Towards an aligned organization on Information Security

Closing the gap between the actual level of information security and business information security requirements

Supervised by: Dr. M.R. Spruit, R. Helms, Frank Herruer, Henk Marsman

master of business informatics utrecht university

Martijn Roeling
s3134792
16-03-2010
Utrecht University

Abstract

Information Security is mainly a topic that is considered to be Information Technology related. However, for successfully implementing information security, an organization's information security program should reflect the business strategy. Nowadays information security is in many companies enforced by the Information Technology department, based on what they think should be in place to protect their business from inside and outside threats and risks. Besides, information security covers many different subjects. This makes it hard for small and medium sized organizations to determine their information security program. Involving the Information Security Focus Area Maturity model (ISFAM) model in this process helps organizations in determining their current level of maturity and is capable of providing high level guidelines which the organization can use to structurally improve their information security level.

Preface

This Master thesis has been made as part of my Business Informatics education program at the University of Utrecht. This research can be of value to any person who is responsible for information security within the organization they work for or anyone that is interested in information security in general.

During the time spent on this project I received a lot of support from many people. First of all, I would like to thank my supervisors: Marco Spruit (University of Utrecht), Remko Helms (University of Utrecht) Frank Herruer (Deloitte) and Henk Marsman (Deloitte) for providing support, contacts and other resources during the research project.

Besides my supervisors I also would like to thank the organizations and other security specialists that have put time and effort into this thesis through interviews, correspondence, reviewing and evaluation. Finally I would like to thank my family, friends, colleagues and fellow students for supporting me throughout this process.

Table of contents

1. Introduction

Information security as a research topic is attracting a lot of attention lately. Newspapers without an article on information security are barely to be found. Take for example the case of the "OV-chipkaart" in the Netherlands. This public transport card is ought to be the standard for travelling by public transport. However, the card is vulnerable to attacks. Hackers passed the security on the card by using a cheap device. The consequence: everyone is able to place an unlimited amount of travelling credit on their OV-chipkaart. This could have led to significant losses for the OV-chipkaart provider and security is therefore a main issue for this organization. Improving the security of the card, would mean more costs but less fraudulent travelers. Another example is the loss of data by Sony's playstation network. Hackers were able to see sensitive data (i.e. Name, Credit card details, address) of every user on the playstation network. Users of the playstation network get the feeling that their data is not safe on the network, which eventually costs Sony more money than a better security. The consequence in this case: if the data gets stolen, the credit card details can be used or sold. In that case the users of the playstation network get involved directly. Cases like these caught the interest of researchers.

Most research if focused around the following topic: how can information security prevent the loss of sensitive information? Most studies done by information security researchers try to measure information security. This appears to be very difficult. According to Andrew Jaquith in his book "*Security Metrics: Replacing Fear, Uncertainty, and doubts*" (2007) IT-security can only improve if it can be measured. However, Jaquith (2007) also mentions that defining metrics to measure IT-security is a tough and sometimes undoable process. Since IT-security is part of information security, it is justified to say that the same holds for information security. Throughout the last years metrics have been defined to measure parts of information security, but the most important part is underdeveloped: metrics to support decision making. This is important because security metrics are servants of risk management and risk management is about making decisions. Therefore metrics to support decision making are a vital part of making information security measurable.

Decision making in the field of information security this thesis is defined as: "The process of selecting the right measures with as objective to improve the information security within an organization"

Since the metrics for assisting an organization with information security are not commonly known and/or ill defined, questions as how to structurally improve information security show up in companies. Organizations do not know how to effectively manage their security and what steps to take to become a 'secure' organization (Chapin and Akridge, 2005).

The topic of maturing information security in a structured way has not received much attention in research yet and is interesting to look at. Another reason to look more closely at this problem is that both IT and business are involved. Hence, implementing information security features/processes/artifacts does not only affect IT, but also business. It still happens that IT has its' own information security program next to the program of the business. Information security is not only about IT security. Information security also has a business side in terms of a secure work environment, not losing confidential papers on the street, and ensuring awareness and compliance throughout your organization. Communication between business and IT is a requirement for the successful creation and implementation of an organization wide information security program.

The problem addressed in this thesis is the lack of understanding and awareness at management level and service/product owners to effectively improve their information security. This starts by understanding where your organization is and where it wants to be. The problem is partly due to a lack of knowledge sharing between the IT personnel, who implement security measures, and the product/service owners who sell, improve and are responsible for the product/service. Another reason for this problem is the lack of attention a product/service owner pays to information security. Hence, If one does not know anything about information security and its' importance, how could that person improve it? Business Security and IT Security should thus be aligned to create awareness and ensure an information security program that suits both the business and IT. To do so, this thesis provides an artifact to improve an organization's information security on a high level in a structured way.

The overall problem is divided into two different research questions; one for science and one for business. The scientific research question is defined as follows:

Science research question:
"How and by what means can the gap between business requirements with respect to information security and the actual level of Information security be minimized or closed?"

The objective for the business is:

Business Objective:
"Providing a method/tool that enables companies and organizations to increase their information security level in a structured and effective way."

The thesis contributes to the development and understanding of information security. The final model addresses the maturity of information security on a high level and is therefore suited for new research. Examples of further researches could be the same research adjusted to a different sector or the extension of the final model to a more detailed level.

An organization can benefit from the model by using it as a guideline for their information security program. Because the model combines literature with field experience and indicates dependencies between different parts of information security, the model provides a solid basis to construct an information security program on. For a consultancy organization this model can be a business opportunity. They can offer information security maturity assessments to help organizations in their information security program development.

The next chapter describes the used research methodology and deliverables. Chapter 3 provides theoretical background on information security. This part of the literature study consists of a timeline containing important information security events to increase not only my knowledge on information security, but also has influence on the final model. Chapter 4 discusses what kind of model is made to satisfy both research questions. Chapter 5 is the start of the actual research. The different focus areas of information security are discussed one by one as a basis for the final model. The final model can be found in Chapter 6 and the evaluation of this model in Chapter 7. Based on the results, the conclusion is made in Chapter 8. Further research and discussion points are covered in Chapter 8. Appendices and the references conclude this thesis.

2. Methodology

Developing an information security artifact requires a structured approach. This chapter points out the consecutive steps necessary to complete the final model. To make the problem statement easier to understand, the problem statement is divided into five sub questions listed below.

Sub questions:

1. *"What are the focus areas in the information security domain? "*
2. *"What are applicable metrics to measure the information security focus areas?"*
3. *"Is it possible to define a maturity scale for the different focus areas and if so how are they defined?"*
4. *"How can the maturity of information security be modeled?"*
5. *"What would be an appropriate distribution for the maturity stages?"*

These five questions are based on an analysis that is stated in chapter 3.2. Conclusion of this analysis is that a maturity model would suit best to close this gap. Based on this decision, the first, third, fourth and fifth question are needed to develop the model. The third question is to assure that the model can be turned into an assessment tool.

Since the goal of the thesis is to develop a model, the design science research method of Hevner et al. (2004) is used. Adapting this model to this thesis gives figure 1 as a result. Looking at figure 1, the environment consists of people, organization and technology. All three needed to complete the research. System Research (the second column) is the research itself and the knowledge base (the last column) comprises the theories on which the model is based and built. An advantage of this model is the ability to scope the research. Within the environment column there is a focus on people with information security affiliation and on processes. In the justify/evaluation box inside the system research column can be seen that the case study is performed at a small/medium sized organization. Peter Fagan (1993) wrote a paper about information security being different in various industries. However, focusing this model on only one industry would negatively impact the benchmark capabilities of the results and therefore it was decided to keep the model as generic as possible and leave the small changes up to the organizations using the model. Another addition to the scope is that metrics are mostly derived from literature. If metrics are not available in literature, they are defined according to literature and evaluated by domain experts. In the last column of the design science model some basic foundations as the ISO27K series are stated. These foundations help developing the final model.

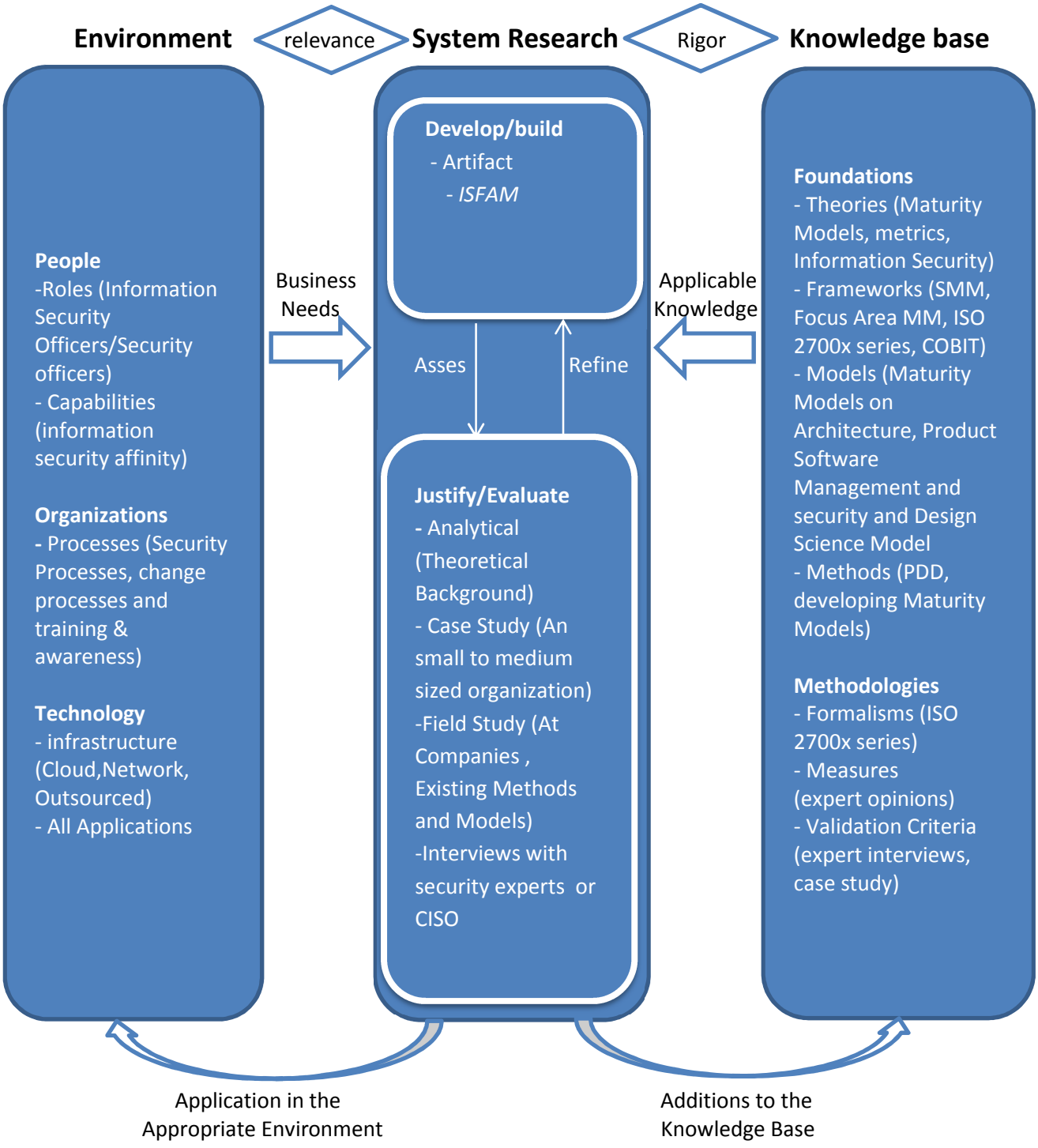

Figure 1: The design science model specified to this research. (hevner et al. 2004)

Steps taken to develop this model are defined by Takeda et al. (1990). Takeda et al. describe the design research cycle by the following fisteps:

1) Awareness of the problem
   The first step in a design science research is to look closely at the problem, to see if it really is a problem and to define the problem.
2) Suggestion "to suggest key concepts needed to solve this problem"
   In the suggestion phase alternatives for the problem are made.
3) Development
   One of the alternatives is developed to a real model.
4) Evaluation
   This model needs to be evaluated by experts and might be validated in a case study to get a proof of concept. Phases 2,3 and 4 are repeated until an appropriate model is made.
5) Conclusion
   The conclusion consists of the results gained from the model. It states whether the model really works and what it's limitations are.

