine which functionalities are needed within the given context. The second aspect (what is provided) contains an information system analysis to determine which functionalities are provided. In case the information system possesses all the functionalities that are required by the context, the information system can be considered as adequate for the particular situation. In case the information system lacks functionalities, the ECM can easily identify them. Furthermore, there is a part that assesses the assurance of an information system. The assurance part determines the degree of trust in the available functionalities.

To test and verify the ECM, the ECM is exposed to a test case. The test case is conducted on an actual organization and shows that the ECM (in its current state) is quite suitable for practical use. The results of the ECM evaluations were well received by the organization of the test case. The organization of the test case was actually interested and impressed by the ECM evaluation results. The test case, however, also shows that the ECM is still prone to improvements. In order to provide the ECM as a service to customers, further research for the ECM is necessary. This is due to the fact that certain steps of the ECM evaluation are not as clearly described as should be. Finally, this thesis can be contemplated as a stepping-stone for the ECM and as a starting point to implement technical oriented security evaluations on information systems.

[1] The situation within which something exists or happens [Camb, 2003].

List of abbreviations

ACL	Access Control List
AMD	Advanced Micro Devices
ASP	Application Service Provider
BS	British Standard
CC	Common Criteria
CCITT	Comité Consultatif International Téléphonique et Télégraphique (Consultative Committee on International Telegraphy and Telephony).
CEM	Common Evaluation Methodology
CPU	Central Processing Unit
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAC	Discretionary Access Control
DoD	Department of Defense
DoS	Denial of Service
EAL	Evaluation Assurance Level
ECM	Enhanced Classification Methodology
EDP	Electronic Data Processing
FC	Federal Criteria
GIAC	Global Information Assurance Certification
IBM	International Business Machines
IDS	Intrusion Detection System
ISO	International Standard Organization

IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
MAC	Mandatory Access Control
NGI	Nederlands Genootschap voor Informatica (Dutch Association for Information Science)
NIST	National Institute of Standards and Technology
OS	Operating System
OSI	Open Systems Interconnection
OWASP	Open Web Application Security Project
PP	Protection Profile
RFC	Request For Comments
ST	Security Target
TCG	Trusted Computing Group
TCSEC	Trusted Computing Systems Evaluations Criteria
TNO-ITSEF	Toegepast Natuurwetenschappelijk Onderzoek (Employed Science Research)-Information Technology Security Evaluation Facility
TOE	Target Of Evaluation
TSF	Trusted Security Functions
WAS	Websphere Application Server

1. Introduction

1.1 The new economy

The economy changes over time, as the agricultural economy has evolved into the industrial economy. Several people claim that the industrial economy already has involved into a new era called the new economy[2] [Marg, 1998] [Carl, 1999]. An often cited, referred, and used definition of the new economy by John Browning and Spencer Reiss [Brow, 1998] is as follows:

"When we talk about the new economy, we're talking about a world in which people work with their brains instead of their hands. A world in which communications technology creates global competition - not just for running shoes and laptop computers, but also for bank loans and other services that can't be packed into a crate and shipped. A world in which innovation is more important than mass production. A world in which investment buys new concepts or the means to create them, rather than new machines. A world in which rapid change is a constant. A world at least as different from what came before it as the industrial age was from its agricultural predecessor. A world so different its emergence can only be described as a revolution".[3]

As John Browning and Spencer Reiss asserted the new economy is an era where peoples' brains play an important role. The economy no longer only evolves around products, but the provision of services in the broadest sense becomes more important. Furthermore the definition of John Browning and Spencer Reiss also states that the intellectual properties become more and more important. As a result, information plays a very important role in this era. The following example reflects a more concrete example of the importance of information.

Amazon, for instance, has patented their "1-click" business method (U.S. Patent 5,960,411) in September 1999. *"The "1-click" patent is an online system allowing customers to enter their credit card number and address information just once. So the follow up visits to the website only requires a single mouse-click to make a purchase from their website".* With the "1-click" business method patent, Amazon filed a lawsuit against Barns and Noble for their former paying system (Express Lane), which is similar to Amazon's "1-click" business method. Due to the lawsuit Barns and Noble had to exclude the Express Lane paying system from their website and use the traditional shopping cart principle. This caused inconvenience to many customers and ultimately led to confusion and annoyance. Due to the customers' dissatisfaction the revenue of Barnes and Nobles decreased significantly [Stan, 2003].

[2] The new economy is also known as the digital economy, the network economy, or the information economy.

[3] Probably not everyone agrees that the new economy is such a revolution. We probably do agree that the new economy can at least be considered as an evolution of the economy.

1.2 Information security

The previous section illustrated that information has become a valuable asset, from worldwide organizations to personal users. As information is valuable to us we need to protect the information from harm as any other valuable asset. Protecting information, however, differs from protecting other assets. Information security namely focuses on the following four security requirements: confidentiality, integrity, availability, and accountability[4] [Burd, 2001] [Ubiz, 2000]. People have realized the importance of information security and many computer/information system security methods have been developed, for instance, logical and physical security. Even though much effort has been spent on the security of information systems, none of the current efforts offers a 100% security[5]. This is not only the case for information system security, but rather for security in general. Banks (financial institutes), for instance, can be considered as one of the most safeguarded instances, but bank robberies still occur despite of the heavy security.

Another point is that everything comes with a price. This is also the case regarding security. Implementing security often costs money, effort, knowledge and much more. Therefore we often (or rather always) do not strive for 100% security, but we rather strive for adequate security to cover the risks to a sufficient degree. The question arises, how do we know when we have adequate security to cover the risks? There has already been several security models designed to cover this question.

These security models can be divided in two categories, namely managerial[6] oriented and technical oriented security models. This thesis, however, focuses on the technical oriented security models. Due to the inadequacies that exist in these models, examples of these inadequacies are:

- The security models are only based on products. This, however, is not sufficient, as information systems consists of several components. By combining several "secure" products, we cannot ensure that the entire information system is "secure" as well.
- The security models are only intended for specific accredited organizations. This leads to large costs in terms of, money, effort, and time. This limits the security models only to manufacturers, since they probably are the only one who are willing to invest in such an amount of money, time and effort.
- None of the current security models mandate that the entire product is evaluated. Thus it is possible for a product to have a high security

[4] Further details of the security requirements are provided in chapter 2.
[5] Many (if not all) actually believe that there is no such thing as 100% security.
[6] Notice that managerial is used instead of organizational. According to the dictionary organizational is an arrangement of something according to a particular system and managerial is the control and organization of something. Thus organizational is a process according to certain rules while managerial is controlling the rules and thus manipulating the process.

classification based on a certain subset of features of the product, which is not relevant at all. This certainly misleads the potential buyers of the product.

1.3 The Enhanced Classification Model

Based on the observations stressed in the previous section, it seems inevitable to create a model, which can address the problems. The intent of this thesis is to create such a model. The model is mainly in line with the existing criteria, but also addresses the following two requirements:

1) Classifications based on information systems rather than products.
2) Create a methodology, which is suitable for the end-users rather than the manufacturer/vendor.

This model is called the Enhanced Classification Methodology (ECM) and is described throughout this thesis. In short, the distinguishing characteristic of this model is that the ECM can be conducted by the end-users and is designed to evaluate information systems. Therefore, the ECM can be tailored to each individual information system and be performed by the owner of the information system.

Another point worth noticing is that the ECM can be considered as quite a pioneering project. At the time of writing, there are not any technical oriented security models available or in development, which are intended for the end-users[7]. Besides, no projects have evaluated an entire information system yet.

1.4 Research process

The methodology to create the ECM is mainly based on literature research. The further steps of creating this thesis can be roughly categorized as follows:

1) Performing research on literature (by means of books, articles, and the Internet) regarding information systems, the security of information systems, and the classification models of information systems.
2) Having lots of discussions with my coaches, my supervisor and others.
3) Identifying the requirements of information system security classification models.
4) Identifying the shortcomings of the current computer security classification models.
5) Creating a methodology based on the characteristics of current computer security classification models with additional features in order to satisfy the requirements and to overcome the shortcomings.

[7] Known by the author.

6) During the shaping of the ECM, an expert was consulted. The ideas of the expert were subsequently incorporated into the ECM.
7) Conducting a real life case.
8) Finally a conclusion was stated, which incorporates the ideas of the expert, the shortcomings of the ECM, and the possible future research.

Even though the steps are in a subsequent order, the actual process was not as clear categorized as above. Some steps were reoccurring during the entire process and some steps were done in parallel with other steps. The trail above, however, does provide a good illustration of how the thesis has been created.

1.5 Outline

This thesis assumes that the reader has little knowledge of computers and of information (system) security.

For those who are not planning to read the entire thesis or for those who wish to read the thesis in another sequence than written, an outline is provided to give the reader a general notion of which chapter might be relevant and in what order to read the thesis.

Chapter 1 this (current) chapter introduces a rough outline of what is discussed throughout this thesis.

Chapter 2 defines what an information system actually is and stresses why information system security is needed in the first place.

Chapter 3 provides an overview of the current security evaluation models.

Chapter 4 describes the methodology of the ECM. This chapter provides a step-by-step methodology to conduct a classification according to the ECM.

Chapter 5 provides an actual test case of the ECM. In this chapter the ECM theory is implemented in practice.

Chapter 6 this chapter provides the conclusions regarding the ECM. Furthermore this chapter points out the possible points for improvements and further research.

2. Information systems and security

This chapter provides a basic understanding of the employed definition of information systems. Moreover this chapter provides the employed definition of security, since the meaning of security may vary in different contexts. Subsequently the two definitions are combined and information systems security is discussed. Finally, the evaluation criteria are briefly discussed.

2.1 The information system

As the name already suggested an information system is a system that deals with information. We probably already have a notion of what an information system is. But it is actually quite hard to define what an information system is and what it is not. The dictionary [Camb, 2003] defines information as *"facts about a situation, person, event, etc."* and defines a system as *"a set of connected items or devices which operate together"*. Thus officially according to the dictionary an information system is a set of connected items or devices, which operate together and deals with facts about a situation, person, event, etc.

A computer network, for example, can undoubtedly be considered as an information system. After all, it fully complies with the definition of the dictionary. But can a voice recorder also be considered as an information system? After all, a voice recorder can record information and playback information. According to the defined definition a voice recorder should be considered as an information system as well. Probably not everyone agrees with the last example. Therefore it is necessary to delimit the definition of an information system.

The American National Standard for telecommunications defined the following three definitions for information systems [ANS, 2001]:

1) A system, whether automated or manual, that comprises people, machines, and/or methods organized to collect, process, transmit, and disseminate data that represent user information.
2) Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.
3) The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Because the security focus of this thesis is technical oriented, the second definition is used throughout the remaining of this thesis. Besides focusing only on the second definition the managerial aspect is excluded[8]. Since the definition of information systems is defined a further description of information systems can be provided.

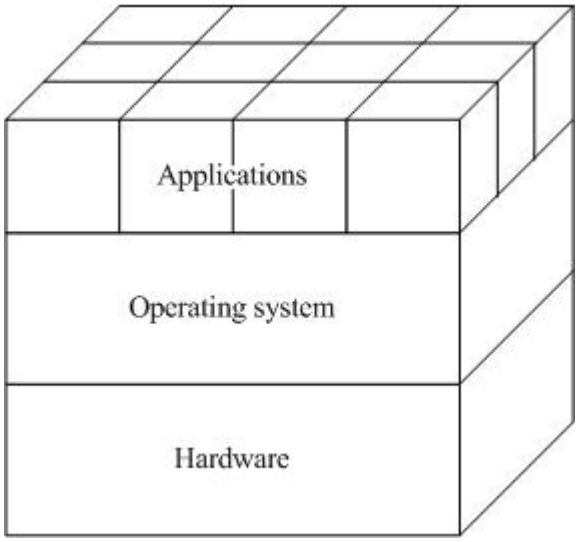


Figure 1: Information system model

Figure 1 provides a very abstract and simple way of viewing an information system. This representation is quite similar to the model used by Andrew Tanenbaum [Tane, 1992]. The model in this thesis, however, is an even more simplified version of the model used by Tanenbaum. Even though the model is very simplistic, it captures all the essential elements of an information system. As Figure 1 shows, an information system can be divided in three layers, namely the application layer, the operating system layer, and the hardware layer. Often a distinction is made between hardware[9] and software[10] as well. The application layer and the operating system layer can be considered as the software layer and the hardware can obviously be considered as the hardware layer. The following section provides a more detailed explanation of each layer.

The hardware layer is the "lowest" layer and contains all physical and electronic parts of a computer, such as central processing units, memory, storage devices etc. The actual processing, storing, and computing of information is handled in this layer. But only having the ability to process, to store or to compute information is useless. After

[8] The remaining of this chapter shows why the managerial aspects are excluded.
[9] Definition according to the dictionary: the physical and electronic parts of a computer, rather than the instructions it follows.
[10] Definition according to the dictionary: the instructions which control what a computer does.

all, there has to be an entity, which can steer the ability to process, to store or to compute information.

The operating system layer is an entity, which can steer/operate the hardware layer (Linux, and Microsoft Windows are examples of operating systems). As Figure 1 shows the operating system layer is the layer between the hardware layer and the application layer. The operating system layer has the ability to communicate with the hardware layer and provides the base for the application layer to work on. The operating system is actually more than just a translator between the application layer and the hardware layer. The operating system also manages the resources, processes, and mandates the processes to enforce the authentication and the authorization scheme of the operating system.

Andrew Tanenbaum [Tane, 1992] stated that the operating system is one of the most important features for the entire information system:

"The most fundamental of all system programs is the operating system, which controls all the computer's resources and provides the base upon which the application programs can be written."

Even though, the operating system is indeed a very important layer of the information system, all layers are as important to an information system. In case a piece of hardware malfunctions, it probably leads to a failure of the entire information system. For instance, when a central processing unit malfunctions, the software stops functioning as well. After all, there is no central processing unit to calculate the outcomes anymore.

The application layer consists of all software on top of the operating system layer. This layer often consists of programs/applications executing on behalf of a user or a process. These applications may vary from form. For example, games, banking systems or text editors are examples of applications. Notice that databases are also considered as an application. After all, a database runs on top of an operating system and utilize the functions of the operating system to communicate with the hardware like any other application.

The following example provides a (complete) view of how an information system operates. In case an application wants to execute a certain command, the application sends a request to the operating system. The operating system in its turn receives the request and subsequently checks the request against the authentication and authorization scheme. If the request is authorized, the operating system translates the request and passes the command to the hardware. Finally the hardware performs a certain action and, if necessary, passes the result back to the operating system, which passes it through to the application.

2.2 Information security

The meaning of security can vary depending on the context. Security for a car, for example, is mainly focused on the safety of the persons inside the car or perhaps to prevent the car of getting stolen. The security for tax authorities[11] on the other hand is to prohibit fraud and probably to safeguard the privacy of the taxpayers.

Security can also vary from severity in different context. The protection of money[12] for a normal person, for instance, can be satisfied by saving it in a vault or by depositing it in on a bank account[13]. These measures, however, are probably not adequate for banks. Banks naturally also have to protect their money, but banks must have a stronger security compared to a regular person. First of all, banks probably have a larger amount of money to protect, thus an attack on a bank has more severe loss compared to a regular person. In order to cover this higher risk more severe measures need to be taken (e.g. alarm systems, guards, and camera surveillances).

As the previous section illustrated, security can vary from meaning and from severity. The most important issue of security is that the risks need to be covered. Risks can be divided in two types:

- Risks that must be covered. These risks are considered as not acceptable and are further referred to as unacceptable risks.
- Risks, which are accepted. These risks are called residual risks and are taken for granted.

For security, the first type of risks must be covered. The second type of risks is considered as accepted. For instance, the costs do not weight up to the benefits or the risk cannot be secured at all.

Notice that there is probably no such thing as a 100% secure. In case we assume that a bank is secure, we actually mean that the bank is protected against all the unacceptable risks. Thus the money of the bank “cannot” be stolen and the information of the bank “cannot” be read, created, altered, or deleted by unauthorized persons. Realize that this is only a subset of the security of a bank. In order to protect the stressed subset is already a highly infeasible job. Probably any vault can be broken (or perhaps blown into pieces), guards can be eliminated, alarms can be bypassed, and so on. Therefore the remaining of the thesis interprets secure as covering all the known unacceptable risks.

[11] E.g. the “belastingsdienst” for the Netherlands, the IRS for America, and the Inland Revenue for England.
[12] Physical money and thus not money in an electronic form or the like.
[13] Thus relying on the security of the bank.

Since a general understanding of security is provided, the context of security for this thesis can be defined. When this thesis mentions security, it implies to strive for the following requirements [Burd, 2001]:

Confidentiality – the ability to contain information to those unauthorized to view and to protect against the disclosure of information where it could be damaging. This would include keeping information private or secret. Confidentiality can be obtained by keeping information secure and preventing unauthorized access to such information.

Integrity – the quality of information that identifies how closely the data represent reality. This is the ability to keep information from being changed by unauthorized users and that the information is complete and unchanged. Unauthorized modification of log files or getting a virus that makes changes to files is a form of an integrity attack.

Availability – goes hand-in-hand with confidentiality and integrity. Availability is the ability to provide authorized users information and/or functionalities when it is requested or needed. A power outage or viruses that crash a computer system are some examples of an availability attack.

Accountability – the ability to trace an action to a unique entity. This would include keeping up all the performed actions. An audit trail is an example to enforce the accountability requirement [Ubiz, 2000].

In order to satisfy these requirements security services can be used. A security service is a service, which ensures adequate protection of the security requirements. For a more detailed description of the security service and other descriptions concerning (Internet) security, the reader is referred to the Internet Security Glossary (RFC2828) [Inter, 2000]. The following main security services are defined by the X.800[14] [X800, 1991]:

- Authentication
- Access Control
- Data confidentiality
- Data integrity
- Non–repudiation

This thesis uses a variant of the provided security services. After all, the security services of the X.800 are designed for networks only. This thesis, however, has a broader scope and focuses on information systems. Thus a more global description of security services is needed for this thesis. This thesis utilizes a combination of the security services of the X.800 and the security framework of the X.810 [X810, 1995]. The X.810 defines security frameworks for open systems, which comes closer to

[14] The X.800 is a security architecture for the OSI/ISO layer model.

information systems than the X.800. The following list defines the security services used throughout this thesis[15]:

- Authentication – measures to ensure the identity of an entity
- Access Control[16] – permit only authorized entities to the resources of the information system
- Confidentiality – disclosure of information only to those who are authorized to access it
- Integrity – prohibit unauthorized alteration or destruction of data, information and information systems
- Availability – ability to obtain access to information and to information systems by authorized users when necessary
- Accountability – ensures that an action can be linked to its initiator

Notice that the accountability security service is renamed. Officially it is defined by the X.810 as the security audit and alarms. The term accountability is used, because it is a broader and more generic definition. Furthermore availability is added to the security services, this is done, because in many situations the availability can be seen as security service as well. Besides Stallings [Stall, 2003] also asserted that availability is considered as a security service by many other persons and models.

The security services in its turn can be divided in (or rather implemented by) security mechanisms [Inter, 2000]. Security mechanisms are mechanisms used to realize the security services. The mechanisms for the OSI layer are also covered by the X.800. This thesis, however, does not discuss security mechanisms, since it is considered as too detailed/low level and not relevant for the thesis.

[15] Notice that the confidentiality, integrity, availability, and the accountability of the security requirements differ from the confidentiality, integrity, availability, and the accountability of the security services. The security services can actually be seen as an elaboration of the security requirements.

[16] Access Control and authorization can be used interchangeable throughout this thesis.

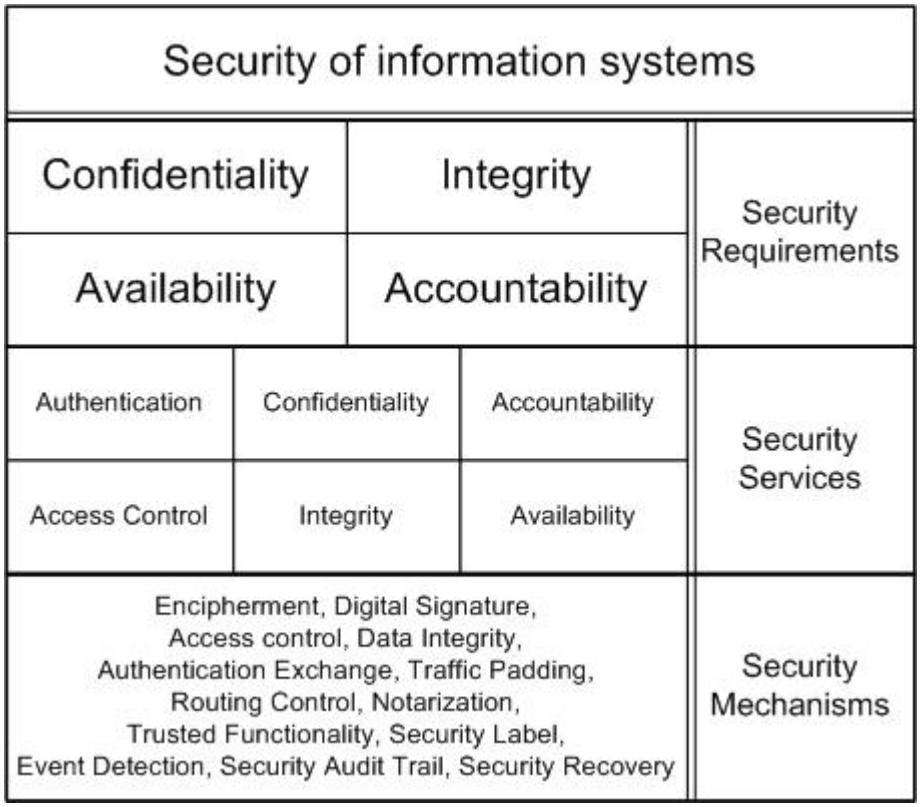


Figure 2: Information security levels

Figure 2 summarizes a complete view of the security definition employed throughout this thesis. The figure shows that information security has four security requirements. These requirements identify what is strived for. The security requirements can be satisfied by appropriately implementing security services. Security services can in its turn be divided in security mechanisms. With the appropriate security mechanisms the actual security requirements for information systems can be fulfilled.