Translated to a process-deliverable diagram (PDD) the design science model becomes the research method as depicted in figure 2. The PDD modeling technique is explained by van de Weerd and Brinkkemper (2008). This research is divided into four phases starting with a literature study. The literature study has as goal to get a better understanding of information security and to gain knowledge about past important (e.g. thesis related, world changing) security events. This phase is comparable to phase one and two in the model of Takeda et al. (1990). Next is the Focus Area Identification phase (e.g. phase 3 of the model of Takeda et al.). This phase has three steps in order to set up a list of focus areas related to information security. First, literature is studied to identify focus areas. This is doing by making a table to compare different existing information security models. Those models hold focus areas that can be used for this thesis. Combining, adding and deleting focus areas from these models results in a list of focus areas that need to be included in the final model.

For the final focus area maturity model there needs to be a maturity model for every focus area. Why this is the case, is further explained in chapter 3.2. The maturity models for every focus area are made using the Capability Maturity Model standard or derived from literature. In both cases, the maturity model for a focus area is evaluated by one domain expert to add practical experience to the model (e.g. phase 4 in the model of Takeda et al.). Metrics are attached to the maturity model, to ensure practical value of the model. Hence, these metrics can be used to measure the maturity level of an organization in that particular focus area on a high level.

The last phase is the development and evaluation of the model (e.g. phase 4 and 5 of the model of takeda et al.). The model is constructed out of the maturity models made in the third phase by using experts, common sense and dependencies. By performing a case study, the model should be practically and theoretically sound.

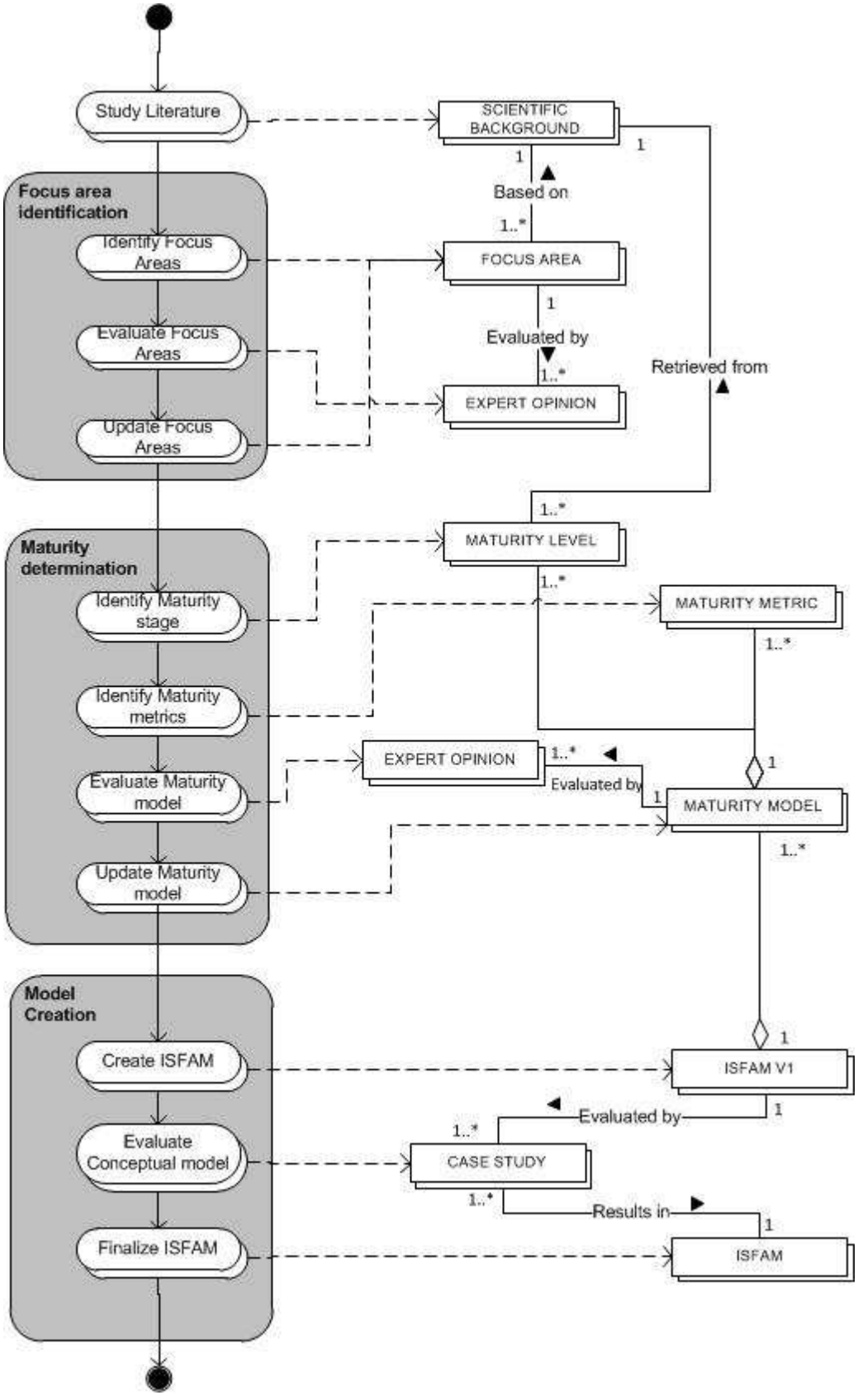

Figure 2: PDD of the Research

3. Information Security History

Information security, although not as a concept, existed already a long time ago. Even when there were no computers it was important for persons to keep their information secure. It was, just as it is now, important to keep your data safe, only give persons access that need access, and make it available to those with the corresponding rights. Information security as a concept arose in the late 1960's. The first area of interest in the field of information security was access control. The Multiplexed Information and Computing Service (MULTICS) operating systems introduced an early type of access control. Thereby it is the first operating system focusing on security as primary goal (Whitman and Mattord, 2009). Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to breach of security (Sandhu and Samatari, 1994). More on Access control can be found in chapter 5.8. Access control within MULTICS is based on directories within a system. For each directory, every user has rights (e.g. read, write, execute, modify entries, append entries or obtain status). By applying those rights on directories it was possible to set access constraints.

The first time information security was introduced as a concept it could better be defined as computer or IT security (Whitman and Mattord, 2009). Information security around 1960 was completely based on the security of computers and did not pay attention to other information security related aspects such as physical access control although it did exist (i.e. locks on doors). The Department of Defense (DoD) made Computer Security publically known. The DoD assigned a task force to identify the problem of time-sharing (sharing of a computing by at least two users) and multi-tasking in a computer environment. The report was published in 1970 and concludes that "providing satisfactory security control was in itself a system design problem" (Whitman and Mattord, 2009).

Before continuing the timeline, pictured in figure 3, information security needs to be defined as it is known in this century. Information security can be defined as (Jones, Kovachich and Luzwick, 2002):

Information Security:
"the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats."

Business often refers to the Confidentiality, Availability and Integrity (CIA) triangle instead of using this definition. CIA is further explained in section 3.3.

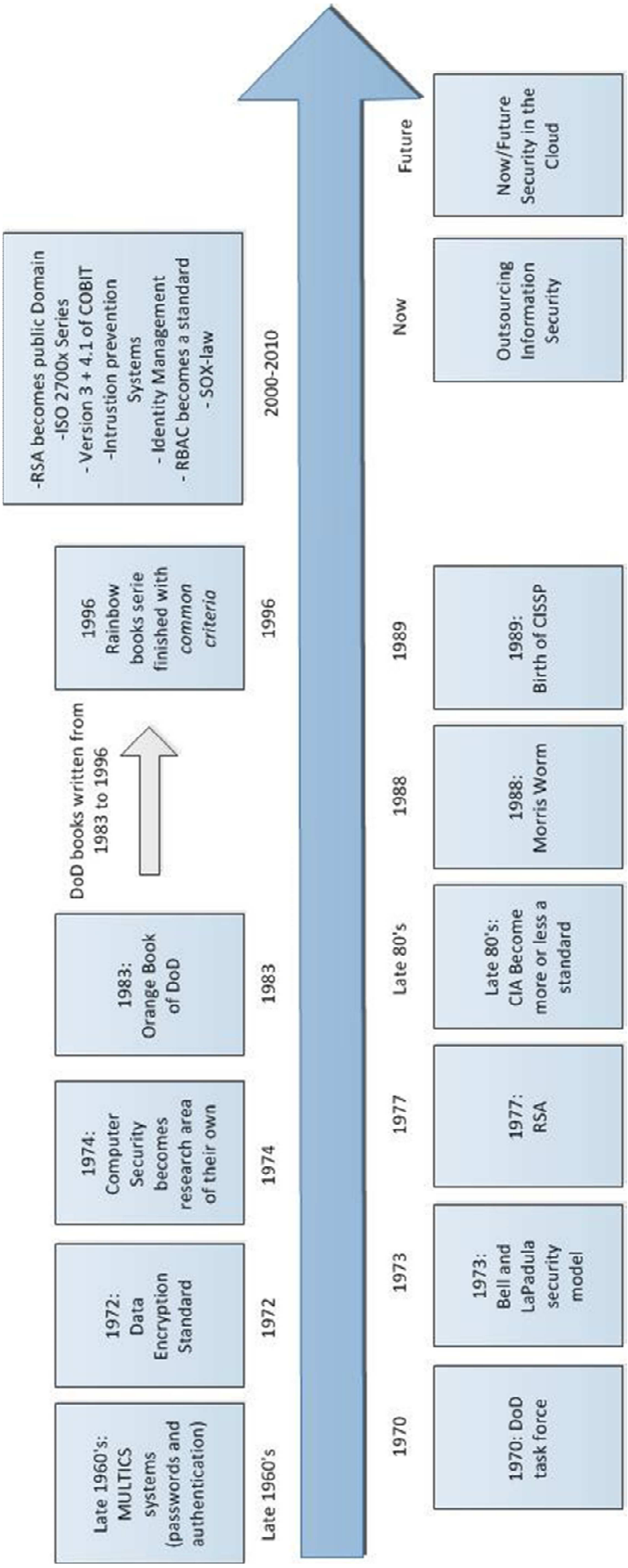

Figure 3: A timeline for information security.

The following sections describe the important historical events for information security. These sections are based on the timeline depicted in figure 3. The sections are mostly ordered in time, except for a few due to readability of this chapter. E.g. it is not readable when switching topics all the time. If the topic handled has much in common with a topic further on the timeline, it is combined with the topic being discussed at that moment.

3.1.Data Encryption

During the time that the DoD was writing a book about their findings on information security, a first encryption algorithm was developed by the National Security Agency. The algorithm became a standard in 1977 and is named Data Encryption Standard (DES) (Landau, 2000). Goal was to secure data sent over networks by cryptography. In this way it becomes more difficult for intruders to gain sensitive data. Although DES used only a 56-bit key length, it turned out to be completely safe until 1990. Advanced Encryption Standard (AES), the follow-up of the DES, uses 128, 192 or 256 bits which is significantly stronger. In 1998 DES was decrypted for the first time by a $250000 dollar computer in 54 hours with as result that DES is barely used these days.

RSA (invented by and stands for Rivest, Shadir and Aldeman in 1977) is an algorithm for public-key cryptography. Consisting of three steps (key generation, encryption and decryption) it provides systems with the necessary security regarding authentication (Burnett and Paine, 2001). Basically, the RSA algorithm uses a public and a private key for communication. Both are necessary to secure, encrypt and decrypt the communication. However, computers are getting more and more processing capacity and that is the weakest point of the RSA algorithm. With a lot of computation time it is possible to trace back the private key and decrypt the encrypted message. However, RSA is still one of the most used and most safe algorithms to secure messages. Since September 2000 RSA is available for the public domain.

3.2.The first security models

Dieter Gollmann is the first to write about security models (Leeuw and Bergstra, 2007). Security models can be defined as “a formal description of a security policy that a system should enforce”. A security model represents a machine in an initial and secure state. The first model, the Bell LaPadula (BLP), uses labels to represent the multilevel security policy. Multilevel security means that the model is able to make a distinction between users in terms of access rights.

Based on the report of the DoD from 1970, the BLP model was created in 1973 by Bell and LaPadula. The BLP model is also called Multi-Level Security (MLS) model. Basically, the model uses two out of three types of Access Control Policies to serve especially the military sector (Bell and La Padula, 1976):

- DAC: Discretionary Access Control
- MAC: Mandatory Access Control
- RBAC: Role Based Access Control

The first one stated is Discretionary Access Control (DAC) - based on access rules knowing what requestors are allowed to do with protected resources.

The BLP model uses one DAC:

- The Discretionary Security Property – Use of an access matrix to specify the discretionary access controls.

An example of this matrix is shown in table 1. The four different access-attributes are (Sandhu and Samatari, 1994):

- Read (r)
- Write (w)
- Append (a)
- Execute (e)

	Program 1	Program 2	Document 1
Alice	R	rw	-
Bob	X	-	r
Charlie	rx	w	rwx

Table 1: An example of a Discretionary Access Control matrix

The second one is Mandatory Access Control (MAC) - compares how sensitive or critical system resources are with which system identities are allowed to access certain resources. Another name for MAC is Lattice-Based Access Control (LBAC) (Denning, 1976). Lattice herein refers to a partially ordered set where every subject and/or object has at least an upper bound (join) and a greatest lower bound (meet) of access rights. For example, if two subjects want to access an object then their security level is defined as the meet of both levels of the two subjects. According to Ferraiolo & Kuhn (1992) MAC can be defined as: "a means of restricting access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity".

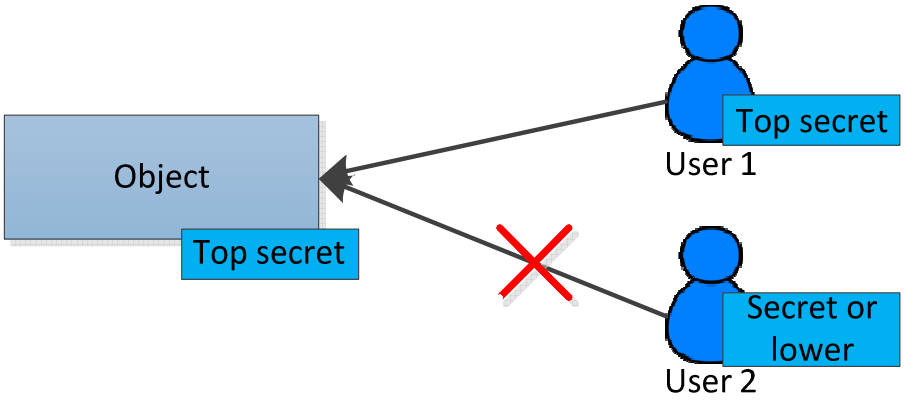

Figure 4: The working of Mandatory Access Control

The BLP model uses two MACs:

- Simple Security Policy: A subject at a given security level may not read an object at a higher security level. The subject may not "read up". For example, a person with a Secret clearance

level may not read a report that is labeled with Top Secret. Hence, Secret is lower than Top Secret.

- The *-property (star property) or Confinement property – A subject at a given security level may not write to any object with a lower security level. The subject may not "write down". For example: a person with a Top Secret clearance may not write to any object except for the Top Secret level. This is not allowed, because Top Secret is the highest security level. Note: Trusted subjects are not restricted by this property.

The third one, not used by BLP, is Role Based Access Control (RBAC). RBAC was proposed in 1992 by Ferraiolo and Kuhn (1992). They oppose that RBAC is more central to the secure processing needs of non-military systems then DAC. As the name already insinuates, RBAC is based on functions of roles within an organization. Users are herein not allowed to pass on rights to other others. This difference can be marked as the main difference between DAC and RBAC. RBAC control is a form of MAC. The difference is that RBAC is not based on multi-level security requirements and MAC is. Multi-level security means that the policy uses security levels as well as categories. Both determine who has access to what. Figure 5 shows how RBAC arranges the access for groups of users to certain functions.

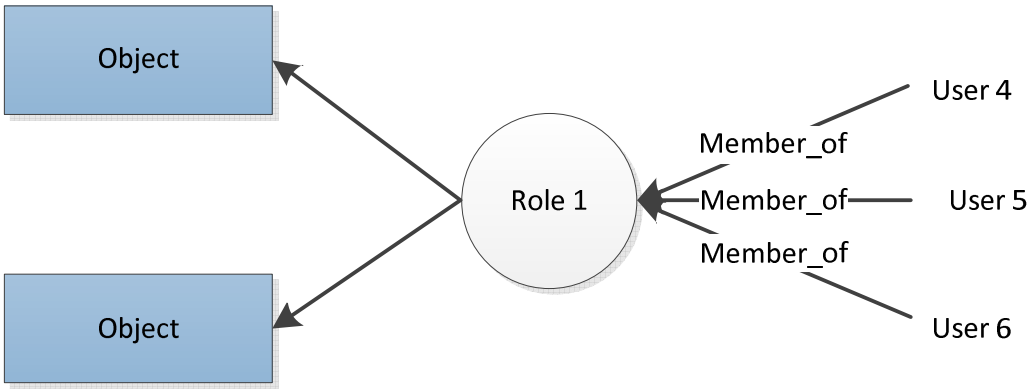

Figure 5: The working of RBAC

In practice many end users do not "own" the information for they are allowed access. The organization is seen as the information "owner" for them. Discretionary Access Control might not be appropriate for these cases since passing-on rights is not what you want (e.g. you will lose control). RBAC is a nondiscretionary access control mechanism aimed at the central administration of a security policy. Decisions regarding access control are role based and those roles are part of an organization. A role specifies a set of transactions that a user or set of users can perform within the context of an organization (Ferraiolo & Kuhn, 1992). RBAC allows assigning tasks to individuals and might thus be more appropriate in some situations if it is not allowed to pass on rights.

Relating the three access control policies back to the BLP model ends up in figure 6.The BLP model is based on a combination of MAC and DAC and is a superset of MAC (cannot be seen in the figure 6) since it complies to the same properties as MAC has.

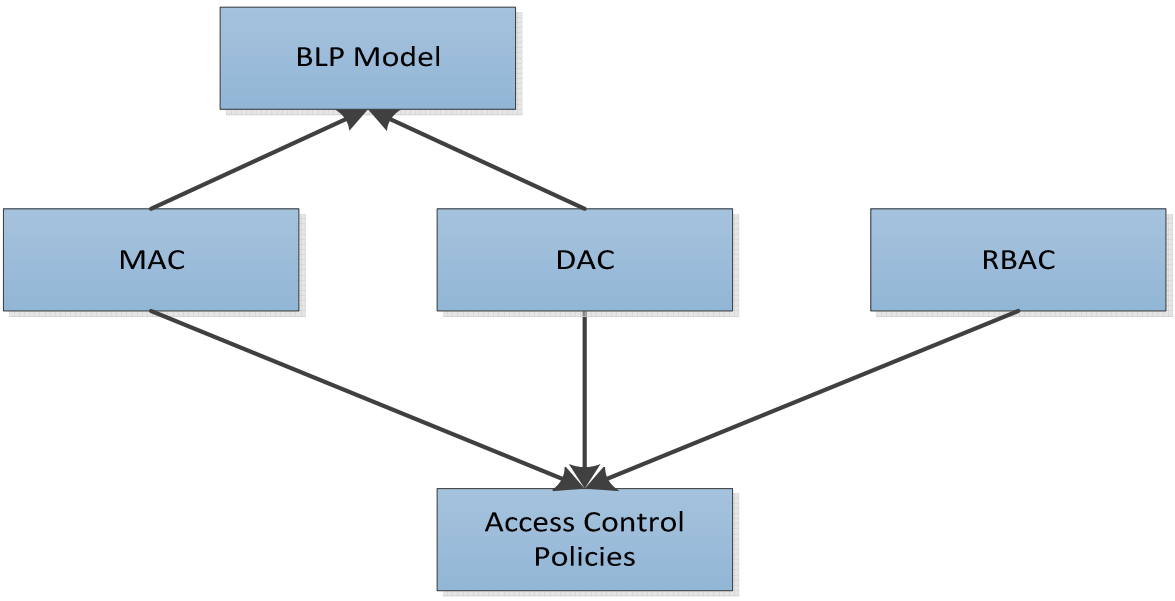

Figure 6: An overview of the three Access Control Policies.

The BLP Model has three major facets:

1) a descriptive capability (elements),
2) general mechanisms (limiting theorems) and
3) specific solutions (rules).

To describe the system's state BLP uses a triple consisting out of the three facets mentioned above:

(subject, object, access-attribute).

This means that a subject has current "access-attribute" to object in the state. The total system can then be described as a set of these triples. This is mostly done by creating a matrix with subjects and objects on the two axes and in the cells the corresponding access-attributes. For filling out the access matrix it uses the Discretionary Security Property (see table 1).

Furthermore the model places labels on the objects and has clearances for subjects. The labels range from top secret as being the most sensitive to unclassified as being the least sensitive. In between are, respectively from high to low sensitivity, secret and confidential. This helps determining in what to invest and in what not (yet) to invest.

The Bell-LaPadula model focuses only on confidentiality and is thus limited considering the cases where it could be used. The Biba Model developed by Kenneth J. Biba (1977), addresses integrity as well as confidentiality. Instead of using the rules of BLP, Biba uses two other rules:

1) A subject at a given level of integrity must not read an object at a lower integrity level (no read down, see figure 7). This is known as the Simple Integrity Axiom.

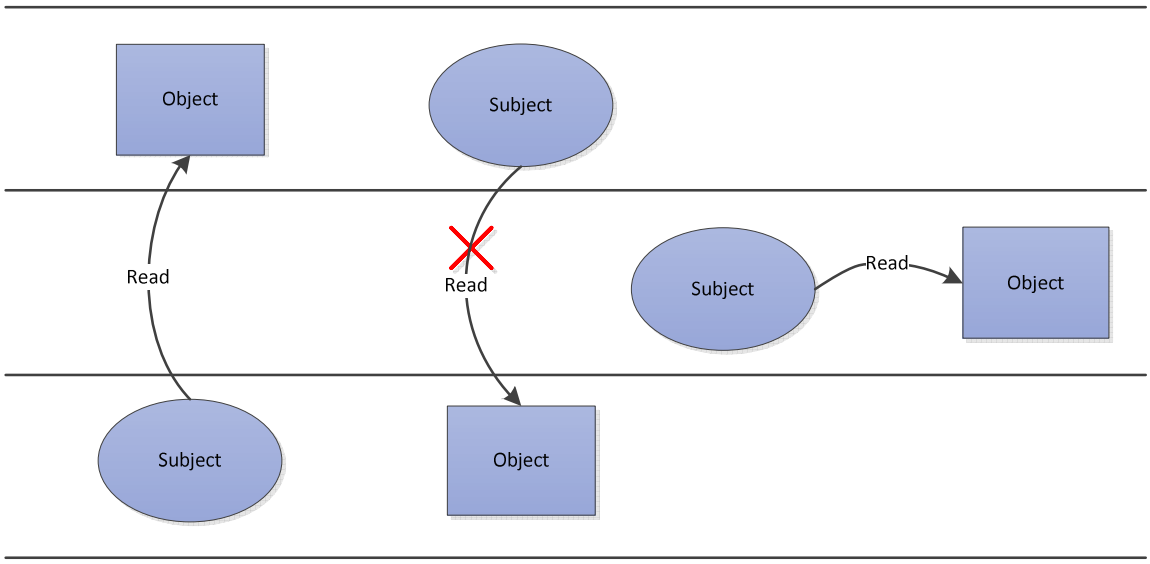

Figure 7: No read down rule of BiBa

2) A subject at a given level of integrity must not write to any object at a higher level of integrity (no write-up, see figure 8). This is known as the * (star) Integrity Axiom.