2.3 Information system security and its threats

2.3.1 The need for security

In the past decades information system security awareness has raised significantly. This is mainly caused by the fact that computers have increased their connectivity, whether by networks or by the Internet[17]. The main advantage of connecting computers is that it allows the users to communicate and to share data with each other.

[17] Which is a network as well.

This is also the main setback, since a malicious user can manipulate a computer without physical access. Due to the fact that physical access is not necessary anymore to access another computer, the possibilities to intrude a system have significantly increased. Figure 3 illustrates, that remote attacks are apparently more often utilized than local attacks. The figure is based on the results of ICAT [Icat, 2003], which is a division of the National Institute of Standards (NIST).

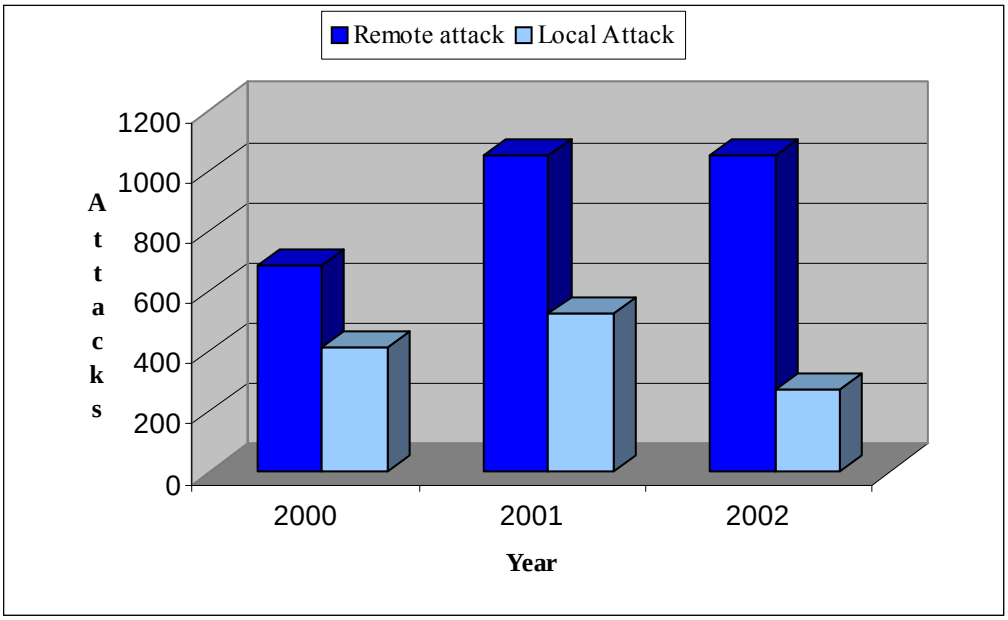


Figure 3: Attackers requirements by ICAT [Icat, 2003]

Local attacks are defined by the ICAT as follows:
"Attacks that utilize the vulnerability can be launched directly on the system that is being attacked. The attacker must have some previous access to the system in order to launch an attack locally. Note, we still define an attack as local if an attacker legally telnets to a host and then initiates an attack on that host. The attack is local because the attacker did not attack the telnet server itself but a component only visible to logged in users."

Remote attacks are defined by the ICAT as follows:
"Attacks that utilize the vulnerability can be launched across a network against a system without the user having previous access to the system."

Notice that physical access is not necessary for being categorized as a local attack by the ICAT. In case an attacker has previous access to the information system it is classified as local as well. Thus in case only attacks with physical contact are

classified as a local attack, the difference between remote and local attacks are even greater.

Even though 1339[18] attacks do not seem very much, this amount only accounts for the reported attacks. The actual amount is probably much higher, since home users often do not report an attack and even many organizations do not always report their attacks. After all, an attack on an organization naturally has impact to the image and trust of an organization. A recent research of ECP.NL (an organization established by the Dutch Ministry of Economic Affairs) and Ernst & Young showed that half of the Dutch organizations had an intrusion in 2002. Nevertheless, less than 20% of the organizations reported the intrusions [ECP, 2003] [Tele, 2003]. Thus the attacks are in practice probably much higher than illustrated in Figure 3.

Since the need for security[19] is covered, what needs to be secured can be discussed.

2.3.2 Where to put security

Recall Figure 1, which states the three layers of an information system. In theory such clear distinctions between the layers can be made, but in practice it is often hard to determine, for instance, what an operating system is and what an application is. The distinction between the layers is blurred. Microsoft Windows 2000 (an operating system), for instance, is standard equipped with all kinds of applications, like WordPad, Internet explorer, and games. It is therefore very hard to make a clear distinction between what the operating system is and what the application is. A common joke about the Windows operating system is actually: Windows is a web browser and you get an operating system for free. Moreover, an increasing amount of applications provide security. Applications even manage hardware by themselves, by misleading the operating system. For instance, think of an application misleading the operating system by manipulating the memory management, in order to increase the performance of the information system. Besides, the Trusted Computing Group [TCG, 2003] (a collaboration of: AMD, Hewlett-Packard, IBM, Intel and Microsoft) aims to combine an operating system with hardware. Thus in the future it may even become harder to make a distinction between the layers.

Implementing security on a single layer of the information system or only implementing it to a subset of an information system is therefore not adequate. Applying security only in one layer probably decreases the complexity and simplifies the management. But security, however, has to be implemented throughout all the critical parts of the information system. As stated earlier in this section an information system depends on all layers. Thus one weak layer can compromise the entire security of the information system. After all, as the saying goes: a chain is as strong as its

[18] Total attacks of the year 2002.
[19] At least from a technical point of view.

weakest link. Therefore the weakest link has to be minimally as strong as the situation requires.

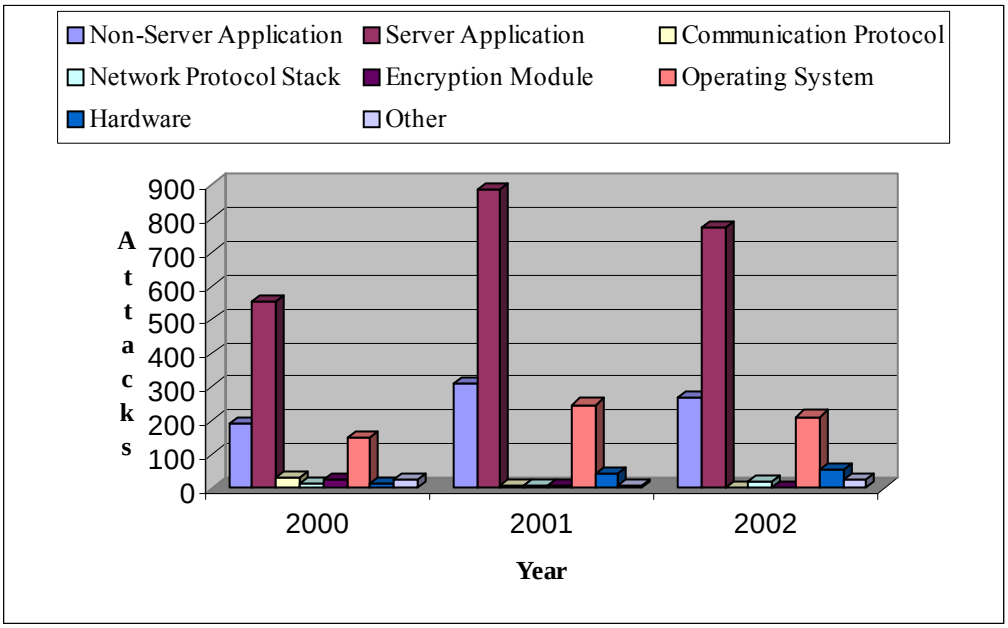


Figure 4: Vulnerabilities accounted by ICAT [Icat, 2003]

Figure 4 shows the attacks accounted by the ICAT. The figure has eight attacks defined, while the information system model only has three layers. The eight attacks can be mapped to the three information system model as follows:
The non-server application, server application can be classified as the application layer. The communication protocol, network protocol stack, and the encryption module can be classified partly as the application layer and partly as the operating system layer. After all, these attacks can occur on the application layer as well as on the operating system layer. The operating system and the hardware can naturally be classified as respectively the operating system layer and the hardware layer. The "other" cannot be assigned to a certain particular layer. After all, the characteristics of the attack are unknown. Table 1 illustrates the classification of the attacks to information systems in a tabular form.

Attacks	Information System Layer
Non-Server Application	Application
Server Application	
Communication Protocol	Application / Operating System
Network Protocol Stack	
Encryption Module	
Operating System	Operating System
Hardware	Hardware
Other	Application / Operating System / Hardware

Table 1: Mapping attacks to information system

Figure 4 shows that attacks are executed on all three layers of an information system. Thus only implementing security on one of the three layers is certainly inadequate. After all, it is not necessary for an attacker to attack all layers in order to harm an information system. Thus it is possible to attack the weakest layer in order to compromise an entire information system.

2.4 Evaluation criteria

In the course of time many security methods[20] have been developed and many have been widely implemented. Security has actually become an integral part of many information systems. Home-users, for example, often use security methods like: virus scanners and personal firewalls. Organizations often use more powerful and more expensive security methods. After all the risk and the consequences of an attack is for an organization probably higher than for a normal user. Organizations can, for example, implement the following security methods: IDS (intrusion detection systems), firewalls, and strong forms of authentication. Despite of the many security methods, attacks on information systems still occur as Figure 3 and Figure 4 illustrated.

In order to reduce the risks of getting attacked successfully, the security methods stressed above can be used. There are actually also other methods that can increase the security of an information system, like setting up a good organizational policy for information system usage, having well educated users and imply physical protection to the information systems. There are even many other security methods available. To address all the possible security methods would require a whole book. That is outside the scope of this thesis. Therefore this thesis focuses on one security method in particular, namely the evaluation of information systems.

[20] Security method, whether a security mechanism or a methodology to attain information security.

Evaluation methods are created to determine and help to improve the security of a product/information system. An Evaluation method is a form of auditing. It can be compared with financial auditing. Financial auditing verifies whether the bookkeeping is correctly performed. The security evaluation methods on the other hand, verify whether the security of an information system is correctly implemented. Notice that security does not have such a clear line between right or wrong as financial auditing has.

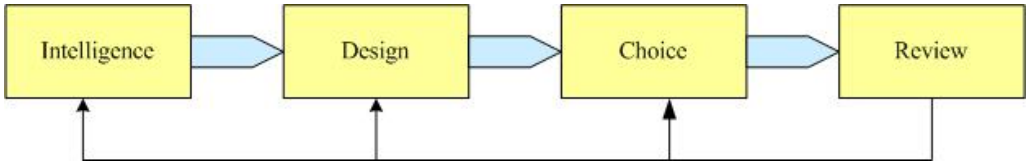


Figure 5: Security management life-cycle [Simo, 1970]

The evaluation methods, however, are not a solution to the information security problem. They are merely one step of the entire information management life-cycle. Figure 5 illustrates a management life-cycle, where review corresponds to the evaluation method. The figure shows that the evaluation method is a very important step, since it influences all the other steps. Furthermore evaluation methods can help the managers to achieve a higher level of information security.

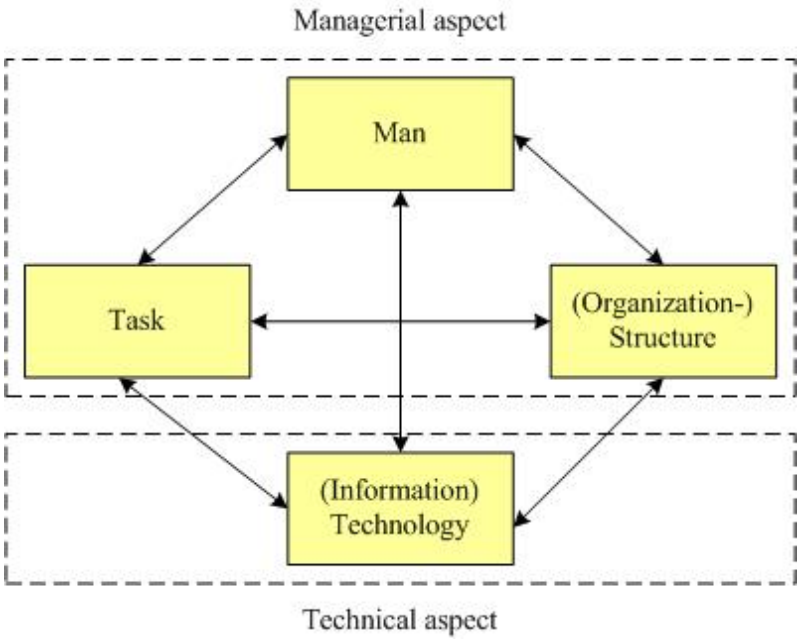


Figure 6: Evaluation methods division [Leav, 1964]

Even though, the subject is narrowed down to evaluation methods of information system security, it is still quite a broad subject. As stressed before information systems have many aspects. A frequent and often used division is to divide information systems in managerial aspects and technical aspects, as Figure 6 illustrates. The evaluation methods of information systems can be divided in a similar style. The technical evaluation can be considered as an evaluation on the actual information system (Information Technology). The managerial evaluation can be considered as an evaluation on the management of information. Information management can be divided in, personnel (Man), procedures (Task), and the organization self (Organization Structure)

The TCSEC (Trusted Computing Systems Evaluations Criteria) is an implementation of a technical evaluation method. The goal of the TCSEC is [TCSE, 1985]:

- To provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information.
- To provide guidance to manufacturers as to what to build into their new, widely-available trusted commercial products in order to satisfy trust requirements for sensitive applications.
- To provide a basis for specifying security requirements in acquisition specifications.

The British Standard on the other hand is an implementation of a managerial evaluation method. The British Standard has other objectives than the TCSEC, namely [BS1, 1999]:

> *"To give recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings."*

As the objectives shows, both evaluation methods have quite different goals. This thesis, however, focuses on the technical evaluation methods rather than the managerial evaluation methods. For the managerial evaluation methods, methods have already been developed and applied widely by many organizations. The technical evaluation methods, however, are only used for limited products and are only used by the manufacturers. This is due to the fact that the current technical evaluation methods have a few shortcomings and therefore cannot satisfy the needs of many organizations.

Another problem of the current technical evaluation methods is the reason for manufacturers to evaluate products. It is doubtful whether they really intend to assess the security of their product. Other possible reasons for manufacturers to evaluate their products are commercial aspects and legal aspects. A certification of security for a product is certainly a powerful selling point. Furthermore, some countries or instances require that their computer products have a certain minimum level of security. Thus in

order to sell a product to the military, for instance, a certain minimum level of security level is required. Thus it remains unclear why many of the classifications are conducted in the first place.

Due to these facts the current technical evaluation methods cannot be considered as adequate. For that reason this thesis developed a methodology to cope with these problems. The next chapter provides a further and a more detailed description of the current evaluation methods, while chapter 4 highlights the shortcomings of the current evaluation methods.

2.5 Summary

This chapter discussed the comprehension of an information system. An information system is basically a system that processes information. This thesis, however, focuses on a technical/computer oriented comprehension. The architecture of an information system can be derived in the following three layers:

- Application
- Operating system
- Hardware

Furthermore the term information security has been defined in this chapter. Information security can namely vary from meaning in different contexts. The essential of security is, however, to assess all the unacceptable risks and information security is no exception. For information security, the following four security requirements are defined:

- Confidentiality
- Integrity
- Availability
- Accountability

The security requirements can in its turn be divided in security services, which in its turn can be divided in security mechanisms. By implementing the appropriate security mechanisms, information security can be fulfilled.

Finally this chapter stressed why information system security is necessary.

3. Evaluation methods

This chapter discusses the current evaluation criteria for information system security and why they are necessary. The evaluation criteria have the characteristic of being quite technical focused. Therefore this chapter also briefly discusses a managerial evaluation method, namely the British Standard. Furthermore this chapter discusses which evaluation criteria are available and discusses how the evaluation criteria evolved to becoming a standard[21].

3.1 Evaluation methods for information system security

3.1.1 Technical evaluation methods

TCSEC

Evaluation methods were created with the purpose to make a well-founded judgment for the security of computer products. The urge to develop a classification method to classify computer products came from the Department of Defense (DoD) of the United States. This is caused by the fact that the DoD of the United States deals with lots of sensitive information. Relying on the commercial security talk of the manufacturers was not adequate. Rather a judgment of an impartial third party was required. To protect their information (their valuable asset as described in chapter 2), secure computer products had to be used. This had lead to the establishment of the first evaluation criteria. This model is called the Trusted Computer Systems Evaluation Criteria (TCSEC) [TCSE, 1985] or informally better known as the orange book, due to the orange cover of the TCSEC.

The TCSEC is a great initiative, but had a few shortcomings. The TCSEC, for instance, is mainly focused on the military sector. Therefore the TCSEC is only suitable for a limited set of products (namely operating systems) and is heavily focused on confidentiality of data and accountability (after all, the goal is to protect sensitive information). Furthermore the TCSEC was a bit out-of-date and was not quite accessible for other countries besides the United States. A classification of the TCSEC stimulated the sales of computer products. This led to a decrease of sales for computer products, which had not been evaluated by the TCSEC [NGI, 1995].

ITSEC

As a response to the TCSEC several other countries created a criteria scheme of their own. In Europe: England, France, and Germany were active in the field of evaluation criteria and they each had their own criteria. In 1990 these countries including The

[21] From this point forward, evaluation criteria for information system security is referred to as evaluation criteria and evaluation methods for information system security is referred to as evaluation methods.

Netherlands combined their knowledge and developed the Information Technology Security Evaluation Criteria (ITSEC) [ITSE, 1991]. The ITSEC became more accessible a broader set of products and for different countries. The ITSEC namely does not only focus on military usage, but the ITSEC focuses on commercial usage as well[22]. Therefore the ITSEC is not merely focused on the confidentiality of data and accountability, but it is rather focused on all security services (confidentiality, integrity, availability, and accountability). This has made the ITSEC such a popular evaluation criteria.

CTCPEC and FC

During the course Canada created a model of themselves, known as the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [CTCP, 1993]. The CTCPEC, however, has never been widespread used. This is due to the fact that the Common Criteria (which the next section discusses) is developed shortly after the CTCPEC. In the mean time, the United States developed the Federal Criteria (FC) [FC, 1992]. The FC was developed as the successor to the TCSEC. The FC, however, never made it through the draft version, due to the development of the Common Criteria.

Common Criteria

As the previous section already suggested, the Common Criteria (CC) [Comm1, 1999] [Comm2, 1999] [Comm3, 1999] is created shortly after the CTCPEC and the FC. The CC is a harmonization of all the previous criteria. The developers of the previous criteria realized that all the different criteria lead to confusion and made mutual recognition nearly impossible. Therefore an initiative was set up to create the CC. The purpose of the CC is to create one standard evaluation method used by all countries. The CC version 2.0 is actually opted by the International Standard Organization (ISO), namely the ISO 15408.

Figure 7 graphically summarizes the evolution of the evaluation criteria. The lines represent the influences of the other criteria. The UK confidence Levels was the national criteria scheme for England, the German Criteria was the national scheme for Germany, and the French Criteria was the national scheme of France.

[22] NGI actually claims that the ITSEC is based on the Biba (commercial) model [NGI, 1995] [Biba, 1977]. This model is mainly focused around the integrity of data. After all, in a commercial environment, preventing disclosure is often important, but preventing unauthorized data modification (e.g. fraud or error) is paramount [Clar, 1987].

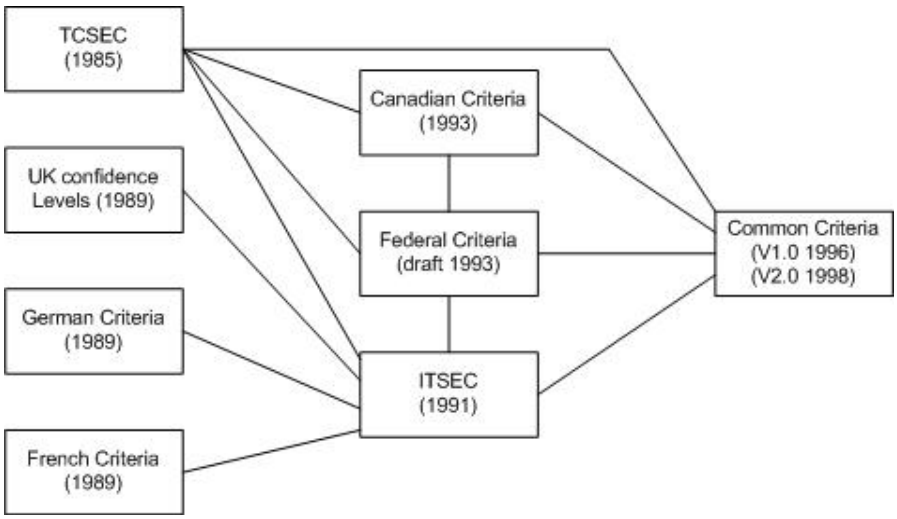


Figure 7: Evaluation of the criteria [Comm, 2003]

3.1.2 Managerial evaluation method

British Standard

As the criteria above are mainly focused on a technical level of information system security, there are also evaluation methods created, which focuses on a more managerial level. The British Standard (BS) [BS1, 1999] [BS2, 1999] is one of the most well known methods and is developed by a group of complementary organizations, with the intention to improve the operational management. This model mainly focuses on information management, ranging from security policy to physical security. The BS also deals with the technical aspect of information systems, but in much less depth. Figure 8 illustrates that the technical aspect of the information system is a part of the security management.

Figure 8: Information security management

The BS consists of two parts, which has different functions. Part 1 is a set of best practices shaped by many organizations. This part has about 148 security guidelines, which an organization can deploy. Part 2 specifies the requirements for a BS certification. An organization must comply with the relevant requirements, stated in part 2, in order to be certified against the BS.

The BS part 1 is also opted by the ISO, the ISO 17799-1 to be precise. At the time of writing, however, BS part 2 is not opted by the ISO yet. Thus one can be compliant to the ISO 17799-1, but cannot be certified against the ISO 17799-2 (yet).

The following section provides a further detailed discussion of the evaluation methods. The CTCPEC and the FC will not be further discussed, since the CTCPEC never got into the wide audience and the FC has never made it pass the draft version. The CTCPEC and FC are merely mentioned in order to get a complete view of the evolution of the criteria. Furthermore, the BS will also not be further discussed. The BS is merely mentioned in order to illustrate a managerial evaluation method. For further readings, the reader is referred to the respectively [CTCP, 1993], [FC, 1992], [BS1, 1999], and [BS2, 1999].