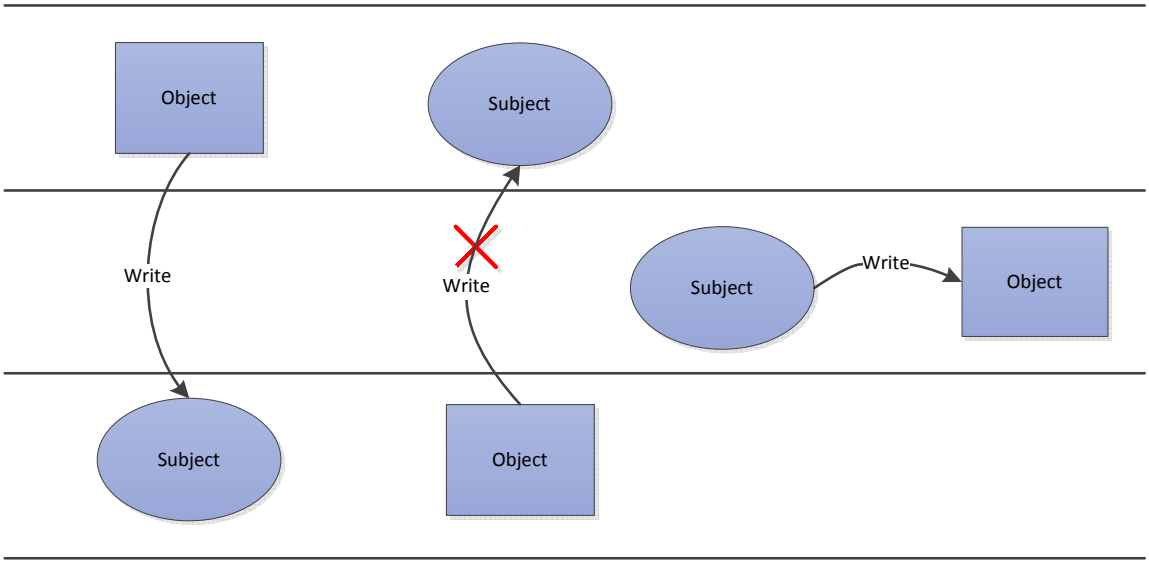

Figure 8: No Write-up rule of BiBa

While BLP uses the sentence “no read up, no write down”, Biba uses the opposite.

Clark and Wilson made their model in 1987 named after them (Clark-Wilson model). It has three types of identification (Clark and Wilson, 1987):

- Identification of data items for which security enforcement is crucial (CDIs)
- Identification of transformation procedures (TPs) that can access data
- Identification of user roles, in terms of authorization to use particular TPs.

Access controls are specified by triples: <user, TP, data>. This representation states that a user is allowed to perform a certain action "TP" on data. To strengthen access control and integrity mechanisms, the Clark-Wilson model uses two mechanisms. First, separation of duty states that each critical operation has to be executed by at least two different roles. Second, the transaction preserves data and prevents users from random manipulating data by assuring that the data stays in a consistent state after changes.

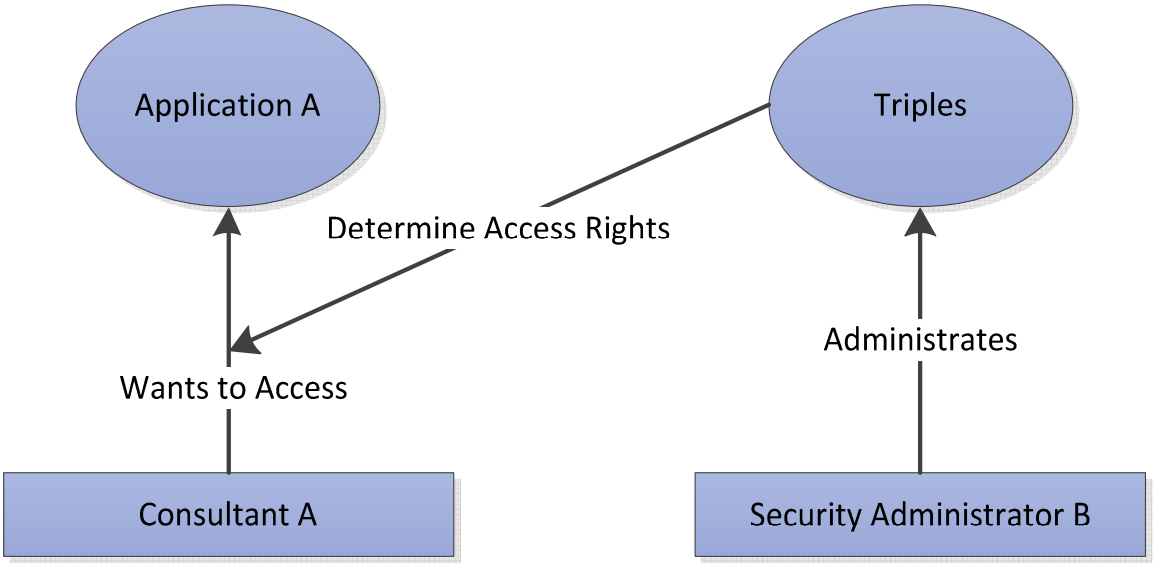

Figure 9: Clark Wilson Model

The Bell LaPadula model has been as important to the military sector as the Chinese Wall policy is to the commercial sector. The Chinese Wall policy (1989) is required in many financial organizations. The basic idea of the Chinese Wall policy is that people are only allowed to access information that is not conflicting with other information already processed. Information already processed is information held on the computer and previously accessed by the user. (Brewer & Nash, 1989)

To following example gives an idea of how the Chinese Wall policy looks like and what the consequences are of adopting this policy. Imagine that there is an independent person who needs information for a certain project he is carrying out for company A. There are two candidate companies that have the information he needs: B and C. Company A and company C are both working in the financial industry and Company B is an energy supplier. When a user first needs certain information, he/she can choose which company to get it from. In this case the user first picks the information of company A to look at, because he is already working for them. No conflicts arise in this situation because the user does not hold any information yet. Now, the user has the information of company A in his/her knowledge base and wants to look for other or more data. Company B works in a different industry and there is thus a high chance that no conflict of interesting class exists. The user in this case is able to access data from Company B and thereby extending the knowledge base. Company C, however, also works in the financial industry and a conflict of interesting classes is very likely to appear. Hence, the information already possessed might be in conflict with the data requested. Advantage of this model is that users cannot use their knowledge of previous assignments in order to help a conflicting company. This would result in more similar solutions which is unwanted because every company has its' own unique selling points.

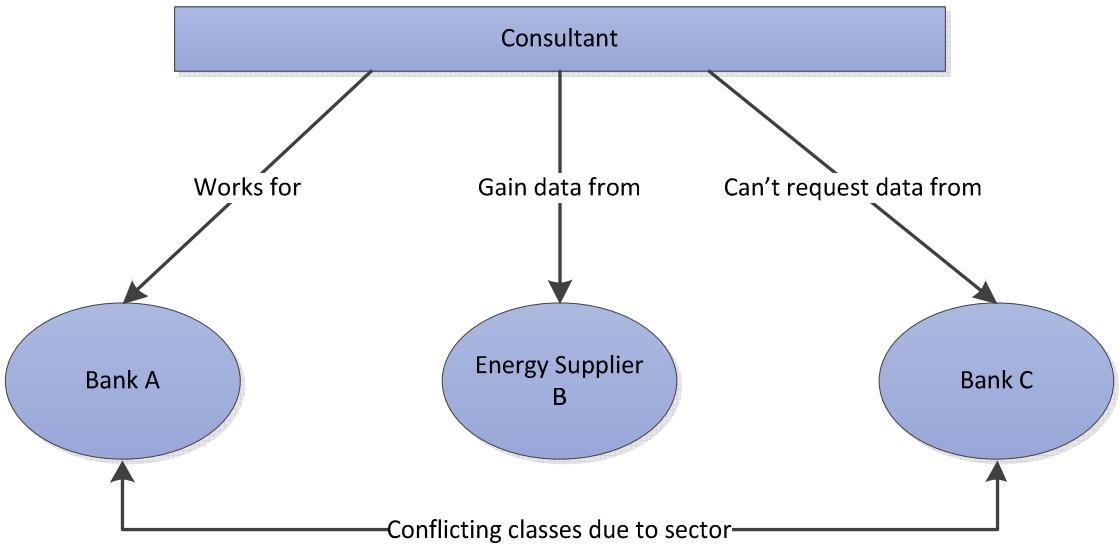

Figure 10: Chinese Wall Policy

After the first models were accepted and used, information security became an important research topic for scientists around 1974 (Leeuw and Bergstra, 2007). Nine years later the DoD published the 'Orange Book'. This book contains the first rating system for measuring and establishing the level of security of any given computer system. After the 'Orange Book' the DoD published more books on information security (in figure 3 marked by the small arrow). Result of all published books is the so-called 'rainbow book series'.

3.3.Standards, Laws and Certificates

In the late 1980's Confidentiality, Integrity, Availability (CIA) becomes known worldwide and an informal standard (Bishop, 2004). Individual processes and systems are judged using the CIA criteria to determine their need for security. This judgment is called the Business Impact Analysis (BIA) and a possible outcome of a BIA can be seen in table 2. The higher the CIA scores for a system or process, the more need for security. In this way, a portfolio manager, security manager or consultant is able to select the most vulnerable systems and processes of the organization. Nowadays, CIA is still an often used method because the method is light weight and fast to execute.

A CIA analysis typically looks like this. Every application receives a rating 1 to 3 where 3 is the highest in terms of criticality.

	Confidentiality	Integrity	Availability
Application 1	3	2	1
Application 2	1	1	1
Application …	2	1	2
Application n-1	1	3	1
Application n	1	1	1

Table 2: CIA analysis

When organizations tend to look further then application level they can look at efficiency and effectiveness as well. Both are used on a governance level as an addition to the CIA ranking method.

In 1989 a certificate for information security was created called Certified Information Systems Security Professional (CISSP). The CISSP certification is controlled by the International Information Systems Security Certification Consortium, abbreviated $(ISC)^2$. At the moment $(ISC)^2$ has over 65000 certified members that hold the CISSP certification and is the best known security certificate at the moment. The CISSP course includes ten different information security domains (ISC^2, 2011):

- Access control
- Application Development Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security Governance and Risk Management
- Legal, Regulations, Investigations and Compliance
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

As a follow-up, there is the ISSAP Certification. This certification can be gained after two years of experience in the field of security architecture. Individuals subscribed to this course usually play a key role in their information security plan. The ISSAP course covers six different domains:

- Access Control Systems and Methodology
- Communications & Network Security
- Cryptography
- Security Architecture Analysis
- Technology Related Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Physical Security Considerations

From 2000 to 2010 information security started to play an important role in the modern society. Due to globalization, the increasing amount of people having access to the internet and the movement of businesses to the World Wide Web (i.e. webshops) a movement from physical crime to cybercrime is taking place. Next to the CISSP, a couple of frameworks were set up of which COBIT and ISO27K are assumed to be most important. These models are known for their capability in supporting information security management. Both frameworks deliver an extensive set of controls and measures to prevent attackers from stealing sensitive and valuable information out of organizations. Being compliant with one of the frameworks does not imply that you are safe. Hence, attackers will always find a new way to get around the security measures taken. Since organizations nowadays even have more entries to their data (physical, logical and on the web) information security has become an inevitable topic for management.

COBIT version 4 (IT Governance institute, 2000) is a framework for IT Governance and Control. COBIT version 5 has been released at the start of 2012. Its goal is to bridge the gap between control requirements, technical issues and business risks. The framework is pictured in figure 11. Although the framework addresses more topics than only information security, it has a Control Objective (CO) named Ensure System Security (DS 5) that is about information security. All Detailed Control Objectives (DCO) that are part of DS 5, a total number of 21, are related to information security.

Furthermore, the COs Communicate management aims and directions (PO6), Assess and manage IT risks (PO9) and ensure continuous service (DS4) contain information security related DCOs which are interesting for the development of the final model.

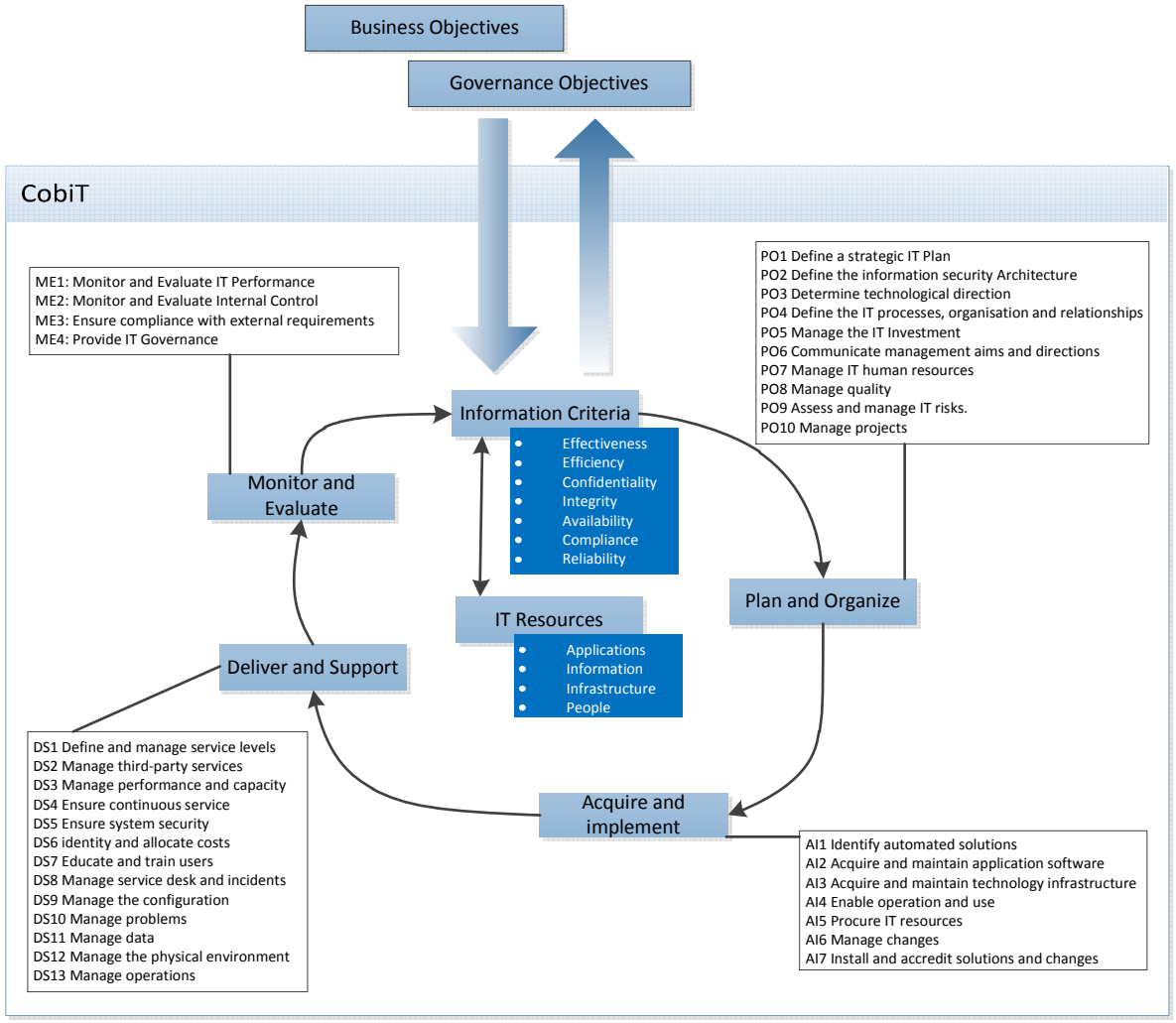

Figure 11: COBIT Framework.

The ISO/IEC 27001 and 27002 make another framework for information security. It was published in 2005 (British Standard Institute, 2005) as the first standards of the ISO 2700x series. ISO/IEC 27002 was formerly known as the ISO/IEC 17799 standard. The ISO/IEC 2700x series consist of five groups with different topics:

1) Information security management systems – Overview and vocabulary. This standard is the basis for the 270xx series and offers an overview of how all standards in the 270xx series relate to each other.
2) Requirements standards. This group has the most important standard of the 270xx series, namely the ISO/IEC 27001 standard.
3) Guidelines standards. This group is about the application of the requirements set up in group 2. The best known standard is the ISO/IEC 27002 – Code for information security. Besides

the 27002 standard, another seven standards are managed by this group: 27003, 27004, 27005, 27007, 27008, 27013 and 27014.

4) Sector-specific requirements/guidelines standards. Not all standards are suitable for every organization or sector. Therefore this group handles sector specific standards. ISO/IEC 27010, 27011 and 27015 are under their supervision.

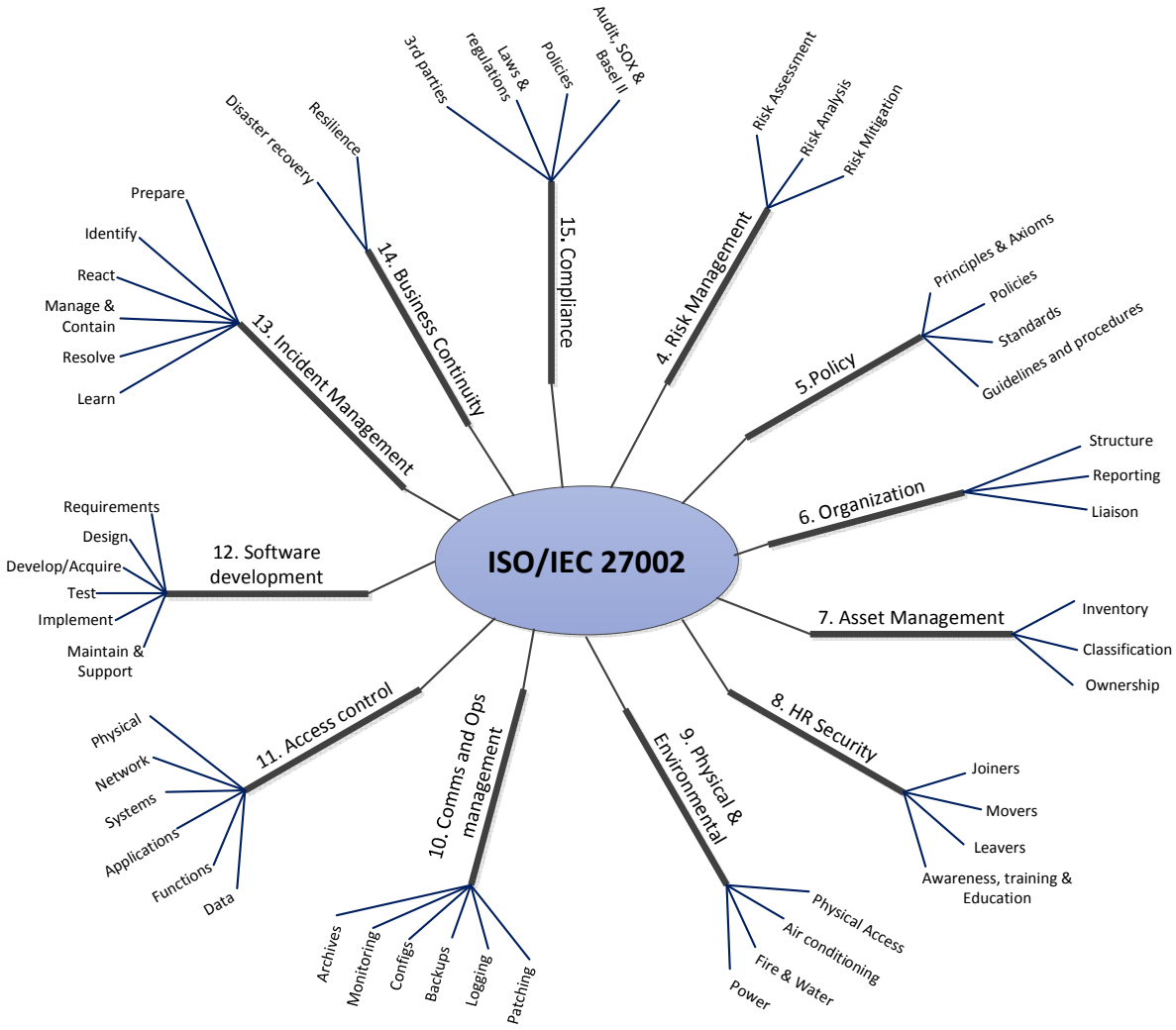

Figure 12: ISO 27001/27002 security Framework chapters.

5) Control-specific guideline standards. This group works on six standards of which most are not yet published. Only the ISO/IEC 27033-1 on network security is published so far.

ISO/IEC 27001's task is to protect all information assets of all types of business. The information security management system standard was developed to secure the information cost effectively and risk management is the main focus of this standard (Humphreys, 2006).

Both the ISO 2700x and COBIT framework are addressing more than IT security. Whereas IT security only encompasses the security of information systems, information security encompasses all ways which enable an organization to protect their data. This includes organizational aspects (i.e. roles, responsibilities and polices) as well as physical (i.e. locked doors, fortified walls) and technical

aspects (i.e. passwords, secure protocols, secure configuration). COBIT even makes an additional step by including information security into IT governance. This implies that information security should be a responsibility of the IT department. However, the contrary is true. Risks should be identified by the business, which should be secured by measures most likely implemented by the IT department. Nowadays, organizations most likely have their security department report to the CIO (Chief Information Officer), CISO (Chief Information Security Officer) or CFO (Chief Financial Officer).

The most famous law, and therefore include in this thesis, in the field of information security is Sarbanes-Oxley (SOX). The SOX law was established by the U.S. Government after the financial scandals of a couple of large companies such as Enron (Coates IV, 2007). Named after Paul Sarbanes and Michael Oxley, this law "defines management responsibilities in annual and quarterly reports, the control environment, risk management, and monitoring and measuring control activities." The SOX act is mandatory since 2002 and consists of eleven titles which are mentioned below. In most cases the laws can be adopted by off the shelve packages. (US Government, 2002)

1. Public Company Accounting Oversight Board (PCAOB)
   PCAOB's purpose is to provide independent oversight of public accounting firms providing audit services.
2. Auditor Independence
   This part of the SOX law contains standards to enhance external auditor independence. In this title is also the restriction that auditing companies providing non-audit services (e.g. consulting) for the same customers.
3. Corporate Responsibility
   Title III states that senior executives are responsible for the accuracy and completeness of corporate financial reports. The title as a whole also describes the communication between executives and external auditors.
4. Enhanced Financial Disclosures
   Title IV describes enhanced reporting requirements for financial transactions (i.e. off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers). The SEC reviews the controls and reports on these transactions.
5. Analyst Conflicts of Interest
   Title V contains measures to help restore investor confidence in the reporting of securities analysts. The measures define the codes of conduct.
6. Commission Resources and Authority
   Title VI contains practices to restore investor confidence in securities analysts. It also defines the power of the SEC regarding censuring/banning securities professionals from practice and when they are allowed to use this power.
7. Studies and Reports
   Title VII is about studies and reports of the organization done by the Comptroller General and the SEC.
8. Corporate and Criminal Fraud Accountability
   Title VIII is also known as the "Corporate and Criminal Fraud Act of 2002". It describes the penalties that can be given for manipulation or every other interference that makes it more difficult for investigators to come up with a report.
9. White Collar Crime Penalty Enhancement
   Title IX is also known as the "White Collar Crime Penalty Enhancement Act of 2002". Just like

Title XIII it describes penalties. In this case the penalties given for white collar crimes and conspiracies. If a company fails to get a certificate on their corporate financial reports, this also counts as a criminal offense.