3.2 Trusted Computer Systems Evaluation Criteria (TCSEC)

As the previous section already gave a brief general description of the TCSEC, this part shows the internal working of the TCSEC.

The TCSEC bases the evaluation on the following four classes:

Policy
The policy class mainly deals with the access control. The access control as used in the TCSEC consists of two methods, namely the Discretionary Access Control (DAC) and the Mandatory Access Control (MAC).

The DAC is a mechanism, which defines which subject[23] may access which object[24]. As a result, the subject that holds the adequate access rights to an object (often the owner of an object) can determine who has which access rights to the particular object. The Access Control Lists (ACL) of Microsoft Windows and UNIX are examples of a DAC implementation.

A MAC is a mechanism, which does not let the subjects to manage the access rights. The access rights are rather set by the administrator and enforced by the system. The TCSEC utilizes one particular version of MAC, namely the Bell-LaPadula model [Bell, 1974]. According to the Bell-LaPadula model, a label has to be assigned to

[23] Active entity, such as user processes.
[24] Passive repository of information, such as files.

subjects and objects. Often-used labels are: top-secret, secret, confidential, and unclassified. Based on the hierarchy of the labels the following two rules are applied by the Bell-LaPadula model:

1. Subject ≥ object: subject may read the object, but may not write to the object.
2. Subject ≤ object: subject may write to the object, but may not read the object.

Figure 9 is a graphical representation of the Bell-Lapadula model, for further reference the reader is referred to [Bell, 1974].

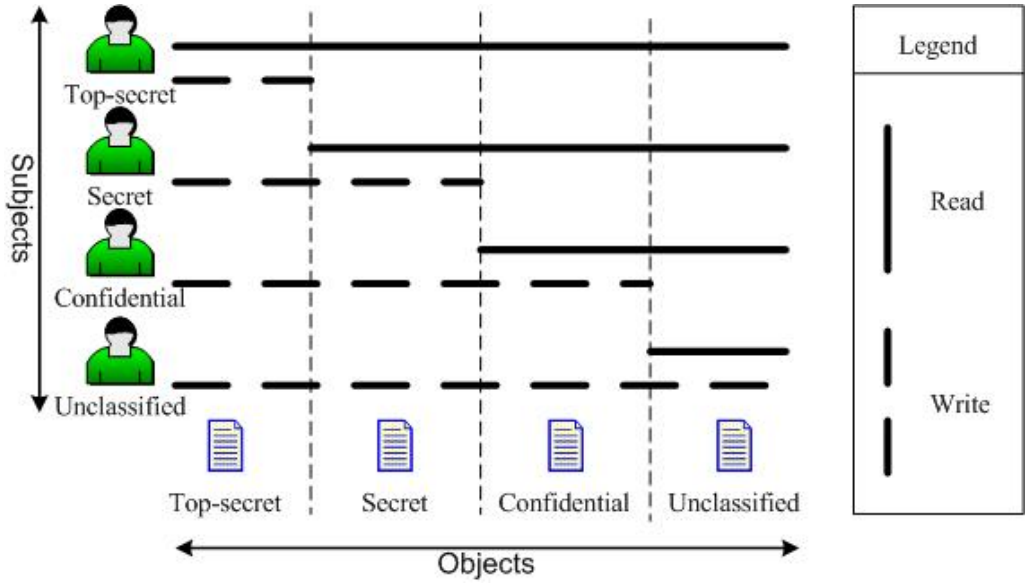


Figure 9: Bell-Lapadula model

Accountability

The accountability class makes it feasible that each action is uniquely traceable to its initiator. This class accounts for the identification and authentication of subjects. Each subject accessing the system must be identified before any other actions are allowed. The authentication part proves that the subject is indeed the subject that it claims to be. A username, for example, is the identification and the password is the evidence that the subject is indeed the certain subject (authentication).

This class also takes care of the audit. An audit monitors all events and can store the certain security relevant events. These stored events can be consulted to verify what happened and who caused the certain event.

Finally the accountability class also accounts for trusted paths. This allows an entity to communicate with another entity and to ensure that they are indeed communicating with each other and not with another (hostile) entity.

Assurance
The assurance class assures that the classes discussed above indeed provide the security as intended to. TCSEC achieves this by requiring documentation (discussed in the next section). This allows other parties to evaluate the product and the documentation to obtain a high level of assurance that the product indeed provides the security as intended. The assurance class takes the delivery and the life-cycle processes of the product into account as well.

Documentation
The final class is the documentation class. This class requires that a product at least have the following documentation: Security features user's guide, trusted facility manual, test documentation, and design documentation.

According to the classes discussed above, a security level can be attributed to the product. The security levels range from levels A to D. Each of these classes in its turn are subdivided with numbers. Level A can be considered as the most secure and level D as the less secure. For further information about the mechanisms and the classification scheme of the TCSEC the reader is referred to the TCSEC documentation [TCSE, 1985] and to the rainbow series [Rain, 2003], which are supplements of the TCSEC.

3.3 Information Technology Security Evaluation Criteria (ITSEC)

The TCSEC explicitly states, which functionalities must be present in a product (functional aspect). The ITSEC on the other hand mainly focuses on the assurance of products (assurance aspect). To elucidate the difference between functional and assurance aspects, the following classification can be used:

- Functional aspects define which functionalities must be present.
- Assurance aspects define the degree of confidence in the functional aspects.

Because the ITSEC is focussed on the assurance aspect, the ITSEC does not explicitly state, which functionalities must be present. This made the ITSEC suitable for a much broader set of products compared to the TCSEC. Besides the ITSEC is not only focused on products, but also on systems. A system is described by the ITSEC as follows: "*An IT system is a specific IT installation with a particular purpose and known operational environment*". Thus a system also takes the environment into account, which is the essential difference between a product and a system (according to the ITSEC definitions).

The evaluation of a product/system of the ITSEC is based on the following two attributes:

- Target Of Evaluation (TOE), the evaluated product/system.
- Security target, formal documentation of the TOE according to the ITSEC.

The security target can be comprised of the following components:

System Security Policy, this component is only used for systems. In case a product is evaluated the product rationale is used instead, which is discussed in the next section. The system security policy describes the procedures of dealing with information and information systems. Furthermore, the system security policy identifies the security objectives and the threats of the system. In order to satisfy the objectives and to cope with the threats, measures are described in the system security policy. These measures can be physical, personnel or procedural.

Product Rationale, is used in case a product is evaluated. The product rationale describes the intended usage of the product, the intended environment for usage, and the assumed threats of the environment. It also describes the measures to be taken in order to function as it is intended to. The product rationale is intended to provide users an overview whether the product is suitable for their situation or not.

Specification of the required security enforcing functions, this part of the security target defines the functionalities, which is provided by the TOE. The ITSEC provides ten predefined functionality classes. These are created, to prevent double work. Five of the classes are similar to the requirements of the TCSEC. The other five concentrates on a security service or a combination of the security services as described in chapter 2. In case the predefined classes are not used, the functionalities must be clearly identified.

Definition of required security mechanisms (optional), describes how the functionalities are provided.

Claimed rating of the minimum strength of mechanisms, states the strength of the security mechanism. There are three levels of strengths available namely: minimum, medium, and high.

The target evaluation level, states the intended security level of the security target. At the end of this section a description of the security levels is provided.

Even though the security target forms the basis for evaluation, other documents are needed as well. These documents describe the design of the TOE, the implementation of the TOE and the operational usage of the TOE.

Based on the TOE, the security target, and the additional documents a security level can be attributed to the TOE. The ITSEC has 7 levels ranging from E0 to E7, with E0 as the lowest level and E7 as the highest level. For further readings about the ITSEC the reader is referred to the ITSEC [ITSE, 1991].

3.4 Common Criteria (CC)

As the TCSEC is mainly based on the functional aspect and the ITSEC is mainly based on the assurance aspect, the CC tried to find a synergy between the two aspects. In order to deal with the functional requirements as with the assurance requirements, the CC has formulated a list of functional requirements and a list of assurance requirements. These two lists define the requirements, which can be applied to a product or a system. For a full list of the requirements the appendix can be consulted. For a detailed description of the requirements the [Com2, 1999] and the [Com3, 1999] can be consulted.

The CC elaborates on the method designed by the ITSEC. As with the ITSEC a TOE and a security target is required. Besides the TOE and the security target, a protection profile is required as well. A protection profile can be compared with the predefined functionality classes of the ITSEC.

Protection Profile
The protection profile is a profile for protection of a certain product/system type. There are, for instance, protection profiles designed for operating systems, databases, and smart cards. These protection profiles are based on a very global environment. Therefore these protection profiles are suitable for reuse. To use a protection profile for an evaluation of the CC, the protection profile has to be evaluated first. The protection profile contains of the following sections:

- The TOE description, this part describes the product/system, which is subjected to the evaluation.
- TOE security environment, this part describes the specific environment of the TOE like, threats, and organizational security policies.
- Security objectives, this part describes the security objectives of the TOE and the environment.
- IT security requirements, this part describes the needed functional requirements and the needed assurance requirements.
- Rationale, this part verifies whether all the requirements of the TOE security environment are covered by the security objectives.

Security Target
As the protection profile serves a more general function, the security target is tailored to a specific situation. The security target takes the environment and the threats into account. Because the security target is tailored to each specific situation the security target is not suitable for reuse. The actual evaluation is mainly based on the security target. In practice the security target is often mapped to a protection profile. The security target can also be seen as a further elaboration of a protection profile. The security target can also be derived from multiple protection profiles or from no protection profile at all. In case the security target is not based on a protection profile, the security target itself has to be evaluated in advance, in order to evaluate the product/system. Therefore the format of a security target is very similar to the format

of a protection profile. The security target actually contains all the sections from the protection profile with the following two sections in addition: TOE summary specifications and the PP claims. The TOE summary specifications specify, what is done in order to satisfy the functional and assurance requirements. The PP claims part states which protection profile is used and what the resemblance and differences are.

Based on the TOE, the protection profile, and the security target a classification can be assigned. The CC has seven levels ranging from EAL1 (Evaluation Assurance Level) to EAL7, with EAL1 as the lowest level and EAL7 as the highest level. For further readings about the CC the reader is referred to:

- [Com1, 1999], which provides a general overview of the CC.
- [Com2, 1999], which describes the functional requirements.
- [Com3, 1999], which describes the assurance requirements.

3.5 Summary

This chapter provided a brief overview of the evolution of the evaluation criteria. After the brief overview, each method was discussed in further details. As the chapter illustrated, the evaluation criteria and the managerial evaluation methods are indeed quite different. This thesis, however, is more technical oriented and focuses on the evaluation criteria rather than the managerial evaluation methods as was discussed in chapter 2.

Notice that the criteria are shifting from mainly functional based to mainly assurance based. The main cause for this shift is that functional based criteria are not suitable for a wide set of products. After all, in order to have a set of functional requirements as the TCSEC, the required functionalities have to explicitly state. As the TCSEC is designed for operating systems, it is hard to evaluate other products, which are significantly different. The functional based criteria, however, also have their advantages. After all, it forms a checklist for manufacturers to what functionalities are needed for a secure product. Moreover, it is easier for an evaluator to evaluate.

The CC made a step in the good direction, by attempting to combine the functional requirements and the assurance requirements. The actual evaluation, however, is still mainly based on the assurance requirements. The functional requirements are merely stressed in the protection profile and the security target. Furthermore, the CC made a good start by standardizing the CC. After all, it made mutual recognition of the evaluations possible.

Even though the CC is quite an improvement compared to the former criteria. The CC cannot deal with the goals set in chapter 1, namely:

- Classifications based on information systems rather than products.
- Create a methodology, which is suitable for the end-users rather than the manufacturer/vendor.

4. The Enhanced Classification Methodology

This chapter describes the Enhanced Classification Methodology (ECM) and the procedures for an ECM evaluation. It starts with an introduction, which describes why the ECM is created in the first place. Next, a general description of the ECM is presented, which generally describes the methodology of the ECM. Subsequently, all the necessary steps to conduct an ECM classification are described step by step. The final section provides a brief summary of the entire chapter.

4.1 Intention and foundation

The goal of the ECM is to create a classification model, which can verify whether an information system is secure enough for a certain context. The model should have a different approach as the current classification models. As the previous chapters discussed, the current classification models are based on products. The ECM is essentially based on information systems and has an end-user point of view instead of a vendor/evaluator point of view. The foundation of the ECM is explained in the following sections.

4.1.1 Information system oriented

Often information systems consist of a combination of different components. Therefore it is not adequate to evaluate a component alone. Rather the entire information system needs to be evaluated, because the security of an information system depends on all essential components and their interactions. In practice, however, only individual components are evaluated. An entire information system as such has never been evaluated yet.

Moreover, the current classification models have a very restricted scope. First of all the current classification models do not mandate that the entire product has to be evaluated, let alone an entire information system. Thus the evaluated products might be evaluated only for a certain subset of the product. Chances are that relevant parts of the product are not evaluated. Microsoft Windows NT version 3.5, for instance, was evaluated for a C2 rating by the TCSEC [Radi, 2003]. Often, however, when Microsoft references to the C2 rating of Microsoft Windows NT version 3.5, they tend to leave out the aspect that the C2 rating was issued to a standalone, non-distributed computing environments and non-networked device [Winn, 2003]. This implies that the system is not connected to a network, has no disk drive, cd-rom drive or whatsoever. This kind of setup is probably not very usable in practice. Thus once the Microsoft Windows NT version 3.5 device is connected to a network or has a storage medium (e.g. a disk drive), the C2 rating becomes invalid.

4.1.2 End-user point of view

Another essential characteristic of the ECM is that it is designed for the end-user to classify an information system. The current classification models are all performed by a certain accredited organization. As for the Common Criteria, the TNO-ITSEF [TNO2, 2003] is the accredited organization for the Netherlands. Thus it is not designed for an end-user to evaluate a certain product. It is not impossible for an end-user to evaluate an information system against the Common Criteria, but it is highly infeasible[25]. In case an organization wants to implement a certain unclassified product into their information system, the organization has no assurance of whether the product can be considered secure enough for the specific context. Besides, it is highly infeasible for an organization to initiate an information system evaluation, because a CC evaluation is very costly in terms of money, time, and effort. For example, an EAL3 evaluation by the Dutch TNO-ITSEF for a small to medium sized product with "good" design documentation approximately costs over €100.000 and takes over six months [TNO1, 2002]. This is probably not cost-efficient for many organizations.

4.1.3 ECM foundation

The ECM utilizes the CC as its basis. The functional requirements and the assurance requirements of the CC are used. The CC is chosen, because it provides a rich set of requirements that can satisfy the needs of the ECM. Another important issue is that the CC can be considered as the de facto standard for classification of security products. The requirements stated by the CC are therefore widely accepted.

4.1.3.1 Protection profile

As stressed in chapter 3, to evaluate a product an evaluated protection profile or an evaluated security target is necessary. There are actually several protection profiles defined and evaluated. For operating systems, for example, the following four protection profiles have been defined and evaluated:

- Controlled Access Protection Profile (EAL3/C2) [Cont, 1999]
- Labeled Security Protection Profile Version 1.b (EAL3/C2) [Labe, 1999]
- Protection Profile for Multilevel OS – Requiring Medium Robustness (EAL4 augmented/B1) [Prot, 2001]
- Single-level OS's in Environments Requiring Medium PP (EAL4 augmented/B1) [Sing, 2001]

Even though, it might seem as a good approach to only utilize evaluated protection profiles (rather than any protection profiles) there are downsides to this approach. After all, the protection profiles are developed and evaluated according to the

[25] Notice that even though a person may be capable of evaluating an information system according to the CC, the person is still not authorized to certify an information system, unless the person is accredited by the CC.

Common Criteria and can be considered as sound. The main setback of this approach is that almost all products use one of the defined protection profiles[26]. After all, it is very costly to define and evaluate a protection profile. Moreover, the protection profiles are designed for a very generic situation. As a result, this might not be suitable for the intended context.

4.1.3.2 Requirements

The classification of the Common Criteria is mainly based on the assurance requirements. The functional requirements, however, are at least as important as the assurance requirements. Since the functional requirements describe what is provided to protect the information system and the assurance requirements define the degree of trust in the functional requirements. A synergy between the two sets of requirements has to be found.

The security target of Microsoft Windows 2000 [Wind, 2002], for instance, shows that the Common Criteria classification is mainly based on the assurance requirements. Microsoft Windows 2000 used the Controlled Access Protection Profile as their protection profile. This protection profile is designed for an EAL3. Microsoft, however, added additional assurance requirements, namely a methodically design. By doing this Microsoft Windows 2000 received an EAL4 augmented classification. Notice that Microsoft has not added any additional functionality. They merely added additional assurance aspects to obtain a higher EAL than designed by the protection profile.

Moreover, the assurance requirements of the CC cannot fully satisfy the needs of the ECM. Only verifying the design and documentation is too high level. The assurance requirements of the ECM should therefore be extended by a more pragmatic approach.

4.1.4 Conclusion

The previous sections illustrated that certain classification rating cannot be fully relied on. The product is often evaluated for a certain context, which does not necessarily resemble the intended use. Actually, often only a subset of the TOE is evaluated. Besides, in case an organization wants to implement a certain product, which has not been evaluated yet, the organization does not have any assurance that the product is secure enough for the given context. Therefore it is necessary to base the ECM on information systems rather than products and utilize an end-user point instead of a manufacturer point of view.

[26] As a matter of fact, all evaluated operating systems used the Controlled Access Protection Profile as their protection profile.

The following list recapitulates the measurements to address the issues discussed above:

1) Focussing on information systems rather than products.
2) Eliminate the accredited organization and the mandatory evaluated protection profiles.
3) Allowing end-users to conduct an evaluation instead of manufacturers.
4) Take the functional and assurance requirements (extended) into account for the evaluation.

4.2 Methodology

The methodology of the Common Criteria (CC) can be roughly represented as Figure 10.

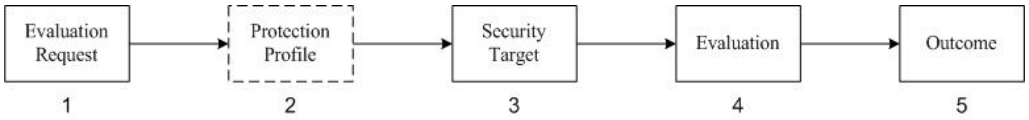


Figure 10: Common Criteria methodology

As Figure 10 illustrates, the CC can be divided in the following five steps:

Step 1 is the evaluation request. After all, there cannot be an evaluation without a request.
Step 2 is the protection profile. The protection profile is a general description of the intended environment of the product and the requirements (functional and assurance) for a certain type of product for a certain EAL. This step, however, is not obligatory and may be skipped. In case a protection profile is used, the protection profile has to be evaluated by the CC first.
Step 3 is the security target. This step is quite similar to the protection profile except for the fact that the security target is tailored to a specific product. In case a protection profile is used the security target has to map itself against the protection profile. Furthermore the security target has to prove that it covers all the relevant requirements of the protection profile. In case there is not a protection profile used, the security target has to be evaluated by the CC first.
Step 4 is the evaluation step. In this step the security target, eventually the protection profile, and the TOE are evaluated. The security target, eventually the protection profile, and the TOE are evaluated for whether they are complete and correct.
Step 5 is the outcome step. The outcome step consists of an EAL. In case security target and the TOE are evaluated as complete and correct the intended EAL of the security target is awarded to the TOE.

Based on the methodology of the CC and the measurements described in the previous section, the ECM looks as follows.

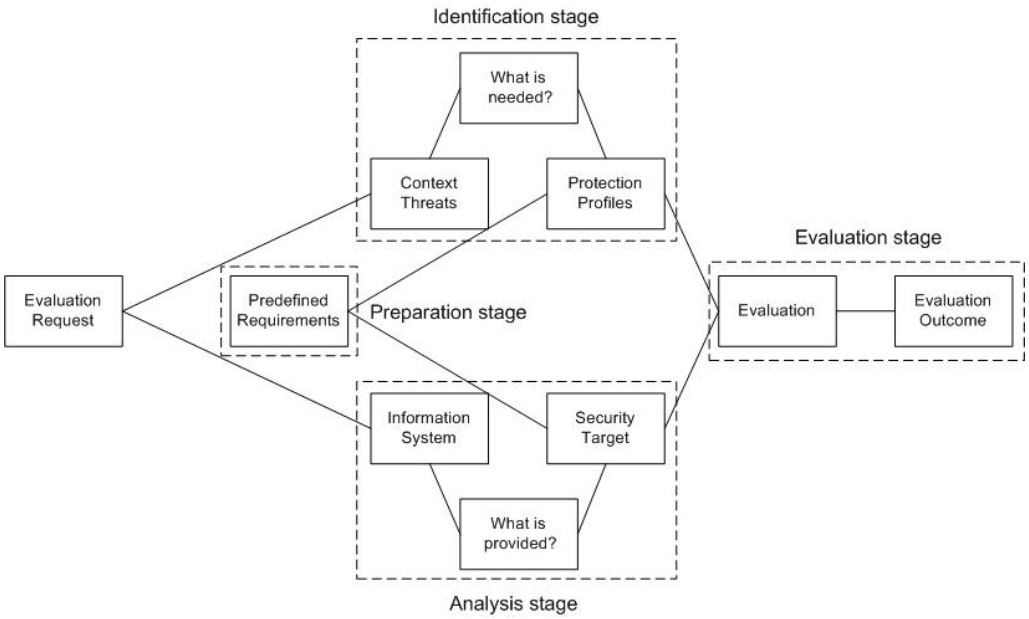


Figure 11: General description of the ECM

Figure 11 illustrates the methodology of the ECM and shows that the ECM is a modified and extended version of the CC. The ECM can be divided into four different stages as the dashed lines illustrate. The four stages are respectively:

1. Preparation stage
2. Identification stage
3. Analysis stage
4. Evaluation stage

The preparation stage: the first stage defines the functional requirements and the assurance requirements. This is necessary to prevent any inconsistencies between the documentation of the identification stage (protection profile) and of the analysis stage (security target).

The identification stage: at this stage the protection profile is created. First of all, the context threats are identified. Once the threats of the information system for a context are identified, the needed requirements to cover the threats are identified. The requirements should be chosen from the predefined requirements of the preparation stage. The threats and the requirements are subsequently documented in a protection profile.