10. Corporate Tax Returns
    Most important of this Title is that the Chief Execute Officer (CEO) should sign the company tax return.
11. Corporate Fraud Accountability
    Another name for this Title is "Corporate Fraud Accountability Act of 2002". This act identifies corporate fraud and records tampering as criminal offenses. The SEC is in this way enable to freeze or stop large and unusual payments.

3.4.Intrusion Detection and Prevention Systems

The Morris Worm was one of the first computer worms distributed over the internet. The Morris Worm is often mentioned as the first computer worm, but that is mostly because this worm was the first worm to get a lot of media attention due to its quick worldwide coverage. Between 6000 and 9000 computers became infected on November the 2nd 1988 (Orman, 2003). An overload of the internet and a lot of failing servers were the result. Morris was brought to court for the damage he had accidentally done by releasing this worm. He had to pay a $10000 fine, serve 400 hours of community service and was convicted to three years of probation. Since this incident, a lot more attention is given to computer security and the prevention and detection of these threats.

Complete security, however, will never exist. In June 2010 another worm was detected: the so-called Stuxnet worm. Primary goal of this worm is to take control of industrial facilities (Symantec, 2010). To do so, the worm uses known vulnerabilities in different operation systems. The Stuxnet worm gets into systems by fooling the anti-virus scanner with a certificate signed by two well-known companies. Once it reached a computer, it installs a rootkit. The rootkit makes sure that the worm is invisible on the system. From this point onwards the worm is able to search and find industrial control systems on which it can inject hidden code.

Intrusion Detection Systems (IDS) are made for warning a human when there might be unauthorized activity (Bace and Mell, 2001). A human has to determine whether this activity truly is unauthorized or a false positive. IDSs are not able to prevent attacks. They can only warn a human when it detects a suspicious activity in progress. Basically, there are two types of IDSs (Lee and Stolfo, 2000, Fuchsberger, 2005):

- **Anomaly detection based.**
  Anomaly detection based systems compare the observed activities with the expected normal usage profiles. Events considering a specific user that occur outside normal behavior of that user are called anomalies. An advantage of an anomaly detection based system is that it can detect attacks without the need for signatures. At the same time this leads to a disadvantage. Because there is no signature needed the IDS finds a lot of false positives.

- **Misuse detection based.**
  Misuse detection based systems search for attack signatures in the audit data which show known misuse. Misuse detection based systems are based on rules and patterns. Misuse detection based systems are often considered as more accurate because they generate less

false positives. Hence, they do work with signatures. However, future unknown attacks are not predictable because there is no pattern or rule available for them. These attacks could thus go undetected until the database has been updated by a human with new patterns and rules.

Very similar to IDSs are Data leakage/loss prevention systems (DLP). DLP systems came to the market after IDSs and are slightly more advanced. The difference between both is the usage of sensitive data. DLP systems identify sensitive data and use that information to be able to protect it better (SANS institute, 2008). Besides, DLP can run in both preventive and detective mode.

An Intrusion Prevention System (IPS) is a system that has the ability to detect attacks and prevent the attacks from being successful. It can be seen as an extension of IDSs. By using different detection methods and its position in the network the system is able to detect and prevent attacks more accurately. This results in less false positives. An IPS has to comply with a certain amount of characteristics. First of all, an IPS should be accurate. False positives generate events to prevent the attack. When the attack appears to be a false positive, it might result in problems for authorized users. Second, an IPS needs to work at wire speed. If not, the IPS can become a bottleneck in the network. Furthermore, an IPS has to use multiple flexible methods to respond to completely new attacks that are not documented yet. Last, the system should also be reliable and high available. Downtime or interference with other programs need to be minimized or in the most favorable conditions should not be there.

IPSs can also be divided into two categories (Fuchsberger, 2005):

- **Host-based IPSs (HIPSs)**
  HIPSs are comparable with antivirus software (SANS Institute, 2008). The main difference is that HIPSs actively respond to intrusion related activities. HIPSs are placed between the kernel and the application utility software that sends out requests to the kernel of the Operating System.

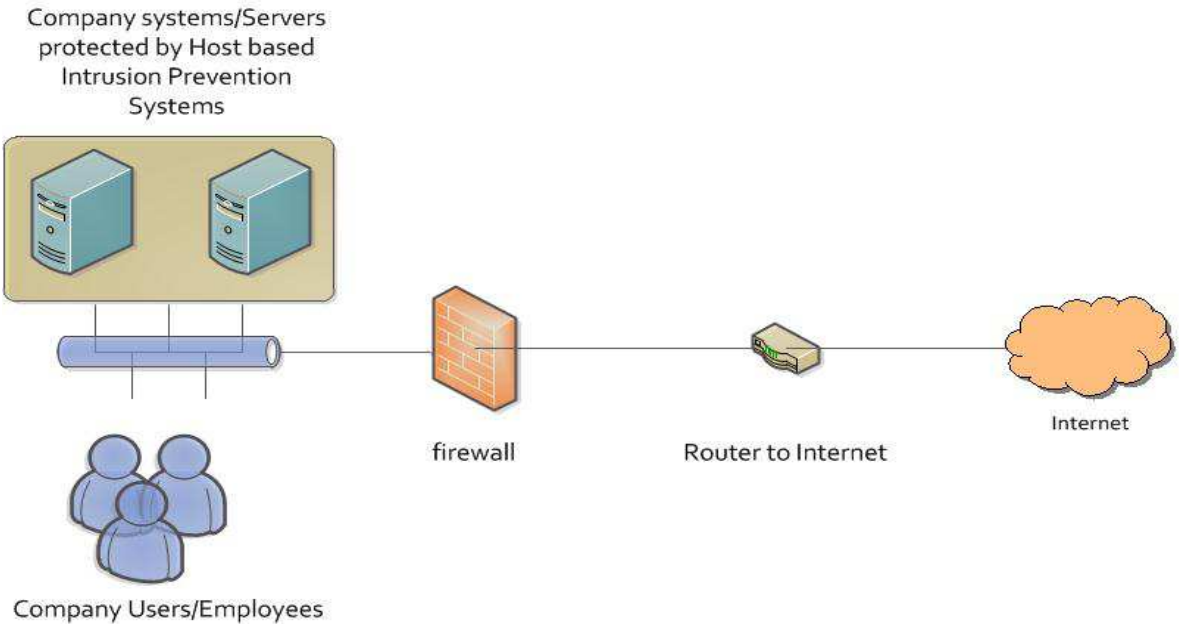

Figure 13: Place of the Host based Intrusion Prevention System

- **Network-based IPSs (NIPSs)**
  NIPSs are built to protect a network. They are placed inline to detect and block malicious attacks. The blocking mechanism is based on analyzing packets on content and matching them against signatures.

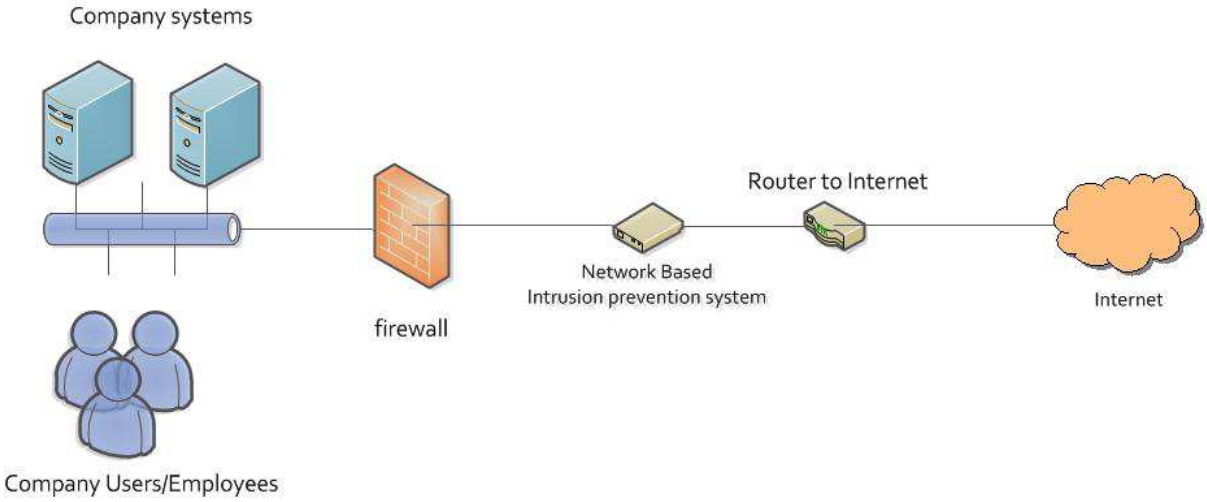

Figure 14: Place of Network Based IPS

3.5.The present and future

Outsourcing business processes and services is nowadays a normal way of procedure to reduce costs (i.e. call centers) and in some cases to improve quality (i.e. software development). The same can be done with information security processes and services. Although the task to secure information is easier in a closed environment, organizations like the benefit or lowering their costs and push off their responsibility towards clients. Outsourcing information security can become as secure as the organization wants. For every security issue there is a solution, only against a price that may not be worth it (Axelrod, 2004).

However, finding the right partner to outsource your information security to is like searching a needle in a haystack. Many of the organizations that handle outsourcing requests are not aware of their own information security status. Therefore outsourcing information security is for a lot of organizations one step too far in maturing their organizations.

Cloud Computing is next to outsourcing an often discussed topic and more future oriented. One of the most challenging parts of Cloud Computing is security. Security in the cloud is considered to be the latest issue in the information security domain. To further address security in the cloud it is first important to know the basics of cloud computing. Gartner (2008) defines cloud computing as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies". This definition already states why security is a difficult part of the cloud. It stores and processes your data externally, is often sourced from other, unnamed providers and contains data of multiple customers (Gartner, 2008).

According to NIST (2010) the Cloud model has five characteristics, three service models and four deployment models. The deployment models are not covered in this thesis since they do not provide added value to the subject of this thesis. The characteristics and the service models are used to explain the concept of the cloud and to make the risks more understandable. The following five characteristics have to be present to speak of a cloud environment:

- On-demand Self-service. A human can provision himself with computing capabilities without human interaction with the service provider.
- Broad Network Access. The cloud is accessible anywhere, anytime.
- Resource pooling. Multiple, different clients are allowed to use the same resources at the same time.
- Rapid Elasticity. The risk of outages is reduced because of the resource pooling. Another effect is that this is the characteristic what makes the cloud beneficial. There is no own infrastructure needed, but according to the resource pooling characteristic you share it with others.
- Measured Service. Resource usage can be monitored. This provides transparency for the client and the provider.

There are three ways cloud capabilities can be provided:

- Software as a Service (SaaS). Software that is available on demand. The applications are often accessible by internet via client devices as a laptop or mobile.
- Platform as a Service (PaaS). PaaS allows customers to develop new applications using APIs deployed and configurable remotely. The platforms offered include development tools, configuration management, and deployment platforms. Examples are Microsoft Azure, Force and Google App engine." (ENISA, 2009)
- Infrastructure as a Service (IaaS). According to NIST IaaS is: "The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)".

Baars & Spruit (2012) identified nine risks concerning cloud computing and the five mentioned characteristics. The last column (cloud specific) mentions whether the risk is cloud specific or not. It if it states partly, then there are new perspectives on these risks.

Risk	Description	Cloud specific
Location awareness	Location awareness, or locationless when no awareness of the physical location of the information systems in use	Yes
Legal/regional	Depending on the physical location of the server, laws and regulations can differ	Partly
Geographic/geo-spatial	Distance between physical systems in place	No
Organizational premises	Are the systems in the cloud environment hosted on organisational premises or not?	No
Network/virtual	Is the cloud environment within the perimeter of the network already in place	Partly
Governance and compliance	Governance and compliance to standards and norms	Partly
Trust chains	The amount of actors involved to serve the subscribed service	Partly
Data loss	Losing data due to the added amount of links and new technologies	Partly
Encryption	Encryption techniques used or new applications for them	Partly

Table 3: Cloud computing risks.

The nine risks mentioned in this table in the end all have to do with information security. Location awareness, for example, decreases when using Cloud Computing as a style of computing. There is no awareness of the physical location of data. Knowing this fact, physical security is of less use and other controls have to be implemented to secure the organizations data.

Considering these risks the question is whether moving to the cloud is a good idea. Cloud computing certainly does provide a couple of advantages why organizations get involved. Main reason is the monetary aspect. Cloud technology is paid incrementally whereby organizations save money (Jamil & Zaki, 2011). Other advantages mentioned by Jami & Zaki are the increased storage, automated environment, flexibility and mobility.

Concluding, the cloud is a new way of providing services to the client in an efficient way. However, not having your information within your own organization makes securing your information a barrier yet to be taken.

4. Maturity Models

Before going further into detail about Maturity Models, it is first important to explain why maturity models suit this research best. The aim of the maturity model is to close the gap between business requirement with respect to information security and the actual level of implementation. Identifying, representing and closing a gap are therefore three main activities that the solution to the research question should comprise. Identification to show the extensiveness of the gap, representing a gap by a comprehensive model and closing the gap by being able to define a roadmap based on the representation. Besides those main goals it is convenient if the answer is useful for the business. The used solution is considered more valuable to the business if it represents the information in a managerial way (e.g. overview, quick to scan, easy to use, based on long term targets), serves as a guideline and because the gap needs to be measured, the solution also needs to be established based on the results of metrics. As a last criterion, business is most likely to be committed to their strategic and tactical plans and therefore the model should be able to reflect these plans.

Besides these six main criteria, there are some alternatives that might be able to suit these six criteria. For this thesis the following four options appeared of value:

- Gap Analysis
- Dashboard
- Maturity Model
- List of metrics

These six main criteria and the four alternatives are listed in the table below. During the analysis of the four different alternatives, the maturity model came out best. Besides the ability to identify and close a gap, the solution also provides guidance and is represented in a structured way suited for the support of management.

	Gap analysis	Dashboard	Maturity model	List of metrics
Defining metrics	A Gap analysis does not necessarily define metrics. Since defining metrics for information security is one of the sub goals of this research gap analysis alone might not be a good solution.	To make a proper dashboard, metrics are needed. The results of the metrics are represented on the dashboard. Dashboards are mostly used for representing KPIs .	Metrics are needed to determine the level of maturity. All kinds of metrics can be presented in a maturity model	This is a good solution for defining metrics.
Identifying a gap	Gap analysis is good in identifying a gap.	A dashboard only measures the as-is situation and is therefore not able to identify a gap.	A maturity model, when presented to different roles in the organization, can lead to different results which indicate a gap.	A list of metrics, when presented to different roles in the organization, can lead to different results which indicate a gap.

Closing a gap	Gap analysis does not suggest any solutions to the gap.	A dashboard does not identify a gap and is therefore also not able to close it.	The results from the gap identification can be used to close the gap and increase corporate knowledge.	The results from the gap identification can be used to close the gap and increase corporate knowledge.
Managerial representation (representing a gap)	Gap analysis does provide value to the business but does not provide a solution to the business.	A dashboard helps a manager get a quick overview of what is going on.	A maturity model gives an overview of where an organization is and where it should be going in a structured way.	A list of metrics is not supporting a manager in efficiently doing his tasks.
Strategic/ tactical Value	Gap analysis can be of strategic value when talking about a gap between what a customer wants and what is already there. This gap is almost the same as in my case (only internal).	A dashboard can help setting up tactical or strategic goals when targets are included on the dashboard.	A maturity model helps in determining the next steps in becoming mature.	A list of metrics is not suggesting or presenting any tactical or strategic advantages. It represents the as-is situation.
Guideline	A gap analysis does not tell you what to do in the next years.	A dashboard does not guide an organization; it only shows what is going right and wrong.	A maturity model shows the best practice of what to do next to the benefit of the organization.	A list of metrics has a limited guidance. It can show bad results but does not relate them to other metrics.

Table 4: Comparison possible research models.

The other three possible solutions (top row) are gap analysis, building a dashboard and providing a list of metrics. Gap analysis is well suited for analyzing a gap. However, there is no managerial idea behind the analysis. Gap analysis identifies the problem, but does not provide assistance on how to solve it. Since this is a vital part of the thesis, this option is not selected for this problem. Building a dashboard is more management oriented and is able to represent metrics in a structured way. Disadvantage of a dashboard is that it only shows information of the as-is situation and does not provide information about the to-be situation nor does it show a way to get there. Although a dashboard is a good management tool and can help identifying a gap, it is not capable of solving the problem central to this thesis. The last option is making a list of metrics. This alternative does not solve the complete research question because it lacks in representation. A list of metrics basically could do the same as a maturity model; it only misses the structure and the guidance. Whereas a maturity model could identify the focus areas of information securities that are underdeveloped, a list of all the metrics does not make this division and makes it therefore less suitable.

Richard Nolan (1973) was the first researcher who thought of maturity models. Already back in in July 1973 he wrote an article about it named: "*Managing the computer resource: a stage hypothesis".* Maturity models, since then, have been and are still an often used artifact to support the incremental improvement of functional domains in information system research. (Bruin, Freeze, Kulkarni and Rosemann, 2005, Mettler and Rohner 2009).

Steenbergen, Bos, Brinkkemper, Weerd and Bekkers (2010) state that maturity indicates the degree of development.

Maturity model:
"Maturity models or matrices provide an ordering of capabilities within a functional domain across focus areas over a sequence of maturity levels" (Steenbergen et al, 2010)

In this definition of maturity models, maturity levels can be defined as

Maturity level:
"A well-defined evolutionary plateau within a Functional Domain (Steenbergen et al, 2010)"

4.1. Staged 5-level model

The staged 5-level model is known for having five fixed maturity stages. An example of this model is the Capability Maturity Model (CMM) (CMMI, 2002). Each level has a number of requirements specified to a certain maturity level. An organization raises their maturity level if they fulfill all requirements on that specific level.

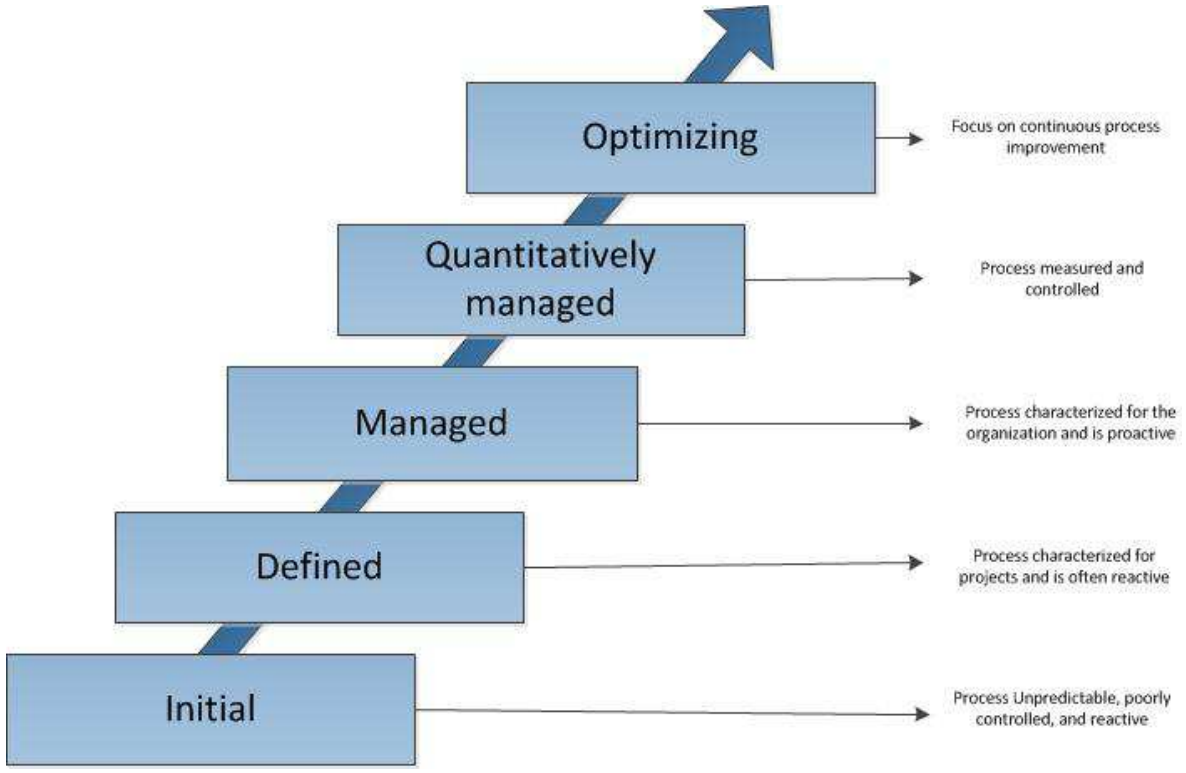

Figure 15: Staged 5-level model. (CMM)

As can be seen in figure 15 the staged five level maturity model exists of an initial, repeatable, defined, managed and optimizing level. Those five stages are generally used to define maturity for a certain domain.

4.2. Continuous 5-level model

The continuous 5-level model also distinguishes domains and five stages of maturity. The difference with the staged variant is that the continuous 5-level model defines five stages for every process area instead of defining actions which relate to a process area for every maturity level (staged maturity model). Examples of those models can be found in papers of Appel, (2000), METAgroup (2001), NASCIO (2003) and Westbrock (2004).

Category	Process Area Including IPPD
Process Management	Organizational Process Focus Organizational Process Definition + IPPD (SG 2) Organizational Training Organizational Process Performance Organizational Innovation and Deployment
Project Management	Project Planning Project Monitoring and Control Supplier Agreement Management Integrated Project Management + IPPD (SG 3) Risk Management Quantitative Project Management
Engineering	Requirements Management Requirements Development Technical Solution Product Integration Verification Validation
Support	Configuration Management Process and Product Quality Assurance Measurement and Analysis Decision Analysis and Resolution Causal Analysis and Resolution

Table 5: Continuous 5-level model (CMM)

Table 5 shows a continuous representation of the CMM. The model focuses on four capabilities instead of maturity levels covering the entire organization. The capabilities are represented by the column categories and for every category process areas have been defined. Every process area consists of 5 stages of maturity. In this way, improvements can be characterized relative to an individual process area instead of to the entire organization.

4.3. Focus Area Maturity Model

The last variant is the focus area maturity model. This model uses the same concept as the continuous 5-level model without the fixed amount of maturity levels. The model allows having three maturity levels for a focus area, but also seven could be possible. Therefore, this option gives the most options to customize the maturity model to your own wishes. This maturity model is proposed by Koomen and Pol (1999). An example can be found below in figure 16. The example is from a study on the field of Software Product Management by Bekkers and Van de Weerd (2010).

Orginally the lay-out for this model is derived from the field of IT Architecture. Before explaining the advantages of a focus area maturity model it is important to explain what a focus area exactly is.

The first part of the research defines the focus areas of information security. A focus area is:

Focus area:
"a well-defined coherent disjoint subset within a functional domain. The total set of focus areas covers the complete functional domain." (Steenbergen et al, 2010)

Maier, Moultrie, and Clarkson (2009) use the term process area instead of focus area although they represent the same. Moultrie (2007) mentions that interviews and an explorative literature study may be selected as methods to define the focus areas. The focus areas related to information security are placed in the left column of the maturity matrix marked by the blue color in table 6. All

	1	2	3	4	5	6	7	8	9
Focus area 1									
Focus area 2									
Focus area …									
Focus area …									
Focus area n									

focus areas together represent the domain of information security. The list of focus areas is identified and defined in chapter 5.

Table 6: The layout of a focus area maturity model

Advantage of this type of maturity model is that capabilities can be related and ranked based on the importance of implementation. Whereas A's are the most basic and important steps an organization can take within a certain focus area and the letters closest to Z represent the final steps to become fully mature within that focus area. In figure 16 are the focus areas on the left side, the maturity levels on top and in the matrix itself are the letters that represent capabilities that have to be reached in order to reach the corresponding maturity level. With every letter there are a couple of metrics that need to reach a certain value in order to fulfill the requirements for that maturity level.