The analysis stage: at this stage the security target is created. First of all the information system is analyzed. The analysis describes which predefined requirements are actually provided by the information system. The requirements should be chosen from the predefined requirements of the preparation stage. The requirements are subsequently documented in a security target.

The evaluation stage: at this stage the information system is evaluated. This is accomplished by verifying whether the security target complies with the protection profile.

The main difference between the CC and the ECM are the protection profile and the security target. The protection profile and the security target of the CC are almost identical. The ECM, however, makes a clear distinction between the protection profile and the security target. This is because the ECM is based on information systems rather than products. Since the ECM is based on information systems each evaluation (and thereby also each protection profile) differs. The protection profile of the ECM is intended to describe the requirements of the context, while the security target is intended to describe the functionalities of the information system.

Furthermore the methodology is intended for the end-users. In order to take this aspect into account, the methodology is kept simple and all the steps are further elaborated. Notice that the methodology is based on “what is needed” and “what is required”. In case all the “what is needed” (SOLL situation) aspects are covered by the “what is required” (IST situation) aspects, the requirements of the context are met by the information system. This concept is quite easy to understand and can be associated with a common way of problem solving problems.

Finally the evaluation outcomes of the ECM are extended compared to the CC with a functional outcome and a pragmatic assurance outcome, as is discussed at the evaluation stage.

The following sections describe each stage in further detail.

4.3 Preparation stage

Figure 12 delimits the part of the ECM, which this section discusses. The figure shows that the pre-defined requirements are defined at this stage. This is necessary to prevent any inconsistencies between the protection profile and the security target. By doing this, the evaluation stage becomes much easier to perform, since mapping two documents of the same format is probably much easier than mapping two documents of different formats.

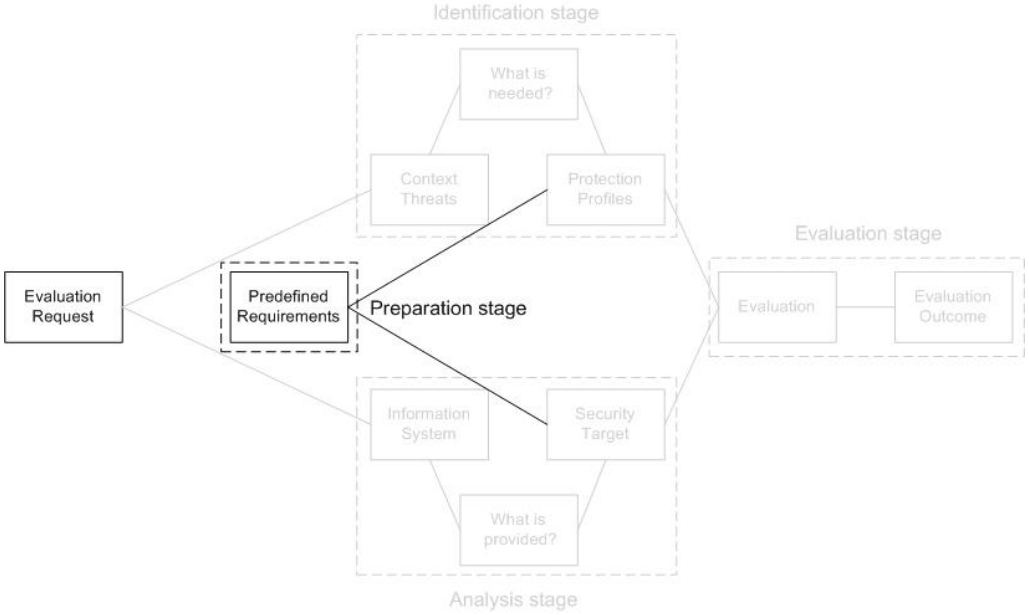


Figure 12: Preparation stage

The following sections discuss the functional requirements and the assurance requirements in further details.

4.3.1 Functional requirements

The ECM utilizes the functional requirements, which are defined in the CC. These are used, since the CC provides a very extensive set of functional requirements. The functional requirements are not restricted to a single product. A very wide variety of products can be subjected to the CC (for instance, from smart card readers to a whole chemical plant). Another important aspect of the CC is that the CC has made a clear distinction between functional requirements and assurance requirements.

4.3.1.1 Coherence of the CC classes

The functional requirements are extensively and in detail described in part II of the CC. The reader is referred to the appendix for a full list of the functional requirements and [Com2, 1999] for a detailed description of the functional requirements. The CC part II, however, only stresses the functional requirements as separate entities. The following section demonstrates how the functional requirements of the CC can be put together, regarding an information system.

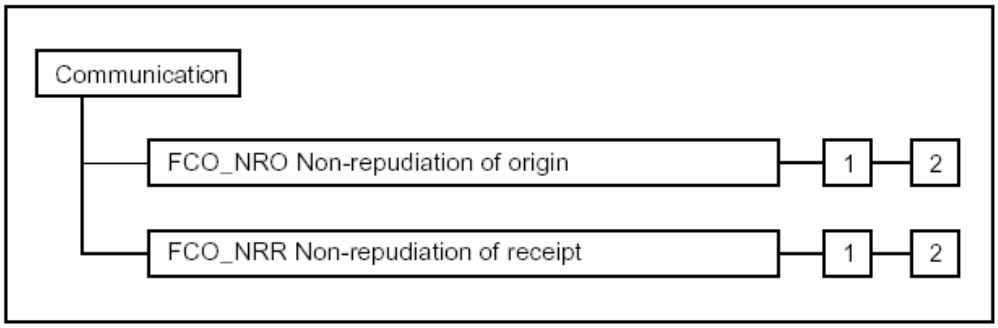


Figure 13: Common Criteria hierarchical structure example

In order to make a coherence of the CC functional requirements, the structure of the functional requirements are discussed first. The functional requirements of the CC are based on hierarchical divisions. The hierarchical divisions are divided in three layers, respectively from a high to low order: class, family, and component. A class is a name for an aggregation of families, which belongs together. A family in its turn can be derived in components. The components are the smallest entities in the hierarchical structure of the CC functional requirements. Figure 13 provides an example of one of the many classes of the Common Criteria. The figure shows the Communication class. The Communication class contains of two families, namely: FCO_NRO Non-repudiation of origin and the FCO_NRR Non-repudiation of receipt. The FCO_NRO Non-repudiation of origin and the FCO_NRR Non-repudiation of receipt in its turn both contain two components, which are indicated by the 1s and 2s.

- FCO_NRO.1: Selective proof of origin requires the TSF[27] to provide subjects with the capability to request evidence of the origin of information.
- FCO_NRO.2: Enforced proof of origin requires that the TSF always generate evidence of origin for transmitted information.
- FCO_NRR.1: Selective proof of receipt requires the TSF to provide subjects with a capability to request evidence of the receipt of information.
- FCO_NRR.2: Enforced proof of receipt requires that the TSF always generate evidence of receipt for received information.

[27] TOE Security Functions — a set consisting of all hardware, software, and firmware of the TOE that must be relied upon for correct/secure functioning.

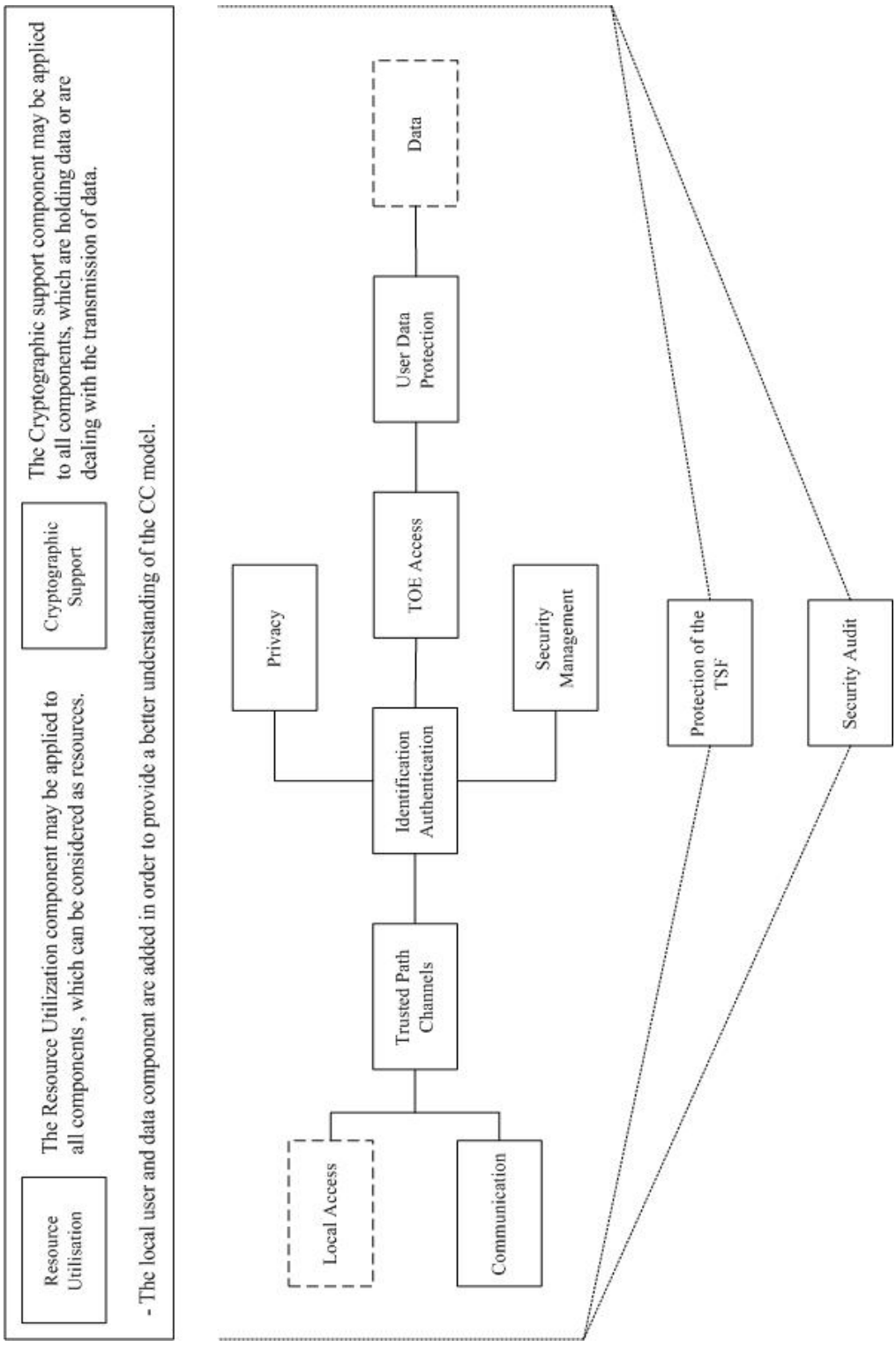


Figure 14: Common Criteria's functional requirements coherence

Figure 14 illustrates a possible information system coherence of the functional requirements of the CC. The figure is influenced by the logical access control method [Halp, 1986].

As Figure 14 shows there are two ways to access the information system, either locally (*local access component*) or remotely (*communication component*).

In order to access the information system a *trusted path/channels* can be set. This may be necessary to ensure the user that he is indeed communicating with the genuine information system.

Before any actions may be performed, the user[28] has to *identify and authenticate* himself/herself. This is necessary to enforce the security audit and the user data protection components. At the identify and authenticate component, the user has to identify himself, for instance, with a username or user number and authenticate himself, for instance, with a password by proving that he is indeed the claimed username or user number.

Furthermore the framework has the ability to enforce the *privacy* of the user. This is handled by the privacy component. This component utilizes that a user is unidentifiable by other users and/or subjects.

The CC also defined a component called the *security management* component. This component manages the rights of which user may alter which part of the TSF. Most likely this component is applicable to the administrators of the information system and users who possess additional authorities.

Once the user has been identified and authenticated for the first time, the *TOE access* component is initiated. The TOE access component manages authorities and actions at the entry of the TOE.

In case the user wants to access data of the information system, the *user data protection* component verifies with the policy whether the request of the user is authorized or not. In case the request is allowed, the information system provides the requested data to the user. In case the request is denied, the information system prohibits the user from accessing the requested data.

During the whole process the *protection of the TSF* component is active. This component protects the information system against events, which may potentially harm the integrity and the management of the TOE security functions.

Next to the protection of the TSF component, is the *security audit*. This component is also initiated during the entire process of the information system. The security audit component monitors and can save all the events of the information system in log files.

[28] Notice that user and application can be used interchangeably throughout the whole section.

By auditing the events, the user who caused an action, which violates the security policy of the information system, can be accounted for the action.

The two components (resource utilisation and cryptographic support) are depicted at the top of Figure 14 and cannot be placed in one section of the information system. The *resource utilisation* component can be applied to all resources. The CPU and the memory are examples of such resources. This component takes care for that resources are used in a way that they are intended to. Notice that this component mainly concentrates on the availability of the service.

The *cryptographic support* component can be applied to all components concerning communication or data storage. The main function of this component is to encrypt clear data to an enciphered data, which is stored or transmitted. This enforces that a malicious user, who obtains the enciphered data, is still not able to read the enciphered data. The cryptographic support naturally also has the ability to decrypt the enciphered data to plain data.

Finally notice that the *local user* and the *data* components are not taken from the CC. They are merely added to the model in order to have a better view of how the model operates.

4.3.1.2 Security services

Another issue that should be done in the preparation stage is to link the functional requirements to the security services as defined in chapter 2. The divisions of security services are necessary in order to verify which functional requirement can influence which security service.

Functional Requirements	Authentication	Access control	Confidentiality	Accountability
FCO_NRO.1				√
FCO_NRO.2				√
FCO_NRR.1				√
FCO_NRR.2				√

Table 2: Functional requirements in relation to security services

The functional requirements and the security services can be placed in a single matrix. This provides a clear overview of which functional requirements are needed for a particular security service. This matrix may differ from information system to information system. But most likely the matrix will not differ much. Table 2 provides such an example. The matrix is only a subset of the functional requirements and a subset of the security services. Furthermore the matrix reveals that the functional requirements FCO_NRO.1 & 2 and FCO_NRR.1 & 2 are relevant to accountability, but are not relevant to authentication, access control or confidentiality. The identification stage elucidates why this step is necessary.

4.3.2 Assurance Requirements

The assurance requirements of the ECM are also adopted from the Common Criteria. This is a logical step, since the ECM makes a clear distinction between functional requirements and the assurance requirements as the Common Criteria does.

The Common Criteria already defined an extensive methodology to classify a product based on the assurance requirements of the Common Criteria. The methodology to classify a product can be found in the Common Criteria part III [Com3, 1999] and in the Common Evaluation Methodology (CEM) [CEM, 1999]. Therefore the ECM utilizes the assurance part of the CEM and the CC part 3 to define the assurance requirements.

The structure of the assurance requirements is similar to the functional requirements. Thus the assurance requirements also consist of a hierarchical structure and are divided in classes, which are in its turn divided in families and in components.

The intention and foundation section already stressed that the ECM uses the assurance requirements of the CC with a pragmatic extension. This part however is postponed to the analysis stage. The pragmatic extension is namely a methodology rather than a list of requirements. Moreover the analysis stage is the point where the pragmatic extension is actually employed.

For further references of the assurance requirements the reader is referred to the Common Criteria part III [Com3, 1999] and to the Common Evaluation Methodology [CEM, 1999].

4.3.3 Additional requirements

Another important issue of the predefined requirements is that even though the requirements defined by the Common Criteria are very extensive, there is still a possibility that the functional or assurance requirements of the Common Criteria do not capture all the requirements of an entire information system. In such cases it is allowed to alter or expand the requirements of the ECM.

The security target of the Sidewinder G2 Firewall version 6.0, for example, has an additional requirement [Side, 2003]. The Identification and Authentication class is extended by a *FIA_UAU.8* - Invocation of authentication mechanisms.

In case additional requirements are added to the predefined requirements, well-founded argumentation is required. Since the additional requirements are by no means a way to undermine the predefined functional and assurance requirements.

4.4 Identification stage

The purpose of the identification stage is to define a protection profile, as Figure 15 illustrates. For a protection profile the following two steps are required:

1. Context assessment, which consists of the context threats step and "the what is needed" step.
2. Predefined requirements, which are defined in the preparation stage.

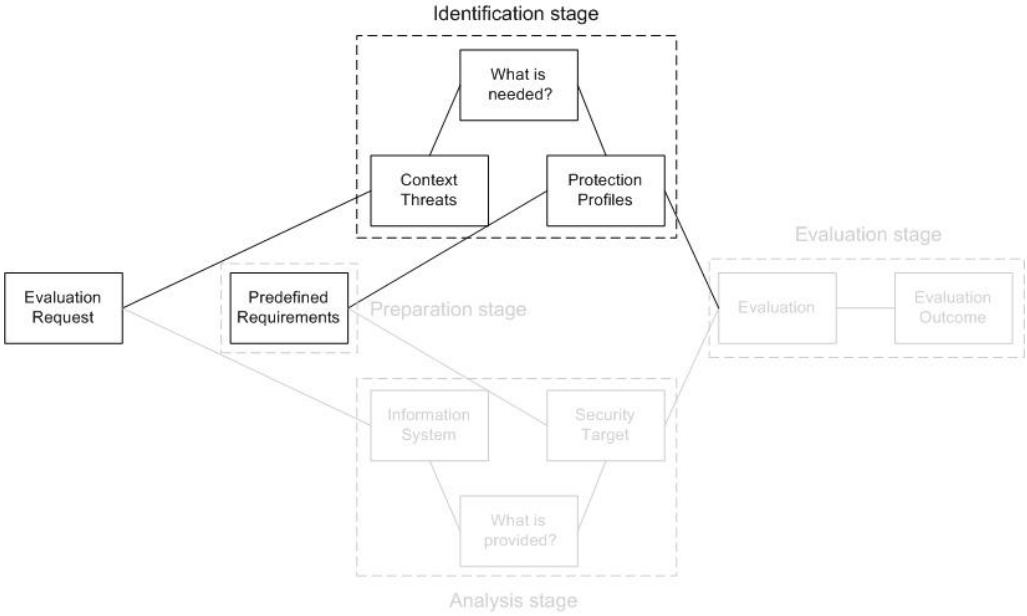


Figure 15: Identification stage

4.4.1 Context assessment

4.4.1.1 Intended use

Before the protection profile is created, the context needs to be assessed to find out the threats of the information system.

First of all, the required information system has to be identified. Moreover the intended use of the information system has to be determined. Is the information system, for instance, used as a web server, which is connected to the Internet or just to a local network?

4.4.1.2 Information system requirements

Once the intended use is determined, the critical parts of the information system are identified. Thus this step defines what is expected from the information system (information system requirements).

For a web server that is connected to the Internet and only provides public information, authentication, access control, confidentiality, and accountability might not be considered as important. After all, everyone is authorized to surf the website. Thus it is not important to determine who has visited the website (accountability) and which user has access to which part of the site (authentication, access control, confidentiality). Integrity and availability on the other hand might be considered as serious requirements of the web server. In case integrity is not safeguarded, malicious users can, for instance, alter the content of the web site. Furthermore, in case the web site is out of service (availability), exposure, revenue, reputation, trust of the company may be seriously damaged.

A backend database on the other hand might require a whole different set of security requirements. For a backend database the authentication, the access control, and the integrity of the information system might be considered as highly important. Probably only authorized users should be authorized to make any modification to the backend database. Non-repudiation, confidentiality, accountability, and availability might be considered as less relevant. These factors, however, cannot be considered as irrelevant.

4.4.1.3 Context needs

After the intended use and the information system requirements are identified, the context needs to be identified. Is the information system, for instance, only accessible to internal employees or is the information system also remotely accessible? Is the information system connected to the Internet or not?

In case a web server or a backend database, for instance, is connected to the Internet, higher security requirements are most likely needed compared to an information system, which is connected to a private network.
In case a web server or a backend database is only accessible to internal employees the security requirements are most likely lower compared to an information system, which is accessible to external users.

Thus once the intended use, the information system requirements, and the context is determined, the context requirements can be determined.

4.4.2 Requirements classification

Once the context is assessed the requirements for the particular context are determined. In the requirements classification step, a classification of the predefined requirements of the preparation stage is made. This is a step, which is made prior to the protection profile in order to make the whole process more structured and more usable for future usage.

Matrix 1				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
FCO_NRO.1				√
FCO_NRO.2				√
FCO_NRR.1				√
FCO_NRR.2				√

Matrix 2	
Req.	**Auth.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 3	
Req.	**Access.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 4	
Req.	**Conf.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 5	
Req.	**Account.**
NRO.1	L
NRO.2	H
NRR.1	L
NRR.2	H

Table 3: Requirements classification

The requirements classification step uses the pre-defined requirements as Figure 15 already illustrated. The first step to create a requirements classification is to take the pre-defined requirements of the preparation stage and separate each security service from each other as Table 3 shows. The figure shows that the original matrix (matrix 1) of the pre-defined requirements is split into four separate matrices (matrices 2, 3, 4, and 5).

Subsequently for each security service a classification of security services is assigned. As matrix 5 of Table 3 illustrates there is a classification based on L (Low), M (Medium), and H (High). The classification has an accumulative structure. Thus in case an accountability-high is desired, the functional requirements of accountability-low and accountability-medium are required to achieve an accountability-high. As matrix 5 of Table 3 illustrates, an accountability-high requires the FCO_NRO.2 and the FCO_NRR.2, but the FCO_NRO.1 and the FCO_NRR.1 are required as well.

This classification of the requirements is based on a set of requirements (whether a set of requirement set by the owner of the information system or a set of requirements based on the industries best practices) and the expertise of the evaluator. Notice that

the requirements classification takes the system usage, the information system requirements, and the context into account. Therefore it is necessary to create a requirements classification for each different evaluation. Because of the fact that the requirements classification is tailored for each context, the set of requirements can be tailored to each context as well. This is a property, which is relevant to the ECM. Thus the proper set of requirements can be used for the evaluation of a certain sector. After all, the requirements in the banking industry may differ from the requirements in the insurance industry significantly.

Thus using a general requirements classification for all situations is not a viable option. After all, each situation and each information system requires different security services as stressed in the context threats and what is needed section. Therefore the option for a requirements classification for each different situation is utilized instead of a general requirements classification.

4.4.3 Sub-protection profiles

Once the requirements classification is defined, the sub-protection profiles can be created. Recall Figure 1 of page 6, which states the layers of an information system. The sub-protection profiles define the functional requirements that are needed per component, thus per application and per operating system. The hardware layer is omitted, since security is often implemented in the software and not in the hardware. Besides, the ECM can be extended with the hardware layer or other layers (e.g. network layer) in the future.

With the requirements classification, the sub-protection profiles can be easily derived. This step determines which security services are necessary and at what level (low, medium or high). The required security services can be determined by the owner of the information system, by the person responsible for the evaluation[29], or by both. This step is important to provide the information system owner a feeling of involvement and commitment in the evaluation.

Once the security services with the corresponding levels are identified, the requirements classification can be consulted. Table 4 illustrates the working of the sub-protection profiles. As the table shows, the matrices 1, 2, 3, and 4 are the same as the matrices 2, 3, 4, and 5 of Table 3. In case a component only requires an accountability-low, the FCO_NRO.1 and the FCO_NRR.1 are required, as is illustrated in the matrix 5 of table 4. Matrix 5 forms the sub-protection profile.

[29] Assuming that the owner of the information system and the person responsible for the evaluation are different persons.

Matrix 1	
Req.	**Auth.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 2	
Req.	**Access.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 3	
Req.	**Conf.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 4	
Req.	**Account.**
NRO.1	L
NRO.2	H
NRR.1	L
NRR.2	H

Matrix 5				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
FCO_NRO.1				√
FCO_NRO.2				
FCO_NRR.1				√
FCO_NRR.2				

Table 4: Protection profile

The procedures above should be executed for the entire list of predefined functional requirements against the security services for each component of the information system separately. Thus there will be most likely at least one sub-protection profile for the operating system layer and one or more for the application layer.

4.4.4 Protection profiles

4.4.4.1 Predefined requirements

Once the sub-protection profiles are created, the protection profile of the information system can be created. The protection profile is an aggregation of the sub-protection profiles. In case two sub-protection profiles are defined as Figure 16 illustrates, the sub-protection profiles can be aggregated into one protection profile. As the figure shows a difficulty might arise, the application sub-protection profile requires an accountability-high while the operating system requires an accountability-low. The following two options are available for the protection profile:

1. Each component needs to be at least as strong as its weakest component, thus the protection profile needs an accountability-high.
2. Each component can be taken separately, thus the protection profile has two values, namely accountability-high for the application and accountability-low for the operating system.

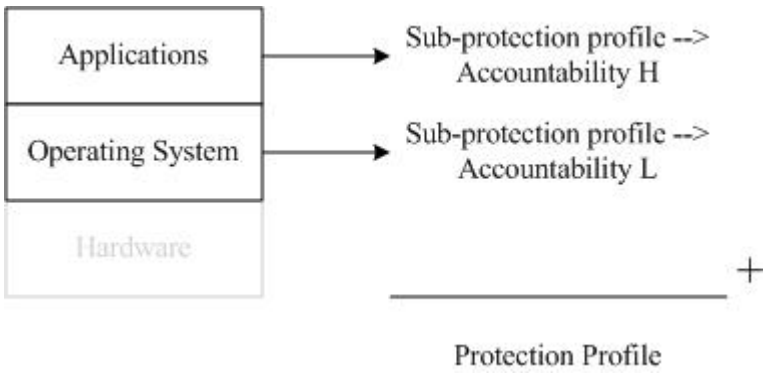


Figure 16: Protection profile

Since the previous step identified the necessary functional requirements, the following step is to create the actual protection profile. Protection profiles are written in specific formats. Before the format of the protection profile is discussed, a graphical summary of the steps to create a protection profile is provided by Figure 17 .

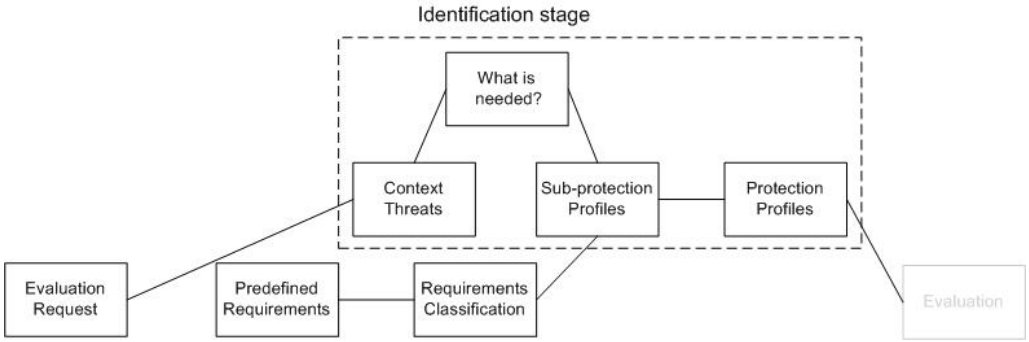


Figure 17: Protection profile overview

4.4.4.2 Protection profile documentation

Once the functional requirements of the protection profile are determined, all the identification stage steps are documented in a protection profile. After all, the protection profile is what this step is trying to create. The formats between the protection profile and the security target[30] are predefined. By having the same formats between the protection profile and the security target simplifies the evaluation stage significantly.

The format of the protection profile of the ECM follows the line, which is set throughout the identification stage. The line throughout this stage is actually quite similar to what the Common Criteria has described in their protection profile.

[30] Which is discussed in the next section.

The format of the protection profile defined by the ECM should look as follows:

Context threats and what is needed
- Intended use
- Information system requirements
- Context needs
- Requirements classification

Requirements (sub-protection profile and protection profile)
- Functional requirements
- Assurance requirements[31]
- Additional requirements

Figure 18 illustrates the protection profile format as the Common Criteria employs [Com1, 1999]. The figure shows that many parts are similar to the ECM protection profile format. The intended use corresponds to the TOE description. The information system requirements and the context needs parts correspond to the TOE Security environment. The Security services requirements correspond to the security objectives. The requirements (functional, assurance, and additional requirements) correspond to the IT security requirements.

Even though the correspondences might not be exactly the same between ECM and the Common Criteria, they deal with similar issues. The ECM however, does not address the PP introduction and the rationale parts. Even though the ECM does not address these points, they are allowed optionally. The protection profiles of the ECM are considered as an internal document and not as a public document as the protection profiles of the Common Criteria are. Therefore these points are not mandatory, but they can come in handy. A PP introduction, for example, is highly advisable to employ.

[31] Notice that the ECM has not set a methodology for the assurance requirements. For a methodology of the assurance requirements the Common Criteria part III can be consulted.

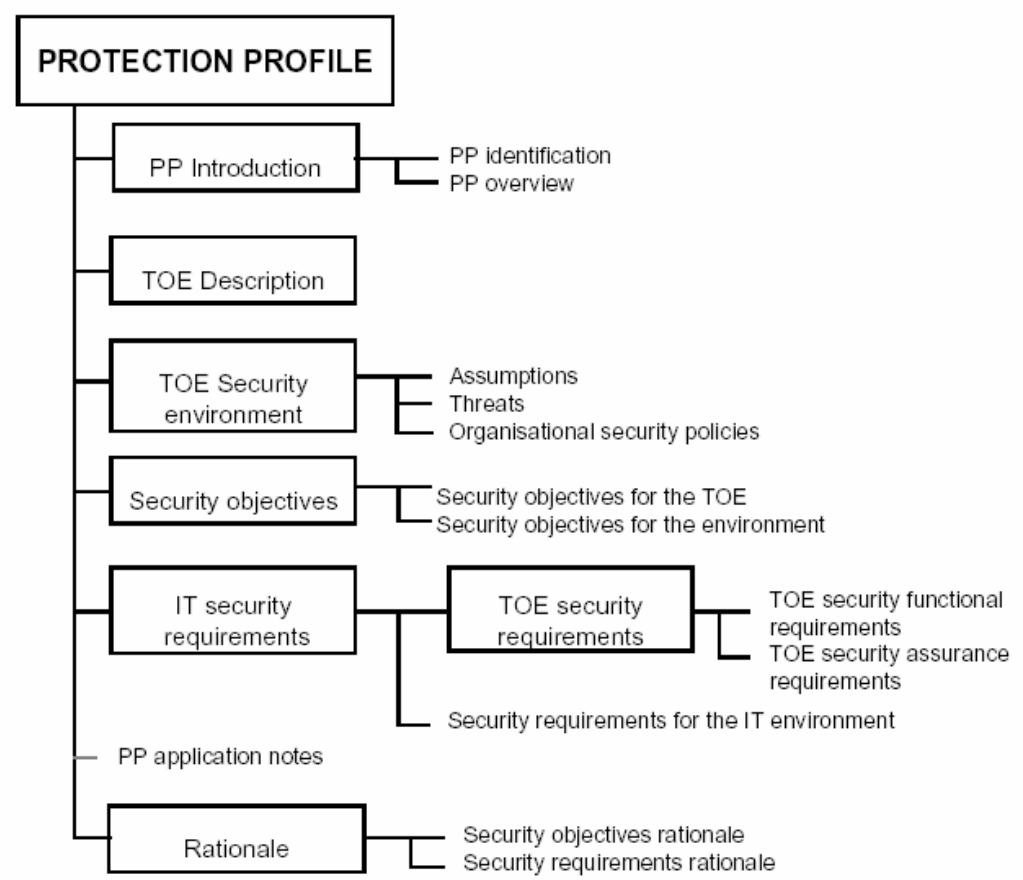


Figure 18: Common Criteria protection profile format

4.4.4.3 Reusability

The sub-protection profiles and protection profiles are actually reusable and can be created templates can be created based on the sub-protection profiles. Once the sub-protection profile for a certain context is created, it is also valid for other information systems with a similar context. Thus once sub-protection profile for a web server is created for company X then company Y can also use it, in case their context is similar.

Table 5 illustrates how the sub-protection profile can be reused. The matrices ranging from 1 to 5 are identical as was discussed at the sub-protection profile section.

In case another protection profile has to be created, with practically the same context, but with different security services, the sub-protection profiles can be reused. For instance, the context requires accountability-high. Matrix 4 shows that functional requirements FCO_NRO.1, FCO_NRO.2, FCO_NRR.1, and FCO_NRR.2 are required. This leads to matrix 6. By using this method the preparation stage and the requirements classification step can be skipped.

Matrix 1	
Req.	**Auth.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 2	
Req.	**Access.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 3	
Req.	**Conf.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 4	
Req.	**Account.**
NRO.1	L
NRO.2	H
NRR.1	L
NRR.2	H

Matrix 5				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
FCO_NRO.1				√
FCO_NRO.2				
FCO_NRR.1				√
FCO_NRR.2				

Matrix 6				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
FCO_NRO.1				√
FCO_NRO.2				√
FCO_NRR.1				√
FCO_NRR.2				√

Table 5: Protection profile reusability

Furthermore once a requirements classification for a certain component is created a template for similar components with different security services requirements can be created. For instance, a template can be created for a certain component (an application for example). The application, for instance, can be classified as non-critical, critical, and highly critical. Based on the criticality security services can be attributed[32] to the type of application. A non-critical application, for instance, requires an accountability-low. While a critical application and a highly application component require an accountability-high, as is illustrated in matrix 5 of Table 6. Notice that the matrices 1 to 4 of Table 6 are similar to the first four matrices of Table 5.

In case a sub-protection profile for a non-critical application is needed, accountability low is required, as matrix 5 of Table 6 shows. Looking at the matrix 4 of Table 6 leads to the requirements FCO_NRO.1 and FCO_NRR.1, as is illustrated in matrix 6 of Table 6.

In case a critical component or a highly critical component is needed, an accountability-high is required, as matrix 5 of Table 6 shows. Looking at the matrix 4

[32] The attributing security services to components based on their criticality can be done based on past experiences or on research.

of Table 6 shows that requirements FCO_NRO.1, FCO_NRO.1, FCO_NRR.1, and FCO_NRR.2 are required.

Matrix 1	
Req.	**Auth.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 2	
Req.	**Access.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 3	
Req.	**Conf.**
NRO.1	
NRO.2	
NRR.1	
NRR.2	

Matrix 4	
Req.	**Account.**
NRO.1	L
NRO.2	H
NRR.1	L
NRR.2	H

Matrix 5				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
Non-critical				L
Critical				H
Highly critical				H

Matrix 6				
Functional Requirements	**Authentication**	**Access control**	**Confidentiality**	**Accountability**
FCO_NRO.1				√
FCO_NRO.2				
FCO_NRR.1				√
FCO_NRR.2				

Table 6: Protection profile templates

4.5 The analysis stage

Subsequently or in parallel to the identification stage the analysis stage can be performed. The purpose of the analysis stage is to define a security target, as Figure 19 illustrates. For a security target the following two steps are required:

1. Information system assessment, which consists of the information system step and “the what is provided” step.
2. Predefined requirements, which are defined in the preparation stage.

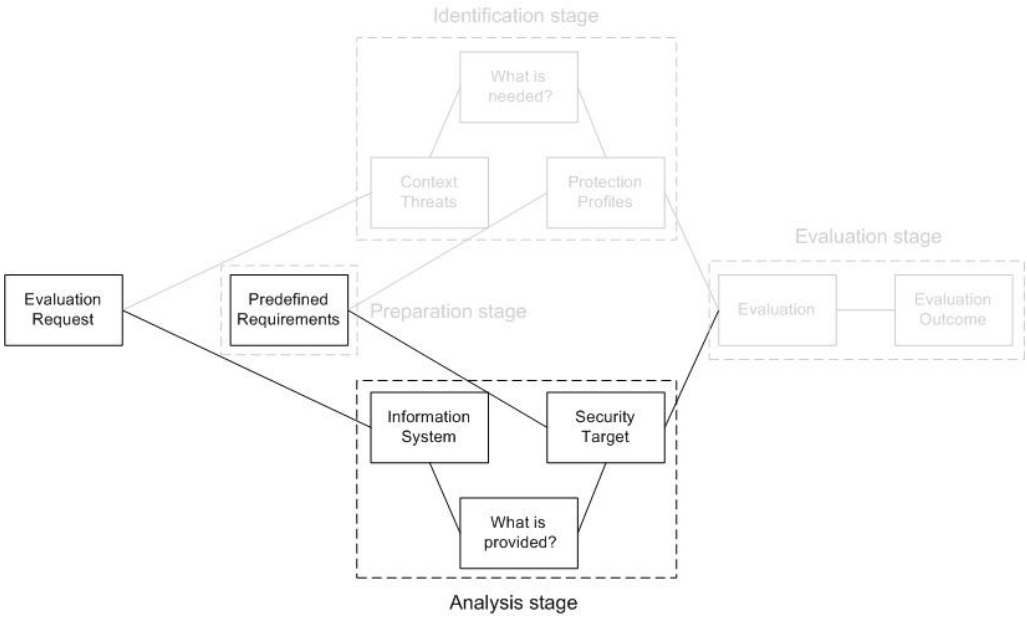


Figure 19: Analysis stage

4.5.1 Information system and what is provided

Figure 19 shows that the goal of the analysis stage is to create a security target. Before a security target can be created, the information system has to be assessed in order to find out what functionalities are provided by the information system. Notice that the context does not influence this step. Furthermore, this step deals with the entire information system rather than a subset of the information system. Due to the fact that the entire information system is assessed the outcomes can be easily used for future usage. In case only a subset information system is evaluated future use is quite limited.

In the information system step, the components (applications, operating system) of the information system are identified first. Once the information system is determined**,** the functionalities of the information system can be defined. The functionalities are identified according to the predefined requirements. Thus the predefined requirements can be used as a checklist to which security functionalities are present in the information system. By having all the available requirements according to the predefined requirements, "the what is provided" step is created.

The information system assessment can be simplified by doing research. In case the information system already has been assessed by the Common Criteria, for instance, the results of the assessment of the Common Criteria can be used as a baseline. Since the Common Criteria often only evaluates a subset of a product, the outcome can be only considered as a baseline and no more. Another point may be to search for the

documents provided by the manufacturer. Often these documents extensively describe the working and security features of their products.

4.5.2 Security target format

Once the functional requirements of the information system are identified, all the steps are documented in the security target. The format of the security target is quite similar to the protection profile. The main difference between the security target and the protection profile is that the security target describes the information system, while the protection profile describes the context.

The format of the security target defined by the ECM should look as follows:

- Information system step (defining the information system and its components)

Requirements (What is provided step)

- Functional requirements
- Assurance requirements
- Additional requirements

The format of the ECM security target differs from the CC security target significantly, as Figure 20 shows. The security target of the CC is namely more extensive compared to the security target format used by the ECM. Figure 20 shows that the security target and the protection profile of the CC shows a lot of resemblance. The format of the CC security target is actually practically the same as the format of the CC protection profile. The CC security target only has two sections added compared to the CC protection profile, namely the TOE summary specification and the PP claims. The TOE summary specification describes how the IT security requirements are met by the information system. The PP claims describes how the security target matches the corresponding protection profile.

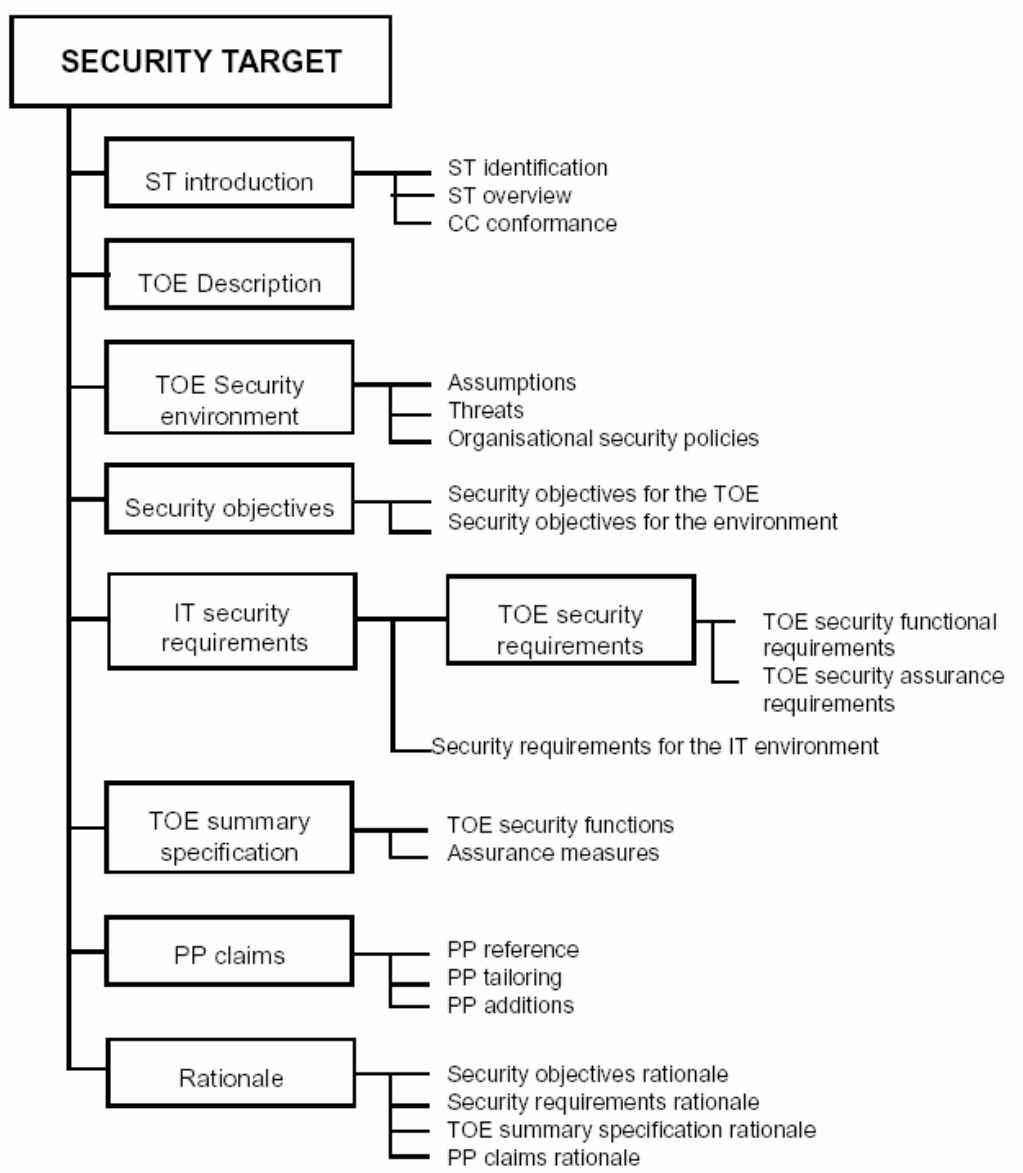


Figure 20: Security target format

The CC has such an extensive security target, due to the fact that the CC utilizes general protection profiles. In case a security target utilizes a protection profile, the security target is required to be mapped against the protection profile. Thus the security target must demonstrate that all requirements of the protection profile are present in the security target.

The security target of the ECM, however, does not need the sections, which are already stressed in the protection profiles. For each evaluation the protection profile is

tailored to a specific context. The security target on the other hand describes the entire information system. Therefore the security target does not need to justify that the context described in the protection profile is also applicable to the security target. Therefore the simple security target format of the ECM can be justified.

In case a comparison is made between the security target of the ECM and the security target of the Common Criteria, the following results can be noted. The ST introduction and the TOE description is quite similar to the information system and "the what is provided" part. The TOE summary specification is comparable to the security target format section. As with the protection profile, these parts show resemblances, but are not identical.

Notice that the combination of protection profile and security target must be verified. After all, it is possible, that the used protection profile and the used security target are not applicable to a certain context at all. This step, however, is postponed to the evaluation stage.

4.6 The evaluation stage

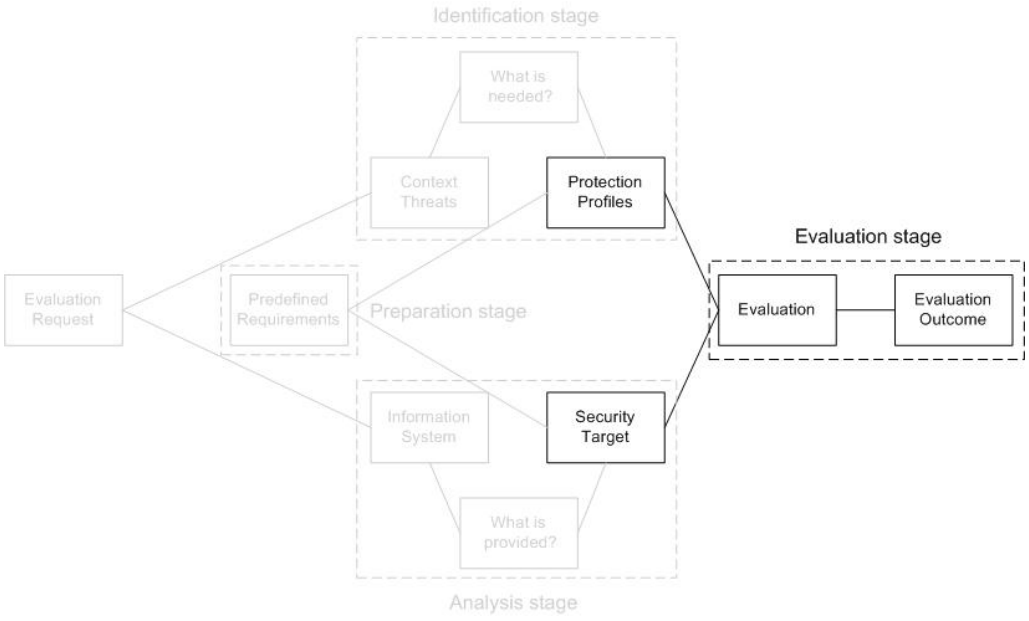


Figure 21: Evaluation stage

The evaluation stage is the final stage of the ECM. The purpose of the evaluation stage is to determine whether the protection profile matches the security target. Thus this stage verifies whether all requirements of the context are covered by all the

functionalities of the information system. To perform the evaluation stage the following two documents are required:

1. Protection profile
2. Security target

The first step is to verify whether the protection profile and the security targets are correct and complete. The protection profile has to be verified whether it covers all the threats. The security target has to be verified whether all the functionalities described in the security target are indeed provided by the information system. Finally the functional evaluation and the assurance evaluation can be performed.

4.6.1 Functional requirements evaluation

Once the protection profile and the security target are verified the functional evaluation process can be performed. Due to the clear distinction between "the what is needed" section (protection profiles) and "the what is provided" section (security target), the evaluation stage can verify whether the functional requirements of the context (needs) are met by the functionalities of the information system (functionalities). Comparing the following attributes can utilize the functional requirements evaluation of an information system:

- Functional needs → functionalities
- Additional needs → additional functionalities

In case all the functional and the additional needs are met by the functionalities and the additional functionalities, the evaluation stage can conclude that the information system is compliant to a predetermined requirement (e.g. best practice). In case the needs are not met by the functionalities the information system can be considered as not compliant to a predetermined requirement. In such cases the ECM can identify which parts did not satisfy the predetermined requirement.

4.6.2 Assurance requirements evaluation

The evaluation of the assurance requirements and the additional requirements are based on the methodology defined by the CC part 3 and the CEM. This is done in order to keep compatibility between the ECM and the CC. After all, the CC is probably the best-known classification model and is generally accepted by the wide audience. Therefore the classification of the CC is preserved for the assurance requirements.

The assurance requirements defined by the CC however are extended by a pragmatic extension. This part of the assurance requirements compares the security services against the security mechanisms defined by a certain best practice. This part may vary

from each evaluation. After all, there might be different best practices for each different context.

	Low (weak)	Medium (normal)	High (strong)
Authentication	Username/password combination	Username/password with policy	Multiple passwords/ alternative methods

Table 7: Pragmatic assurance extension

Table 7 is an (fictional) example of such a (subset of) best practice. As the table shows, for an (weak) authentication-low a regular username/password combination is sufficient. For an (normal) authentication-medium a username/password with a policy is required. The policy, for instance, should state the minimum password strength, by means of length, time, and usage. For an (strong) authentication-high a multiple username/password combination or alternative methods are needed as in, tokens, biometric authentication schemes.

In case an information system requires an (strong) authentication-high then the information system should according to the best practice have multiple passwords or alternative methods. Thus the information system can be compliant to the best practice or not. In case the information system is not compliant to the best practice, the ECM can identify the lacking parts.

4.6.3 Evaluation outcome

The outcome of the ECM consists of two sections, one for the functional requirements and one for the assurance requirements. The functional requirements can be compliant to a predefined requirement or not. The assurance requirements are similar to the classification form of the Common Criteria. Thus the outcome is divided in 7 EALs, which indicates what the level of assurance is. Furthermore the assurance requirements are extended by the pragmatic extension. The pragmatic extension can be compliant to a predefined best practice or not.

The compliancy method is chosen intentionally instead of extending the EALs by adding the functional requirements and the assurance pragmatic extension to each EAL. The main reason to choose for the compliancy method is that companies often do not care whether their products or their information system possess a certain security level or not. They rather want to know whether they are compliant to the industries best practices or not. The EAL are kept, however, to provide a yardstick for the ECM to the CC.

Notice that it might be hard for a person to identify which level of assurance is required for a certain information system. The functional requirements (security services) on the other hand are easier to determine. Therefore a variant of the ECM is

also possible. It is, for example, also possible to only determine the functional requirements in the protection profile and the security target. The assurance part of the evaluation is then postponed to the evaluation stage. By doing this, the information system can still be verified for whether it is compliant to the industries best practices and provide a level of assurance for the information system. Afterwards the level of assurance should be analyzed, for whether it is acceptable or not.

4.7 Summary

This chapter described the ECM, which is a variant of the Common Criteria. The ECM is created, due to the fact that the current classification models cannot satisfy the needs of the ECM. The ECM utilizes the requirements, which are defined by the Common Criteria. The main advantages of the ECM are:

1. Focussing on information systems rather than products.
2. Eliminate the accredited organization and the mandatory evaluated protection profiles.
3. Allowing end-users to conduct an evaluation instead of manufacturers.
4. Take the functional and assurance requirements (extended) into account.

The ECM is divided in four stages, respectively: the preparation stage, the identification stage, the analysis stage, and the evaluation stage.

Recall Figure 11 of page 32, which illustrates how the stages are put together. First of all there is an *evaluation request*. In order to evaluate the information system the functional requirements and the assurance requirements have to be determined at the *preparation stage*. This is done in order to prevent any inconsistencies between the protection profile and the security target. Once the functional requirements and the assurance requirements are determined the *identification stage* can be performed. This stage the requirements for a certain context and subsequently results in a document called the protection profile. The *analysis stage* can be performed subsequently or parallel to the preparation stage. This stage describes the functionalities of the information system and subsequently results in a document called the security target. After the identification stage and the analysis stage the *evaluation stage* can be performed. The evaluation stage matches the protection profile (what is needed) and the security target (what is provided). In case all the needs are covered by the provided functionalities, the information system can be considered as compliant to the ECM and in case all the needs are not covered by the provided functionalities, the information system can be considered as not compliant to the ECM. Furthermore there is also an assurance part, which evaluates the assurance of the information system.

5. The Enhanced Classification Methodology test case

The previous chapter introduced the concept of the ECM. This, however, does not end the discussion. This chapter shows that the ECM is not merely a cerebration and demonstrates that the ECM quite is suitable for practical use. As the saying goes, *"In theory, practice is the same as theory. In practice it is not"*. To show that the ECM is suitable for the practice a test case is conducted. This chapter is the result of that test case.

5.1 Framing the test case

Before the test case is discussed the goals of the test case have to be defined first. The test case should demonstrate that the ECM is well founded and suitable for the practice. The following list summarizes the goals that are set for the test case.

1) Verify whether the ECM is complete.
2) Verify whether the ECM is applicable in practice.
3) Verify whether the ECM is suitable as a service to customers.
4) Verify whether all components need to be as "secure" as the overall information system.

The test case is conducted on an actual organization. Due to privacy reasons the name of the organization and the results of the ECM evaluation are not published. Besides, we are not interested in the results of the test case, we should rather be interested in whether the ECM can satisfy the goals or not. But in order to create an impression for the readers, a global description of the organization and the evaluation is provided in the following sections.

The organization of the test case possesses an online transaction system and heavily relies on it. Roughly 80% of the customers utilize the online transaction system, rather than the "old-fashioned" manual manner. Furthermore, the online transaction system is involved with large amounts of money and a lot of sensitive data. Therefore the online transaction system is of great importance to the organization and need to be well secured.

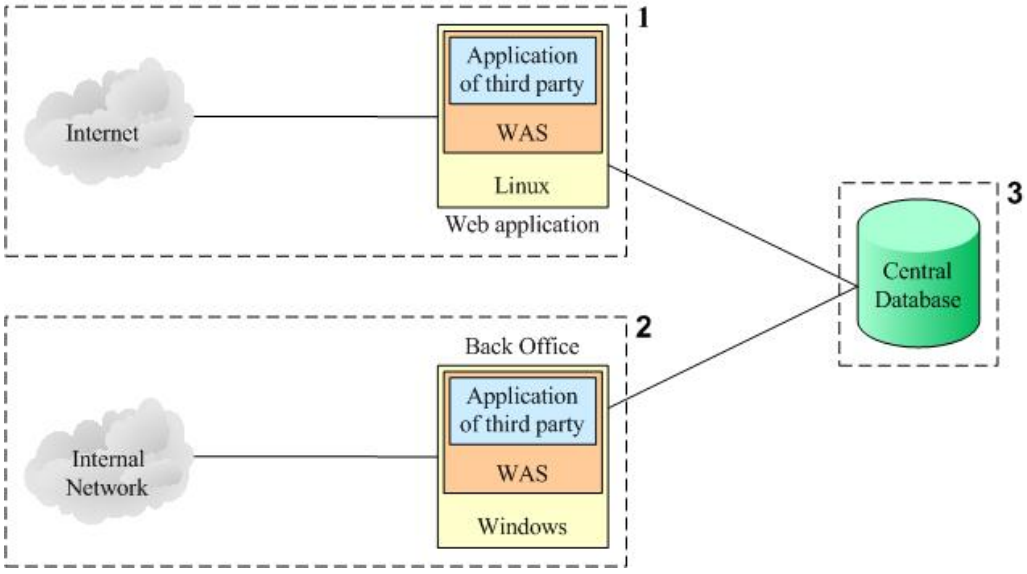


Figure 22: Architectural design of the test case

Figure 22 illustrates the architectural design of the organization. Notice that this is a simplified version of the actual architectural design. Components as the firewall, the router, and the proxy server are left out, since they are not relevant in this example. As the figure illustrates the information system can be roughly divided in the following three segments:

1) Web application
2) Back office
3) Database

The *web application* is connected to the Internet and allows the customers to enter transactions into the online transaction system. Furthermore, the web application allows the customers to view the processed and the ongoing transactions. The transactions of the online transaction system are not stored in the web application, but all the transactions are rather stored in the central database.

The *back office* is connected to the internal network and allows the personnel of the organization to view the status of transactions of the customers. This information is necessary for the personnel to be able to provide support to the customers. Furthermore, the back office allows the personnel to insert new customers into the online transaction system. As was the case with the web application, all the data of the back office are stored in the central database.

Due to the time constraints, the scope of the test case is limited to the web application and the back office. The central *database* is left out of the scope. This is done deliberately, since a lot of effort had already been put in reviewing and improving the

security of the central database. The reviewing and improving the security of the central database was not done by the author, but by a third party.

The web application and the back office are running on separate computer systems. As Figure 22 illustrates, the web application and the back office consists of the following three components, namely:

- Operating system
- Application server
- Application by third party

As is partly illustrated in Figure 22, the web application consists of a Redhat Linux operating system, an IBM Websphere Application Server (WAS), and an application developed by a third party. The back office does not differ from the web application very much. The back office namely consists of a Microsoft Windows operating system, an IBM Websphere Application Server (WAS), and an application developed by a third party. Notice that the main difference between the web application and the back office are the operating system and the application build by the third party. Furthermore, both of the applications running on top of the application servers are developed by the same third party. Therefore they have a lot in common. But since they both serve for different purposes and possess different functionalities, they cannot be considered as the same. Thus the information systems show some resemblances, but are not similar.

5.2 Preparation stage

In order to gather all the necessary information for the ECM evaluation interviews were conducted. The test case intentionally chose for interviews rather than verifying information system from a workstation of the organization. First of all, the test case did not want to take too much time and resources of the organization. Furthermore, the web application and the back office are both production machines. The organization cannot afford an accidental interruption of one of those machines. In case one of the machines was accidentally interrupted it could lead to a dramatic loss of revenue and loss of the customers' trust.

Prior to the interviews research had been done to gather all the available information that can be relevant to the interviews. This was done by analysing the internal documents of Ubizen and by searching the Internet. As the saying goes *"a good preparation is half the work"*. The research prior to the interviews was concentrated on the organization and on the information systems of the organization. First of all, the organization was analysed for the type of business they are in and what their information systems serve for. After the organizational research the information systems were analysed. Each of the components of the information system was identified and subsequently analysed.

After having gathered all the necessary information, the questions for the interviews were set up. There were two interviews taken for the test case.
The first interview was mainly focused on the organizational issues. This interview was intended to get a general view of the organization and its information systems. Issues like, what the organization does and what is expected from the information system were stressed in this interview. The following questions were for example asked during the first interview for the identification and authentication part:

- Are there explicit measurements taken for accountability? For example, are the owners of a user account fully responsible for his/her actions?
- Are there specific requirements set for the passwords?

The second interview was mainly focused on the technical issues. This interview was intended to get a clear view of the design and the functioning of the information systems. Issues like, how does the architecture of the information system look like and how does the information system work were stressed in this interview. The following questions were for example asked during the first interview for the identification and authentication part:

- How does the certificate system of the online transaction system exactly work?
- Is encryption employed to the password files?

The interviews can be considered as adequate, since they practically covered all the necessary information for the ECM evaluation. Parallel to the two interviews, the preparation stage of the ECM was performed. This stage went according to the ECM and no big deviations occurred. The only deviation that occurred at this stage was that all the functional requirements were divided into security services. Thus the unnecessary functional requirements were divided as well. The elimination of the unnecessary functional requirements was postponed to the identification stage and the analysis stage. This is done on purpose, since we probably have a better overview of the actual needs at those stages. Besides, it is better to have unnecessary functional requirements than accidentally leaving out necessary functional requirements. Table 8 illustrates a division of a subset of the functional requirements (the identification and authentication class) into security services. As the table shows, all the components are relevant for the authentication security service. Furthermore the user-subject binding component is also relevant for the access control security service. In this style the rest of the classes are linked to the security services as well.

Identification and Authentication	Auth.	Access	Conf.	Int.	Avail.	Accoun.
Authentication failures						
1. Authentication failures	√					
User attribute definition						
1. User attribute definition	√					
Specification of secrets						
1. Verification of secrets	√					
2. Generation of secrets	√					
User authentication						
1. Timing of authentication	√					
2. User authentication before any action	√					
3. Unforgable identification	√					
4. Single-use authentication mechanisms	√					
5. Multiple authentication mechanisms	√					
6. Re-authenticate	√					
7. Protected authentication feedback	√					
User identification						
1. Timing of identification	√					
2. User identification before any action	√					
User-subject binding						
1. User-subject binding	√	√				

Table 8: Functional requirements division in security services

The organization did not make any assurance requirements at this stage. After all, one has to be familiar with the CC, in order to set an EAL target. Therefore the actual assurance evaluation of the products was postponed to the evaluation stage.

5.3 Identification stage

After the information gathering, the identification stage was conducted. In order to conduct the context assessment a combination of the ECM and the CC was used. This was done, because the ECM did not explicitly define a method for the context needs. Therefore the ECM was used for the intended use and the information system requirements steps, while the context needs step was based on the CC.

Even though the test case utilized the CC method for the context needs step, it did not use the exact method of the CC. To be suitable for the test case some modification had to be made. The method used for the test case was as follows:

1) Define the security needs of the organization.
2) Make the necessary assumptions/demands.
3) Identify the threats on the information system.
4) Determine the security requirements of the information system.

Step 1 - The organization have not explicitly defined their security needs. Therefore security needs had to be defined by the author. This is done by combining CC's protection profiles and security targets, best practices and own perception. One of the security needs was for example:

Identification and authentication	All users must identify and authenticate himself/herself prior to accessing the resources of the information system, with exception to the public resources.

Step 2 - These assumptions/demands were outside the scope of the ECM evaluation. They are, however, essential to the organization. In case the organization cannot satisfy these assumption/demands, the security of the information system cannot be safeguarded.

For this step the same resources as step 1 were consulted. This made step 2 quite easy to perform and showed no significant difficulties. One of the assumptions/demands was for example:

Secrecy	All the users have to keep "secret" data confidential and not reveal them to others. Transactions and passwords are example of such "secret" data.

Step 3 - While step 1 and step 2 were quite straightforward, step 3 on the other hand was harder to perform. After all, it is not easy to identify all the threats of an information system. Therefore sequence diagrams were made for the web application and the back office. By having all the steps defined in the sequence diagrams, a more systematic approach of assessing the threats had been created.

Figure 23 shows the sequence diagram of the web application. The web application can be divided in two parts. One part is the website for public information. The other part is for the online transaction application. Furthermore the connection between the customers and the online transaction system is by the Internet. The connection between the online transaction system and the database, however, is by the internal network.

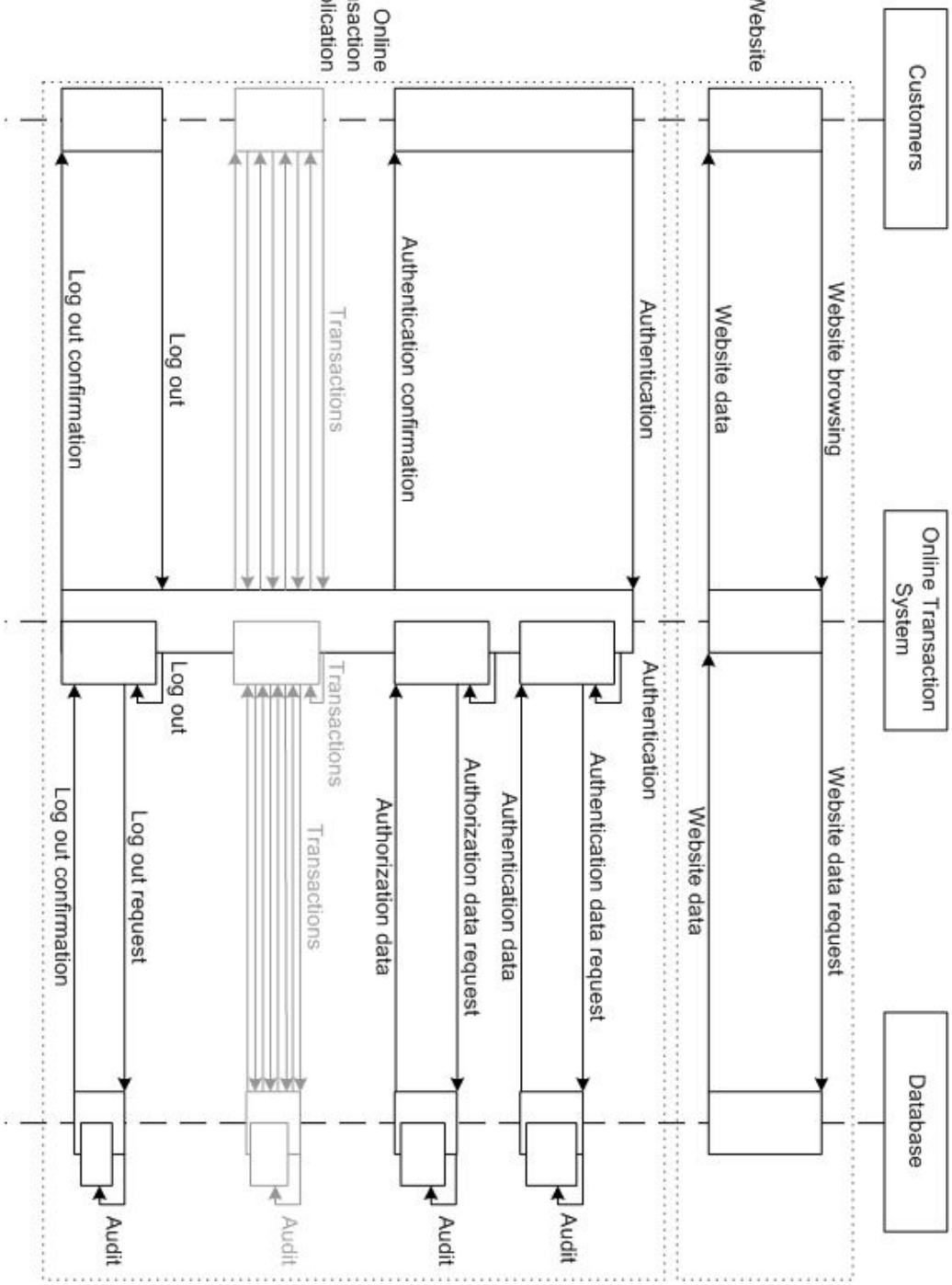


Figure 23: Web application sequence diagram

Figure 23 shows that customers have to authenticate themselves before accessing the online transaction application. First of all, the customer has to send the (identification and) authentication data to the online transaction system. Subsequently the online transaction system starts a process to verify the provided authentication data (e.g. username and password). In order to attain the authentication data the online transaction system sends an authentication data request to the database. The database thereupon provides the authentication data to the online transaction system. While the database receives the request for authentication data and sends the requested authentication data, the audit process of the database logs all the actions. The authentication process of the online transaction system finally verifies the provided authentication data of the customer against the authentication data of the database. In case the data matches the authorization process is started, in case the data does not match an authentication error message is sent to the customer.

The authorization process of the online transaction system on the other hand determines the access rights of the customers. First of all, the online transaction system sends an authorization data request to the database. The database subsequently provides the authorization data to the online transaction system. While the database receives the request for authorization data and sends the requested authorization data, the audit process of the database logs all the actions. Once the access rights of the customer are received by the online transaction system they are stored by the online transaction system throughout the entire session. Finally, a confirmation is send to the customer that the authentication is succeeded. The customer can subsequently proceed with the online transaction application (within the boundaries of the access rights).

As all steps of the web application are illustrated in Figure 23, all the threats of the information system can be gradually identified. For identification, for instance, the information system is up against the following threats:

Authentication bypass	A malicious entity can bypass the information system by impersonating another entity.
Information system masquerade	A hostile entity can masquerade itself and act as the information system.
Communication	Compromising the confidentiality or integrity of communication-data.

Step 4 – This step did not show any significant difficulties as well. The security requirements are simply a further elaboration of the security needs and protection against the threats. Subsequently, all the defined security requirements were associated with the security needs of step 1 or the threats of step 3. Thus all the security requirements contribute to the security of the organization and no unnecessary security requirements were defined at this stage. The following security requirements were, for example, defined for the online transaction system:

User identification The information system should uniquely identify each user.

User authentication The information system should verify the given identity of the users.

Trusted path The information system should guarantee the users that they are indeed communicating with the information system and vice versa.

Access The information system should only allow authorized users to access the information system and the resources of the information system.

Encryption services The information system should have the ability to offer encryption services to authorized processes or users.

Communication The confidentiality and the integrity of communication-data should be protected.

Table 9 illustrates the dependencies between the security needs/threats and the security requirements.

Security needs	**Security requirements**
Identification and authentication	User identification User authentication Trusted path
Threats	**Security requirements**
Authentication bypass	User identification User authentication Access
Information system masquerade	Trusted path Communication
Communication	Encrypted services Communication

Table 9: Dependencies between security needs/threats and security requirements

Once the security requirements of the organization were defined, the requirements classification step can be easily performed. The classification of the security services was performed based upon the security requirements defined in the context assessment step, the CTCPEC, and the FC. These two criteria were quite suitable for the requirements classification step, since some functional requirements are similar to the functional requirements of the CC. Besides that, the functional requirements of the CTCPEC and the FC are already classified in levels. While setting up the requirements classification, all the unnecessary functional requirements were removed from the list.

Table 10 illustrates the example for the identification and authentication class. As the table shows, the user authentication 3, 4, 5, and 6 are omitted. These are not applicable in the situation of the organization. There are, however, two components added, namely user authentication *1 and *2. These are actually replacements for the user authentication 3, 4, 5, and 6. After all, the user authentication 3, 4, 5, and 6 are a form of (or rather an attempt to) strong authentication. The user authentication *1 and *2, however, provide a more global description. Through this, the strong authentication requirements become less restrictive.
(L = Low → weak authentication, M = Medium → average authentication, and H = High → strong authentication)

Identification and Authentication	Authentication
Authentication failures	
1. Authentication failures	M
User attribute definition	
1. User attribute definition	M
Specification of secrets	
1. Verification of secrets	M
2. Generation of secrets	H
User authentication	
1. Timing of authentication	L
2. User authentication before any action	M
7. Protected authentication feedback	M
*1. Strong administrator authentication	M
*2. Strong user authentication	H
User identification	
1. Timing of identification	L
2. User identification before any action	M
User-subject binding	
1. User-subject binding	M

Table 10: Requirements classification

The next step of the ECM was to create the sub-protection profiles. In this step, sub-protection profiles should be created for each component of the information system. Since there are two information systems, at least two sub-protection profiles have to be created. The test case, however, did not make a sub-protection profile for each component. This step was eliminated, since it would probably be too confusing for the organization to classify the security services for the operating system and the applications. Therefore only two sub-protection profiles were created, one for the web application and one for the back office. The classification of the security services was defined by the author and the organization. This point is essential to provide the organization the opportunity to have input in the evaluation. The security service for identification and authentication was set as high for the web application and low for

the back office[33]. Table 11 is the result of the functional requirements of the protection profile.

	Web application	Back Office
Identification and Authentication	**Authentication**	**Authentication**
Authentication failures		
1. Authentication failures	√	
User attribute definition		
1. User attribute definition	√	
Specification of secrets		
1. Verification of secrets	√	
2. Generation of secrets	√	
User authentication		
1. Timing of authentication	√	√
2. User authentication before any action	√	
7. Protected authentication feedback	√	
*1. Strong administrator authentication	√	
*2. Strong user authentication	√	
User identification		
1. Timing of identification	√	√
2. User identification before any action	√	
User-subject binding		
1. User-subject binding	√	

Table 11: Protection profiles' functional requirements

As the ECM defined a format for the protection profile, the test case did not utilize the protection profile format. After all, the organization is probably not interested in such a technical document. The protection profile and the security target were rather combined into a final document. This will provide a better overview for the organization. Moreover, the organization is probably not interested in all the steps of the ECM evaluation, therefore only the results of the ECM evaluation are opted in the final document. Besides, all the steps of the protection profile are available for internal use. In case a protection profile is desired, it can be easily derived by combining the protection profile steps and the final document.

[33] Notice that the classification of the security services is fictional and do not reflect the actual situation of the organization.

5.4 Analysis stage

Even though the analysis stage can be performed parallel to the identification stage, the analysis stage was performed subsequently to the identification stage. This is due to the fact that the evaluation was conducted by a single person. In case two or more persons ware involved in the evaluation, they can easily work in parallel and perform the identification stage and the analysis stage simultaneously. This, however, was not the case.

At the analysis stage of the ECM the functionalities should be identified per component. Therefore the components of the two information systems had to be defined first. The web application was divided in two components, namely the operating system and the application system. The application system contains of the IBM Websphere Application Server and the application build by the third party. This was done, since the IBM Websphere Application Server and the application build by the third party cooperates very closely. To make a distinction between those two components would be superfluous. The back office has the same subdivision. One component for the operating system and one component for the IBM Websphere Application Server combined with the application build by the third party.

For the analysis stage several sources had been consulted, from the CC to the manufacturer documents. These documents alone, however, were not enough to define all the functionalities of the products. The products were also installed and analysed for the functionalities. By taking these steps all the functionalities of the products were identified.

Among the components, Microsoft Windows already had been evaluated by the CC. The CC evaluation of Microsoft Windows was therefore used as a baseline and made the analysis for that component a lot easier to perform. For the other remaining components there was not a CC evaluation available and had to be analysed from top to bottom. While performing the analysis of the components, the list of the functional requirements for the protection profiles (Table 11) of the identification stage had been analysed for missing and unnecessary functionalities.

Table 12 illustrates the results of the available functionalities of the components for the identification and authentication class.

	Web application		Back office	
Identification and Authentication	**Linux**	**Application**	**Windows**	**Application**
Authentication failures				
1. Authentication failures		√		√
User attribute definition				
1. User attribute definition	√	√	√	√
Specification of secrets				
1. Verification of secrets	√	√	√	√
2. Generation of secrets				
User authentication				
1. Timing of authentication	√	√	√	√
2. User authentication before any action	√		√	√
7. Protected authentication feedback	√	√	√	√
*1. Strong administrator authentication				
*2. Strong user authentication		√		
User identification				
1. Timing of identification	√	√	√	√
2. User identification before any action	√		√	√
User-subject binding				
1. User-subject binding	√	√	√	√

Table 12: Information system functionalities

The analysis stage went as planned and no significant irregularities occurred. But as the identification stage of this chapter already stressed, there had not been a security target developed according to the format of the ECM, since the protection profile and the security target were combined into a final document. Even though, there was not a security target developed, the analysis stage steps are available for internal use. Therefore the security target can be easily derived by combining the analysis stage steps and the final document.

5.5 Evaluation stage

As the previous sections illustrated, the identification stage and the analysis stage were conducted according to the ECM. The functional requirement evaluation should be quite straightforward. After all, at the identification stage the needed functionalities of the context were defined and at the analysis stage the provided functionalities of the information systems were defined. By verifying whether the needed functionalities were covered by the available functionalities per component, the evaluation can be conducted. This was quite straightforward; it came down to comparing two tables, to verify which functionalities were missing.

Table 13 is a combined table of the protection profiles' functional requirements (Table 11) and the information system functionalities (Table 12). The √ stands for the available functionalities, while the **X** stands for the missing functionalities. As Table 13 shows, the web application misses eight functionalities. The back office on the other hand does not miss any functionality.

	Web application			**Back office**		
Identification and Authentication	**Req.**	**Win.**	**App.**	**Req.**	**Lin.**	**App.**
Authentication failures						
1. Authentication failures	√	**X**	√			√
User attribute definition						
1. User attribute definition	√	√	√		√	√
Specification of secrets						
1. Verification of secrets	√	√	√		√	√
2. Generation of secrets	√	**X**	**X**			
User authentication						
1. Timing of authentication	√	√	√	√	√	√
2. User authentication before any action	√	√	**X**		√	√
7. Protected authentication feedback	√	√	√		√	√
*1. Strong administrator authentication	√	**X**	**X**			
*2. Strong user authentication	√	**X**	√			
User identification						
1. Timing of identification	√	√	√	√	√	√
2. User identification before any action	√	√	**X**		√	√
User-subject binding						
1. User-subject binding	√	√	√		√	√

Table 13: Evaluation table

Table 14 illustrates the lacking functionalities with possible recommendations. There is actually one point worth noticing. The web application namely misses the functionalities user authentication.2 and user identification.2. These two functionalities, however, cannot be considered as lacking. After all, the online transaction system consists of a public information section and an online transaction system section. The public information should be accessible to everyone and therefore authentication should not be necessary for the entire web application.

Identification and Authentication	Web application			Recommendations
	Req.	Win.	App.	
Authentication failures				
1. Authentication failures	√	**X**	√	Verify whether the authentication failure functionality is enabled (e.g. account blocking).
Specification of secrets				
2. Generation of secrets	√	**X**	**X**	Implement a password generator software.
User authentication				
2. User authentication before any action	√	√	**X**	This point cannot be seen as a deficiency.
*1. Strong administrator authentication	√	**X**	**X**	Implement strong forms Of authentication (e.g. smartcards, tokens or Biometric authentication).
*2. Strong user authentication	√	**X**	√	Implement strong forms Of authentication (e.g. smartcards, tokens or Biometric authentication).
User identification				
2. User identification before any action	√	√	**X**	This point cannot be seen as a deficiency.

Table 14: Recommendations

The assurance part on the other hand was a bit harder to perform. After all, there were not any steps of the assurance evaluation performed yet. Thus the entire evaluation had to take place at the evaluation stage. As was indicated at the analysis stage of this section, Microsoft Windows had already been evaluated by the CC and therefore already has an EAL (EAL4 augmented). For the other three components the EAL had yet to be determined.

Even though the CC developed a methodology (CEM) to evaluate products on assurance requirements, this was not as easy as it seems. This is due to the fact that the remaining three components were not been designed for the CC evaluation. Thus the components miss some documentation (or parts of documentation) and some procedures that are required by the CC. Furthermore the application build by the third party had not been documented at all. Due to the lack of documentation the two application system components could not be evaluated for the assurance part. In order to provide some form of assurance, the IBM Websphere Application Server alone (without the application build by the third party) had been evaluated for the assurance part.

In order to cope with these problems three EALs were attributed to the components that had not been evaluated yet.

1) The probable EAL that a component would receive in the current state strict according to the CC.
2) The probable EAL that a component would receive in the current state in case the rules of the CC are held loosely.
3) The probable EAL that a component would receive in case the component would be tailored for the CC.

The results of the test case were as follows:

1) In case the rules of the CC are strictly applied, none of the three components would receive an EAL. They all miss several necessary documents and procedures.
2) In case the rules of the CC were held loosely the Redhat Linux could receive an EAL2. This can be achieved by including the general documentation of Linux. Even though the documentation is not explicitly intended for Redhat Linux, they do cover most aspects of Redhat Linux. However, notice that some parts of the documents may differ. The IBM Websphere Application Server on the other hand, can still not satisfy the CC Assurance requirements.
3) In case all three components would be tailored to the CC, the Redhat Linux could expect to receive an EAL4 augmented, while the IBM Websphere Application Server could expect to receive an EAL3 to EAL4. Notice that these are estimates and cannot be considered as certainties.

Table 15 summarizes the assurance results in a tabular form.

	Web application		Back office	
	Windows	Application	Linux	Application
Strict CC	EAL4 augmented	-	-	-
Loosely held	EAL4 augmented	-	EAL2	-
Tailored to CC	EAL4 augmented	EAL3 – EAL4	EAL4 augmented	EAL3 – EAL4

Table 15: Assurance overview

Even though the components had not gone through a CC evaluation, some advice can be given to the assurance part. Next to the CC assurance part, the ECM also contained a pragmatic assurance part. This part, however, had not been conducted in the test case. This was due to the fact that for some parts of the pragmatic assurance evaluation the components had to be physically analysed. But as the beginning of this chapter already stressed, this method had not been chosen. Even though the pragmatic evaluation had not been conducted, a checklist was provided to the organization. By doing this, the organization or a third party can verify whether the information system is compliant to the checklist or not. The checklist is based on a best practice defined by the OWASP (Open Web Application Security Project) [Owas, 2003]. The OWASP is chosen as the best practice, since it is not product related. Therefore it can be

applied to all kinds of web application and besides it can be applied to future projects as well.

5.6 Conclusion

This section evaluates the test case by revisiting the goals set in the beginning of this chapter.

1) Verify whether the ECM is complete.
First of all, the functional requirements and the assurance requirements can be practically considered as complete. The requirements covered all the requirements of the test case. Furthermore, the requirements of the CC covered all the requirements of the CC evaluated products. The requirements, however, are prone to improvements. As the test case illustrated some functional requirements of the authentication class were modified to suit the test case. If we are realistic no set of requirements can cover all the requirements for all information systems. After all, information systems can differ very much and the technology shifts very fast. The CC and the ECM overcame this problem by having the additional requirements. Thus the requirements of the ECM can be extended by other necessary requirements.

The following table recapitulates the deviations that occurred during the test case.

Preparation stage
Elimination of the unnecessary functional requirements was postponed to later stages.
The assurance evaluation was postponed to the evaluation stage.
Identification stage
ECM did not explicitly define a methodology for the context needs step.
The test case did not explicitly utilize the sub-protection profiles.
The protection profile is not documented.
Analysis stage
The security target is not documented
Evaluation stage
The EAL grading is slightly modified/extended.
The pragmatic assurance was not conducted.

Table 16: Deviations of the test case

2) Verify whether the ECM is applicable in practice.
As the test case showed, the ECM is certainly applicable in practice. The ECM, however, should be improved at certain points. The following points should be improved in order to apply the ECM is practice:

- Develop a well-founded methodology for the context needs step (this is partly done in the identification step of the test case)

- Develop a well-founded metric or methodology for the assurance requirements (this is partly done in the evaluation step of the test case)
- Develop a pragmatic assurance that can be implemented without physical analysis (or perhaps include physical analysis to the evaluation).

3) Verify whether the ECM is suitable as a service to customers.

First of all the test case was conducted as a service to the organization. The final documentation for the organization was coupled to a presentation. During the presentation the overall impression of the organization was quite positive. The organization was "surprised" by the fact that there were quite a few recommendations on such a small section of their information system. Furthermore, the customer was interested in the provided recommendations. Whether the customer is actually going to implement the recommendations is at the time of writing unknown. Another point worth noticing is that the ECM is an ideal stepping-stone to "walk in" to an organization. Besides the recommendations of the ECM, the ECM also highlighted other insufficiencies (mainly organizational) and possible relevant projects. This led to many discussions and interest of the customer.

Another point is that concrete recommendations can be given the lacking requirements (Table 14). Even though, this point is not described in the ECM, it is certainly important for the ECM evaluation as a service to customers. After all, customers do not want to hear that their information system is "insecure". They rather want to hear that their information system is "secure" or possible solutions to make their information system "secure".

4) Verify whether all components need to be as "secure" as the overall information system.

The purpose of this goal is to determine whether a verdict can be given to an entire information system by focussing on the separate components. Thus in case an information system requires an EAL3, does this imply that all the components at least need an EAL3? The rationale also works the other way around. Thus in case all components have an EAL3, does it imply that the entire information system has an EAL3?

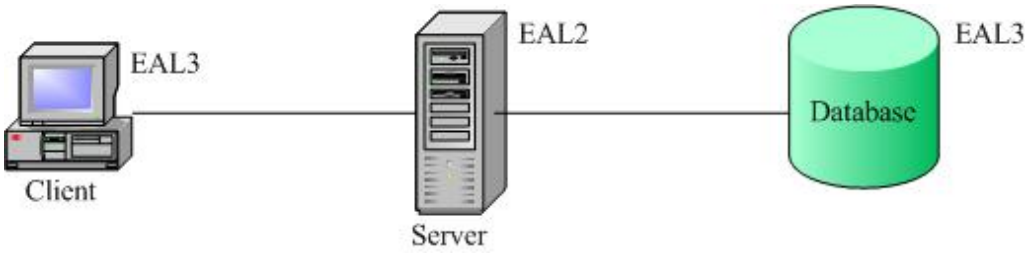


Figure 24: Aggregation of components

Figure 24, is a more concrete example of this goal. As the figure illustrates the information system consist of three components the client, the server, and the database. In case two of the components possess an EAL3 and one of the component possess an EAL2. Does this imply that the EAL of the overall information system is an EAL2 or an EAL3? This is the point that this goal is researching on.

As Table 13 of page 70 illustrates, not all the components need to be as strong as the overall information system. After all, identification and authentication is not necessary for the public information.

Another functional requirement of the CC is stored data integrity monitoring (FDP_SDI.1). This functional requirement can detect modifications of the file system. This functional requirement was mandatory for the online transaction system of the test case. The stored data integrity monitoring, however, was only mandatory for the operating system and not for the application system (application server and application by third party). After all, in case a modification occurred to the file system, the operating system should detect it, while it is the operating system that manages the file system. By adding the data integrity monitoring to the application server would be superfluous. Thus even though the application system does not provide the data integrity monitoring functionality, the overall information system (application system and operating system) does.

The two examples above illustrates that not all components need to be as “secure” to achieve a “secure” overall information system. After all, some components closely cooperate and can overcome each others’ weaknesses. The main issue is that a “less secure” component does not necessarily lower the overall security level of the information system, as long as the risks are still covered by the information system.

Final conclusions of the test case

The final conclusion is that the goals of the test case are partly met. After all, ECM is applicable in practice in the current state. The ECM, however, is still prone to improvements. This thesis is actually only the first step of the ECM. To provide the ECM as a service, further research has to be done to improve the ECM.

Another point that may arise is the necessary foreknowledge of an ECM evaluation. The test case showed that an ECM evaluation can be performed with basic managerial knowledge and with basic technical knowledge. Even though the ECM evaluation is quite technical oriented, the managerial knowledge is necessary for the identification stage. At this stage the security requirements of the information system have to be defined. To conduct the steps to achieve the security requirements of the information system cannot be performed by merely technical knowledge. Technical knowledge on the other hand is necessary for the identification stage and for the analysis stage. After all, technical knowledge is necessary to identify the available functionalities. Foreknowledge of the involved components is not necessary, but it can drastically fasten the evaluation.

6. Conclusion and possible further research

The main goal of this thesis is to create a methodology to evaluate the security of information systems. This chapter concludes the thesis by revisiting the goals, to verify whether the goals are accomplished. Furthermore a final conclusion is provided to state the most important results/observations of this thesis. Finally some possible directions are given for further research.

6.1 Goals revisited

The goals as stated in chapter 1, was to develop an evaluation methodology that addresses the following two requirements:

- Classifications based on information systems rather than products.
- Create a methodology, which is suitable for the "customer" rather than the manufacturer/vendor.

The first goal is addressed by chapter 4 and chapter 5. First of all chapter 4 described a methodology (ECM) that is specifically designed to evaluate information systems. Second of all, the test case of chapter 5 actually evaluated an information system (or better yet actually two information systems).

The second goal is also addressed by chapter 4 and 5. After all, the ECM is designed to be conducted by the end-user. This allows the end-users to evaluate their information systems themselves or let a third party evaluate their information system for a reasonable price. By doing this large overhead (costs, time, and effort) are saved and therefore the ECM is suitable for "customers". Furthermore chapter 5 illustrated that the methodology can indeed be conducted by an end-user or a third party instead of a manufacture. After all, the evaluation is performed by the author.

The goals defined in chapter 1 were not the only goals set for this thesis. As chapter 3 and chapter 4 went in further details of the current evaluation methodologies, more improvement points came to the surface. In chapter 4 two additional goals came to the surface, namely:

- Eliminate the accredited organization and the mandatory evaluated protection profiles.
- Take the functional and assurance requirements (extended) into account for the evaluation.

The first goal of chapter 4 can be split in two sections, namely *"eliminate the accredited organization"* and *"eliminate the mandatory evaluated protection profiles"*. The first part of the first goal of chapter 4 is addressed by chapter 5, as the evaluation is conducted by the author rather than an accredited organization. The second part of the first goal of chapter 4 is addressed by chapter 4 self. In chapter 4 a

methodology is described that explicitly stated that the mandatory evaluated protection profiles were superfluous. Furthermore chapter 5 emphasized this point, by conducting the methodology without the mandatory evaluated protection profiles.

The second goal of chapter 4 is addressed by chapter 4 and chapter 5. First of all chapter 4 described a methodology (ECM), which was designed to take the functional requirements and the assurance requirements into account. Second of all, chapter 5 showed that both of the requirements were indeed taken into account. After all, the evaluation had results for both of the requirements.

6.2 Conclusion

This thesis describes a methodology to evaluate the security of information systems. Even though, this might not seem to be very different from the CC at first sight, the ranges of applications have increased significantly. It is now not only limited to evaluate products, but the ECM is also suitable to evaluate an entire information system. Besides, the ECM is developed for an entire different target group. As the CC is only reserved for the accredited organizations, the ECM is accessible for all users with some technical knowledge and some managerial knowledge. Moreover the ECM can be utilized in three different ways, namely:

- The ECM can be used as described in chapter 5, to verify whether an information system/product is secure enough for a particular context. For instance, is Windows 2000 secure enough for a particular context?
- The ECM can be used to verify which information systems/products are suitable for a certain context. For instance, should firewall of brand X or should firewall of brand Y be used for a particular context?
- The ECM can be used to verify which context is suitable for a certain information system/product. For instance, a web server, should it be managed by the information system owner self or should it be outsourced to a hosting company or to an ASP (Application Service Provider)

An important point worth noticing is that the ECM is not a solution, which can solve all the information security problems. First of all, there is not a thing as absolute security. Therefore, there will probably never be a complete solution to the information security problem. Furthermore, the ECM is not a one-stop strategy. An ECM evaluation is merely a snapshot of the information system security. The ECM evaluation should be performed regularly and form an integrated part of information management life cycle. Each modification to the information system can influence the information security and should therefore be evaluated. Finally, information security consists of technical aspect and managerial aspect. Thus the ECM is only one part of the story. In order to get a complete view, it is necessary to address the managerial aspects of information security as well.

Even though there is not such a thing as absolute security, the ECM can help organizations to achieve a higher level of security. The ECM namely forms a systematic approach to address information security. By having a systemic approach, all the security evaluations can be done in a uniform manner. A uniform manner can subsequently lead to an acceleration of the process. After all, in case all evaluations are done in a uniform process, the evaluators will most likely get handiness in the evaluation process and this will certainly accelerate the evaluation process. Besides, a uniform security evaluation is much easier for the management to compare different information systems/products. This subsequently can lead to better decision-makings of the management.

Even though the test case meets all the initial goals[34], the ECM is still prone to improvements as the test case showed. The test case also showed that the ECM is indeed quite suitable for practical use. After all, the ECM evaluation was actually implemented in practice and the organization of the test case was quite satisfied with the results of the ECM evaluation. The ECM, however, cannot be considered as a finished product. In order for the ECM to function as a service to customers at least the following improvements should be made to the ECM:

- Develop a well-founded methodology for the context needs step.
- Develop a well-founded metric or methodology for the assurance requirements.
- Develop a pragmatic assurance that can be implemented without physical analysis.

The requirements utilized by the ECM, on the other hand, can be considered as complete. After all, the requirements covered all the needed requirements of the test case. Besides, The CC showed that the requirements are adequate to cover the needed requirements by the CC evaluated products. This, however, does not imply that the requirements of the CC can fully satisfy the needs of the ECM. As the test case illustrated, the requirements of the ECM are prone to improvements and can/should be tailored to information systems.

Another point that the test case showed is that the foreknowledge required for an ECM evaluation is limited to basic managerial knowledge and basic technical knowledge. The basic managerial knowledge is required the identification stage, while the technical knowledge is required for the identification stage and the analysis stage. Notice that foreknowledge of the components may fasten the analysis stage, but is not considered as obligatory. Thus the required foreknowledge is not very extensive and therefore the ECM evaluation can be performed by many end-users.

Finally, notice that this thesis is merely the first step (of many) to develop a technical oriented evaluation for the security of information system. This thesis can be

[34] Notice that this is only one experiment, whether the ECM actually can meet all the goals requires further research.

contemplated as a stepping-stone and a starting point for other research projects on the field of technical oriented evaluations for the security of information system

The next section provides some possible directions for further research to enhance the ECM.

6.3 Possible further research

Even though the ECM is developed and even applied in a test case, the ECM is still prone to improvements. The following points are interesting for further research:

Create a methodology for assessing the context needs step
As chapter 5 already illustrated, the ECM currently lacks a methodology to assess the context needs step. This part should be considered as an important step and therefore a methodology should be explicitly defined for this step. The methodology can be based on the methodology that is described in chapter 5 or perhaps even a better and easier methodology can be developed.

Combine the ECM with a managerial evaluation
As the thesis explicitly stated, the ECM is a technical oriented evaluation. It would be very useful to combine the technical aspects and the managerial aspects in one evaluation. Combining the ECM and the British Standard, for instance, can be a viable option. By doing this, a complete evaluation is created, which may be easily adopted by the wide audience. After all, the British Standard is already widespread used by many organizations.

Create a handbook for the ECM evaluation.
By having a handbook, the evaluator can perform the evaluation by following the step-by-step instructions provided by the handbook. At the time of writing a handbook is in development. The handbook, however, is intended for the internal use of Ubizen and will therefore not be publicly publicised.

Create templates of security targets to accelerate the process
By having templates for security targets the evaluation procedure can be significant accelerated. During the test case of the ECM, the analysis stage took a considerable amount of time. By having templates of the security targets, the duration of the ECM evaluation can be easily reduced by quart to half of the time.

Appendix

The following section defines the functional requirements, which are defined in the Common Criteria and are used by the ECM. The appendix only mentions which classes, families, and components are present in the Common Criteria. For further explanation of the classes, families, and components the Common Criteria part II [Com2, 1999] can be consulted.

Interpretation:

The first column stands for the abbreviated name and the second column is the full name.

The dark grey cells stand for the classes

Class

The light grey cells stand for the families

Family

The white cells stand for the components

Component

FAU	Security Audit
FAU_ARP	**Security audit automatic response**
1.	Security alarms
FAU_GEN	**Security audit data generation**
1.	Data generation (level of audit)
2.	User identity association
FAU_SAA	**Security audit analysis**
1.	Potential violation analysis
2.	Profile based anomaly detection
3.	Simple attack heuristic
4.	Complex attack heuristic
FAU_SAR	**Security audit review**
1.	Audit review
2.	Restricted audit review
3.	Selectable audit review
FAU_SEL	**Security audit event selection**
1.	Selective audit

FAU_STG	Security audit event storage
1.	Protected audit trail storage
2.	Guarantees of audit data availability
3.	Actions in case of audit trail loss
4.	Prevention of audit trail loss (full)

FCO	Communication
FCO_NRO	**Non-repudiation of origin**
1.	Selective proof of origin
2.	Enforced proof of origin
FCO_NRR	**Non-repudiation of receipt**
1.	Selective proof of receipt
2.	Enforced proof of receipt

FCS	Cryptographic Support
FCS_CKM	**Cryptographic key management**
1.	Cryptographic key generation
2.	Cryptographic key distribution
3.	Cryptographic key access
4.	Cryptographic key destruction
FCS_COP	**Cryptographic key operation**
1.	Cryptographic operation

FDP	User Data Protection
FDP_ACC	**Access control policy**
1.	Subset access control
2.	Complete access control
FDP_ACF	**Access control function**
1.	Security attribute
FDP_DAU	**Data authentication**
1.	Basic data authentication
2.	Data authentication with the ID of guarantor
FDP_ETC	**Export to outside TSF control**
1.	Export of user data without security attributes
2.	Export of user data with security attributes
FDP_IFC	**Information flow control policy**
1.	Subset information flow control
2.	Complete information flow control
FDP_IFF	**Information flow control functions**
1.	Simple security attributes
2.	Hierarchical security attributes
3.	Limited illicit information flows
4.	Partial eliminated illicit information flows

5.	No illicit information flows
6.	Illicit information flow monitoring
FDP_ITC	**Import from outside TSF control**
1.	Import of user data without security attributes
2.	Import of user data with security attributes
FDP_ITT	**Internal TOE transfer**
1.	Basic internal transfer protection
2.	Transmission separation by attribute
3.	Integrity monitoring
4.	Attribute-based integrity monitoring
FDP_RIP	**Residual information protection**
1.	Subset residual information protection
2.	Full residual information protection
FDP_ROL	**Rollback**
1.	Basic rollback
2.	Advanced rollback
FDP_SDI	**Stored data integrity**
1.	Stored data integrity monitoring
2.	Stored data integrity monitoring and action
FDP_UCT	**Inter-TSF user data confidentiality transfer protection**
1.	Basic data exchange confidentiality
FDP_UIT	**Inter-TSF user data integrity transfer protection**
1.	Data exchange integrity
2.	Source data exchange recovery
3.	Destination exchange recovery

FIA	Identification and Authentication
FIA_AFL	**Authentication failures**
1.	Authentication failures
FIA_ATD	**User attribute definition**
1.	User attribute definition
FIA_SOS	**Specification of secrets**
1.	Verification of secrets
2.	Generation of secrets
FIA_UAU	**User authentication**
1.	Timing of authentication
2.	User authentication before any action
3.	Unforgable identification
4.	Single-use authentication mechanisms
5.	Multiple authentication mechanisms
6.	Re-authenticate
7.	Protected authentication feedback
FIA_UID	**User identification**

1.	Timing of identification
2.	User identification before any action
FIA_USB	**User-subject binding**
1.	User-subject binding

FMT	Security management
FMT_MOF	**Management of functions in TSF**
1.	Management of security functions behaviour
FMT_MSA	**Management of security attributes**
1.	Management of security attributes
2.	Secure security attributes
3.	Static attribute initialisation
FMT_MTD	**Management of TSF data**
1.	Management of TSF data
2.	Management of limits of TSF data
3.	Secure TSF data
FMT_REV	**Revocation**
1.	Revocation
FMT_SAE	**Security attribute expiration**
1.	Time-limited authorisation
FMT_SMR	**Security management roles**
1.	Security roles
2.	Restrictions on security roles
3.	Assuming roles

FPR	Privacy
FPR_ANO	**Anonymity**
1.	Anonymity
2.	Anonymity without solicitating information
FPR_PSE	**Pseudonimity**
1.	Pseudonimity
2.	Reversible pseudonimity
3.	Alias pseudonimity
FPR_UNL	**Unlinkability**
1.	Unlinkability
FPR_UNO	**Unobservability**
1.	Unobservability
2.	Allocation of information impacting unobservability
3.	Unobservability without solicitating information
4.	Authorised user observability

FPT	Protection of the TSF
FPT_AMT	**Underlying abstract machine test**

1.	Abstract machine testing
FPR_FLS	**Fail secure**
1.	Failure with preservation of secure state
FPR_ITA	**Availability of exported TSF data**
1.	Inter-TSF availability within a defined metric
FPR_ITC	**Confidentiality of exported TSF data**
1.	Confidentiality during transmission
FPR_ITI	**Integrity of exported TSF data**
1.	Inter-TSF detection of modification
2.	Inter-TSF detection and correction of modification
FPR_ITT	**Internal TOE TSF data transfer**
1.	Basic internal TSF data transfer protection
2.	TSF data transfer separation
3.	TSF data integrity monitoring
FPR_PHP	**TSF physical protection**
1.	Passive detection of physical attack
2.	Notification of physical attack
3.	Resistance to physical attack
FPR_RCV	**Trusted recovery**
1.	Manual recovery
2.	Automated recovery
3.	Automated recovery without undue loss
4.	Function recovery
FPR_RPL	**Replay detection**
1.	Replay detection
FPR_RVM	**Reference mediation**
1.	Non-bypassability of the TSP
FPR_SEP	**Domain separation**
1.	Domain separation
2.	SFP domain separation
3.	Complete reference monitor
FPR_SSP	**State synchrony protocol**
1.	Simple trusted acknowledgement
2.	Mutual trusted acknowledgement
FPR_STM	**Time stamps**
1.	Reliable time stamps
FPR_TDC	**Inter-TSF TSF data consistency**
1.	Inter-TSF TSF data consistency
FPR_TRC	**Internal TOE TSF data replication consistency**
1.	Internal TSF consistency
FPR_TST	**TSF self test**
1.	TSF testing

FRU	Resource Utilisation
FRU_FLT	**Fault tolerance**
1.	Degraded fault tolerance
2.	Limited fault tolerance
FRU_PRS	**Priority of service**
1.	Limited priority of service
2.	Full priority of service
FRU_RSA	**Resource allocation**
1.	Maximum quotas
2.	Minimum and maximum quotas

FTA	Toe Access
FTA_LSA	**Limitation on scope of selectable attributes**
1.	Selectation of scope of selectable attributes
FTA_MCS	**Limitation on multiple concurrent sessions**
1.	Basic limitation on multiple concurrent sessions
2.	Per user attribute on multiple concurrent sessions
FTA_SSL	**Session locking**
1.	TSF-initiated session locking
2.	User-initiated session locking
3.	TSF-initiated termination
FTA_TAB	**TOE access banners**
1.	Default TOE access banner
FTA_TAH	**TOE access history**
1.	TOE access history
FTA_TSE	**TOE session establishment**
1.	TOE session establishment

FTP	Trusted Path/Channels
FTP_ITC	**Inter-TSF trusted channel**
1.	Inter-TSF trusted channel
FTP_TRP	**Trusted path**
1.	Trusted path

The following section defines the assurance requirements, which are defined in the Common Criteria and are used by the ECM. The appendix only mentions which classes, families, and components are present in the Common Criteria. For further explanation of the classes, families, and components the Common Criteria part III [Com3, 1999] can be consulted.

Interpretation:

The first column stands for the abbreviated name and the second column is the full name.

The dark grey cells stand for the classes

Class

The light grey cells stand for the families

Family

The white cells stand for the components

Component

ACM	Configuration Management
ACM_AUT	**CM automation**
1.	Partial CM automation
2.	Complete CM automation
ACM_CAP	**CM capabilities**
1.	Version numbers
2.	Configuration items
3.	Authorisation controls
4.	Generation support and acceptance procedures
5.	Advanced support
ACM-SCP	**CM scope**
1.	TOE CM coverage
2.	Problem tracking CM coverage
3.	Development tools CM coverage

ADO	Delivery and Operation
ADO_DEL	**Delivery**
1.	Delivery procedures
2.	Detection of modification
3.	Prevention of modification
ADO_IGS	**Installation, generation and start up**

1.	Installation, generation and start up procedures
2.	Generation log

ADV	Development
ADV_FSP	**Functional specification**
1.	Informal functional specification
2.	Fully defined external interfaces
3.	Semiformal functional specification
4.	Formal functional specification
ADV_HLD	**High-level design**
1.	Descriptive high-level design
2.	Security enforcing high-level design
3.	Semiformal high-level design
4.	Semiformal high-level explanation
5.	Formal high-level explanation
ADV_IMP	**Implementation representation**
1.	Subset of the implementation of the TSF
2.	Implementation of the TSF
3.	Structured implementation of the TSF
ADV_INT	**TSF internals**
1.	Modularity
2.	Reduction of complexity
3.	Minimisation of complexity
ADV_LLD	**Low-level design**
1.	Descriptive low-level design
2.	Semiformal low-level design
3.	Formal low-level design
ADV_RCR	**Representation correspondence**
1.	Informal correspondence representation
2.	Semiformal correspondence representation
3.	Formal correspondence representation
ADV_SPM	**Security policy modeling**
1.	Informal TOE security policy model
2.	Semiformal TOE security policy model
3.	Formal TOE security policy model

AGD	Guidance Documents
AGD_ADM	**Administrator guidance**
1.	Administrator guidance
AGD_USR	**User guidance**
1.	User guidance

ALC	Life-cycle support

ALC_DVS	Development security
1.	Development security
2.	Sufficiency of security measures
ALC_FLR	**Flaw remediation**
1.	Basic flaw remediation
2.	Flaw reporting procedures
3.	Systematic flaw remediation
ALC_LCD	**Life cycle definition**
1.	Developer designed life-cycle model
2.	Standardized life-cycle model
3.	Measurable life-cycle model
ALC_TAT	**Tools and techniques**
1.	Well-defined development tools
2.	Compliance with implementation standards
3.	Compliance with implementation standards - all parts

ATE	Tests
ATE_COV	**Coverage**
1.	Evidence of coverage
2.	Analysis of coverage
3.	Rigorous analysis of coverage
ATE_DPT	**Depth**
1.	Testing: high-level design
2.	Testing: low-level design
3.	Testing: implementation representation
ATE_FUN	**Functional tests**
1.	Functional testing
2.	Ordered functional testing
ATE_IND	**Independent testing**
1.	Independent testing - conformance
2.	Independent testing - sample
3.	Independent testing - complete

AVA	Vulnerability Assessment
AVA_CCA	**Covert channel analysis**
1.	Covert channel analysis
2.	Systematic covert channel analysis
3.	Exhaustive covert channel analysis
AVA_MSU	**Misuse**
1.	Examination of guidance
2.	Validation of analysis
3.	Analysis and testing for insecure states
AVA_SOF	**Strength of TOE security functions**

1.	Strength of TOE security functions
AVA_VLA	**Vulnerability analysis**
1.	Developer vulnerability analysis
2.	Independent developer vulnerability analysis
3.	Moderately resistant
4.	Highly resistant

AMA	Maintenance of Assurance
AMA_AMP	**Assurance maintenance plans**
1.	Assurance maintenance plans
AMA_CAT	**TOE component categorisation report**
1.	TOE component categorisation report
AMA_EVD	**Evidence of assurance maintenance**
2.	Evidence of assurance maintenance
AMA_SIA	**Security impact analysis**
1.	Sampling of security impact analysis
2.	Examination of security impact analysis

References

[ABC, 2003] ABCNews.com, article: Web Under Attack - Five Leading Web Sites Suffer Outages After Coordinated Attacks This Week, Website: http://abcnews.go.com, 2003.

[ANS, 2001] American National Standard for telecommunications – Telecom Glossary 2000, Alliance for Telecommunications Industry Solutions, 2001.

[Bell, 1974] D. Bell, L. LaPadula, "Secure Computer Systems" ESD-TR-73-278 (Vol. I-III) Mitre Corporation, Bedford, 1974

[Biba, 1977] Integrity Considerations for Secure Computer Systems, K. J. Biba, Mitre Computer Systems, 1977.

[Brow, 1998] Encyclopedia of the New Economy, John Browning, Spencer Reiss, Wired magazine, 1998.

[BS1, 1999] Information Security Management – part 1: Code of Practice for Information Security Management, British Standard Institute (BSI), 1999

[BS2, 1999] Information Security Management – part 2: Specification for Information Security Management Systems, British Standard Institute (BSI), 1999

[Burd, 2001] Security Essentials for the home network, Mike Burden, Sans Institute, as part of GIAC practical repository, 2001

[Camb, 2003] Cambridge Advanced Learner's Dictionary (online version), Cambridge University, 2003.

[Carl, 1999] Organizational Change and the Digital Economy: A Computational Organization Science Perspective, Kathleen M. Carley, Carnegie Mellon University, 1999

[CEM, 1999] Common Methodology for Information Technology Security Evaluation – part 2: Evaluation Methodology, Common Criteria, 1999

[Clar, 1987] A Comparison of Commercial and Military Computer Security Policies, D. Clark, D. Wilson, 1987.

[Com1, 1999] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model – version 2.1, Department of Defense, 1999

[Com2, 1999] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements – version 2.1, Department of Defense, 1999

[Com3, 1999] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements – version 2.1, Department of Defense, 1999

[Comm, 2003] The Common Criteria Homepage, website: www.commoncriteria.org, 2003

[Cont, 1999] Controlled Access Protection Profile – version 1.d, National Security Agency, 1999

[CTCP, 1993] The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) – version 3.0, Canadian System Security Centre Communications Security Establishment Government of Canada, 1993

[ECP, 2003] ECP.NL, website: www.ecp.nl, 2003

[FC, 1992] Federal Criteria for Information Technology Security - Volume 1 & 2, National Institute of Standards and Technology & National Security Agency, 1992.

[Halp, 1986] Handbook of EDP Auditing, Halper, Davis, O'neil-Dunne, and Pfau (Coopers & Lybrand), 1986.

[Icat, 2003] ICAT metabase, NIST (National Institute of Standards and Technology), website: http://icat.nist.gov, 2003

[Inter, 2000] Internet Security Glossary (RFC2828), Network Working Group, 2000

[ITSE, 1991] Information Technology Security Evaluation Criteria, UKSP01, Communications-Electronics Security Group, 1991

[Labe, 1999] Labeled Security Protection Profile - version 1.b, National Security Agency, 1999

[Leav, 1964] Applied Organizational Change in Industry Structural, Technical, and Human Approaches, H. J. Leavit, 1964

[Marg, 1998] The Emerging Digital Economy, Lynn Margherio, Dave Henry, Sandra Cooke, Sabrina Montes, Kent Hughes, Secretariat on Electronic Commerce, U.S. Department of Commerce, 1998.

[NGI, 1995] Evaluatiecriteria voor IT-beveiliging, Nederlands Genootschap voor Informatica, Afdeling Beveliging, Dr. Ir. P.L. Overbeek, Drs. M. de Graaf, T. Newman, Ir. H. Schoone, L.A.M. Strous, 1995

[Owas, 2003] The Open Web Application Security Project (OWAS), website: www.owasp.org, 2003

[Prot, 2001] Protection Profile for Multilevel Operating Systems - Requiring Medium Robustness – version 1.22, National Security Agency, 1999

[Radi, 2003] Radium Customer Information Provider, website: http://www.radium.ncsc.mil, 2003

[Rain, 2003] Rainbow series, National Computer Security Center (NCSC) website: http://csrc.nist.gov/publications/secpubs/rainbow/index.html, 2003

[Side, 2003] Sidewinder G2 Firewall version 6.0 – Security Target, Secure Computing Corporation, 2003

[Simo, 1970] The New Science of Management Decision, H. A. Simons, Harper, 1970

[Sing, 2001] Single-level Operating Systems in Environments Requiring Medium Robustness – version 1.22, National Security Agency, 1999

[Stall, 2003] Cryptography and Network Security – Principles and Practices, William Stallings, 2003

[Stan, 2003] Amazon One-Click Shopping, Class: Computers, ethics and Social Responsibilities, Stanford University, website: www.stanford.edu, 2003

[Tane, 1992] Modern Operating Systems, Andrew S. Tanenbaum, Prentence Hall inc., 1992

[TCG, 2003] Trusted Computing Group (TCG), website: www.trustedcomputinggroup.org, 2003

[TCSE, 1985] Trusted Computing Systems Evaluations Criteria, Department of Defense 5200.28-STD, 1985.

[Tele, 2003] Telegraaf.nl, Nieuwsportaal van Nederland, article: Computercriminaliteit groot probleem voor bedrijven, 10 juli 2003, 09:48, website www.telegraaf.nl, 2003

[TNO1, 2002] Evaluation Assurance Level 3 – Common Criteria Guidance for developers, D. Out, E. Wesseling, TNO-ITSEF BV, 2002

[TNO2, 2003] TNO-ITSEF BV Information Technology Security Evaluation Facility, website: www.commoncriteria.nl, 2003

[Ubiz, 2000] Ubizen HIZEN – High Level Simplified Risk Management Methodology (internal document), 2000

[Wind, 2002] Windows 2000 Security Target – ST version 2.0, Science Application International Corporation, 2002

[Winn, 2003] Windows and .Net magazine network, website: http://www.winnetmag.com, 2003

[X800, 1991] Security Architecture for Open Systems Interconnection for CCITT Applications (X.800), The International Telegraph and Telephone Consultative Committee, 1991

[X810, 1995] Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview (X.810), The International Telegraph and Telephone Consultative Committee, 1995

[Yank, 2003] The Yankee Group, website: http://www.yankeegroup.com