	0	1	2	3	4	5	6	7	8	9	10
Requirements management											
Requirements gathering		A		B	C		D	E	F		
Requirements identification			A			B		C			D
Requirements organizing				A		B		C			
Release planning											
Requirements prioritization			A		B	C	D			E	
Release definition			A	B	C				D		E
Release definition validation					A			B		C	
Scope change management				A		B		C		D	
Build validation					A			B		C	
Launch preparation		A		B		C	D		E		F
Product planning											
Roadmap intelligence				A		B	C		D	E	
Core asset roadmapping					A		B		C		D
Product roadmapping			A	B			C	D		E	
Portfolio management											
Market analysis					A		B	C	D		E
Partnering & contracting						A	B		C	D	E
Product lifecycle management					A	B			C	D	E

Figure 16: Software Product Management Maturity Matrix as proposed by Bekkers, Van de Weerd, Spruit & Brinkkemper(2010)

The focus area maturity model is used for this thesis. It can represent and interrelate most of the aspects of Information security. This is a huge advantage for this study, especially because the goal is to provide business with a tool for improving their Information security stepwise. With this model, an organization is able to define a road map for their information security. Most likely this is done by IT and Business together to know for sure that the gap between the assessed Information security and the business security requirements is closed or at least as small as possible. More about focus area maturity models is explained in chapter 5. The initial ISFAM model is discussed in chapter 6.

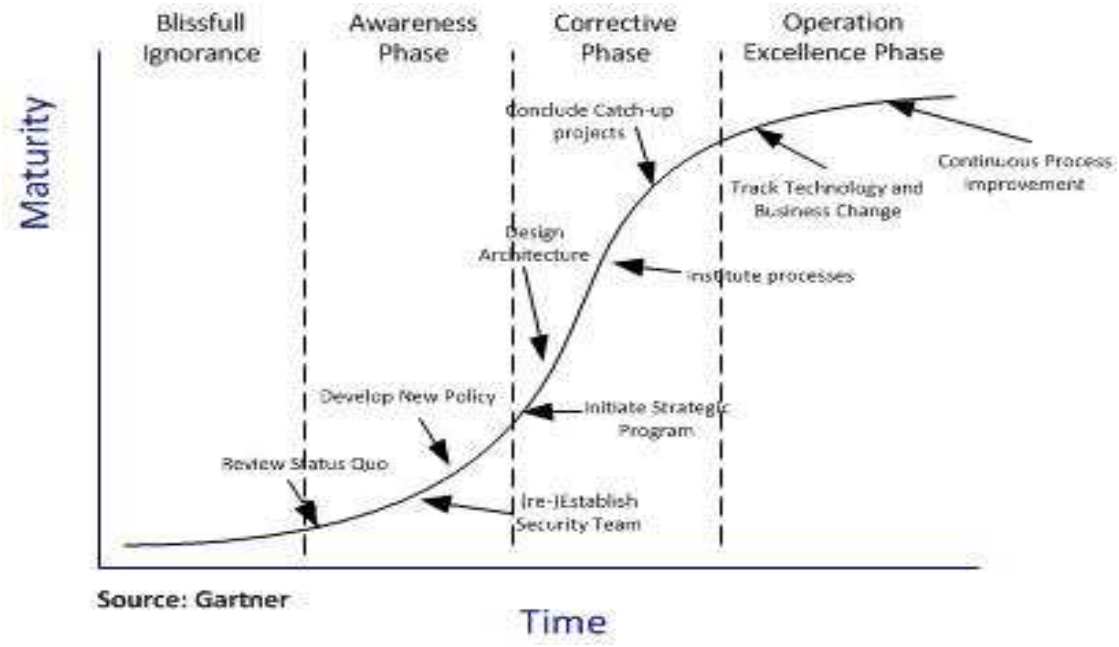

Figure 17: The Security Maturity Model

One of the many maturity models addresses Security (see figure 17). This model was published by Gartner in 2005 and defines four stages in time. The goal is to reach the operational excellence phase where the maturity reaches its maximum level. The security maturity model can be classified

as a staged maturity model. Although it looks continuous, it only defines four stages of maturity in which the actions need to take place in order to improve the maturity. There are no distinct maturity levels per focus area and therefore it is mostly a staged maturity model. Blissful ignorance is the first phase and indicates that almost nothing is done about security. When entering the awareness phase employees within an organization become more and more aware of what security is and how they should deal with it. In this phase it is important to develop new policies and to establish a security team. Further on the organization reaches the corrective phase where processes are standardized and projects are executed. The operations excellence phase is then the last phase. This phase is about optimizing the processes of integrating security into the organization continuously.

5. Focus Areas and their maturity

The purpose of this thesis is to make a Focus Area Maturity model as has been mentioned in the previous chapter. There are a couple of steps involved in making a Focus Area Maturity Model. First, the focus areas need to be defined. After, the next step is to take a closer look at them en define a maturity scale for each focus area. The maturity scale of each focus area can be compared with a staged model not necessarily bound to the usage of five stages. Hence, a focus area is allowed to have more or less maturity levels in this model. In the next chapter, the focus areas are discussed one by one. Every section has the same structure:

- *Introduction to the focus area and explanation why it is important to information security:* The development of the maturity models for every focus areas starts in every section with a general overview of the focus area. It explains what the focus area entails and why it is a focus area for the final model.
- *Defining maturity scales for the focus area:* The second part of a section elaborates on the maturity models available in literature and if necessary combines various models to one model usable for the final model. If no applicable maturity model can be found, the maturity model is created using the stages of CMM.
- *The capabilities that determine the maturity level:* Keeping the stages of the second part into account, the third part defines metrics related to these stages. Initially the metrics are derived from literature. These metrics can either be of an already existing model in this literature or the metrics is defined using important factors of a focus area mentioned in the different references. The maturity model defined in the third part of every section represents the final version after evaluation by an expert. The maturity models consist of capabilities and within these capabilities (i.e. A, B, C, D, E) the metrics are defined. For every capability in a maturity model the same rules apply. These rules are:
    - Every metric/statement within a capability has to be answered with yes before the entire capability is marked as completed. E.g. if not all statements for capability A have been answered with yes, capability B can never be reached.
    - Statements can be left out of the model if not applicable to your organization, but is not recommended. Leaving one statement out can affect the dependencies in the entire model. If a statement is not applicable it is better to answer the statement with yes and keep that in mind.
    - Statements might exclude the applicability of other statements. i.e. one statement entails that something is driven by IT and the next statement is about something driven by business. In this case, the maturity model has 'OR' at the end of a statement with the conflicting statement behind it. An example can be found in the Business Continuity maturity model. Statement A1 conflicts with B1.
- Evaluation of the focus area maturity model by an expert: The evaluation of the maturity models is detailed in the last section where a semi-structured interview with experts can be found. The experts had to answer at least four questions:
    - Do you think x stages of maturity adequately represent this focus area? (where x is the amount of stages initially proposed in the model)
    - Do you think that there are some statements superfluous or do you miss some statements applicable to this focus area?

- Are the statements well distributed over the capabilities or would you consider replacing statements to a different capability?
- Are there any other comments?

Besides these four questions, the discussion was open to give additional information from the business and explain concepts that relate to the focus area. In total there were 13 interviews held (1 for each focus area) with 11 different persons. At the end of every evaluation section an overview is given covering the most important changes.

Expert Number	Topic(s)	Experience	Industry/job
1	Risk Management Compliance	> 3 years	Finance/oil
2	Policy development	> 3 years	Finance/oil
3	Organization of information security	> 5 years	Security management/ various industries
4	Asset Management	> 5 years	Security management/ various industries
5	HR Security	> 10 years	Consultancy security manager
6	Physical & Environmental	> 3 years	Social Engineering in various industries
7	Change Management	> 1 year	Audit in several industries
8	Identity and access management	> 5 years	Telecom, Media & Technology
9	Software Development	> 3 years	Finance
10	Incident Management Business Continuity management	> 10 years	All Industries
11	Information Security Architecture	> 5 years	Finance

Table 7: Overview of experts

The ISFAM model consists of 13 focus areas. 12 of these focus areas are translated from the ISO27K series. The additional area is Architecture. Reason for this addition is the CISSP course and the Standard of Good Practice who both handle this area separately. CISSP is, as already elaborated on in the literature study, a course in the field of information security. Architecture is one of the ten areas. The Standard of Good Practice of the Information Security Forum (ISF) defines a lot more areas than the list shown in the table below. However, most of them can be combined and have overlap with other areas. The last six areas in table 8 are not used as focus area for the ISFAM model for the same reason. They are part of another focus area and/or overlapping. For keeping the maturity model easy to use and understandable they are combined with the other focus areas. One exception out of these six is privacy. Privacy is often associated with security, but for this thesis privacy is not handled as part of security but as a concept that exists next to security.

Other frameworks used to identify information security focus areas are the information security framework, which is based on the ISO27K standard, and the IBM framework. After studying the information security framework it became clear that this framework is a simplified version of the ISO27K and does not provide additional value to the definition of the final focus areas. The IBM framework is interesting because of the practical focus. This framework is internally developed and based on IBM's experiences. However, it only addresses a few focus areas and is not specifically

made for information security but for information security problems they encountered during their work. After studying the frameworks and the CISSP course the following 13 focus areas (shown in table 8) have been identified for the final ISFAM model. The combination of the maturity of every single focus area determines the overall information security maturity of the organization.

	CISSP	ISO 2700x	Information security framework (Based on ISO)	Standard of Good practice (ISF)	IBM Security framework	**Roeling 2012**
Risk Management	x	x	x	x		**Area 1**
Policy, Laws & Standards	x	x	x	x		**Area 2**
Organization	x	x	x	x		**Area 3**
Asset Management		x	x	x		**Area 4**
HR Security		x	x	x	X	**Area 5**
Physical & Environmental	x	x	x	x	X	**Area 6**
Change Management	x	Communications & operations Management	x	x		**Area 7**
Identity and access management	x	x	x	x	X	**Area 8**
Software development	x	x	x	x	X	**Area 9**
Incident Management	x (disaster recovery)	x	x	x	X	**Area 10**
Business Continuity	x	x	x	x		**Area 11**
Compliance	x	x	x	x		**Area 12**
Architecture	x (+ design)			x		**Area 13**
Malicious Attacks (prevention)		partly		x		Part of other areas
Cryptography	x	tool		x		Part of malicious attacks
Telecommunications & Network security	x	x	x	x		Part of architecture
Governance	x	organization	organization	x	X	Part of organization
Privacy				x	X	
Transaction and data integrity				x	X	Part of other areas

Table 8: Information security focus areas

5.1.Information security risk management

A key concept related to an information security framework or model is risk management (Bodin, Gordon and Loeb, 2008). An organization cannot make their information perfectly secure all the time, but is able to manage risks. Risk management is a vital part of identifying potential breaches and preventing data from being lost and therefore a focus area in this thesis. To indicate the importance of risk management the CISSP forum and ISO27K implementer's forum started a project to identify the top information security risks. "*Top information security in risks for 2008"* (CISSP and ISO27k, 2007) is the deliverable produced by the experts. To discuss all these risks is outside the scope and is therefore not elaborated on. Blakley, McDermott and Geer (2001) define business risk as

Business Risk:
"The possibility of an event which would reduce the value of the business were it to occur. Such event is called an "adverse event"."

Possibility in this definition is mostly referred to as a number between 0 and 1 where 0 is no chance of occurrence and 1 is completely sure the risk will occur. Risk can be managed in many different ways. One often is used is liability transfer. Liability transfer is paying another organization for taking the responsibility of an adverse event (Blakley et al, 2001). This type of risk management is not interesting for the rest of this thesis, because an organization needs to become more mature in risk management and transferring risks is not part of risk management. When outsourcing risks to a third party, you rely on their risk management process. This can be good solution, but does not tell something about the organization's risk level. The other three options are more interesting:

- Indemnification: The organization tries to avoid the costs of a possible adverse event. This might be done through splitting the costs of such an event over all business units (pooling) or by making a betting system where business units and organizations can bet money on whether an adverse event will occur or not (hedging).
- Mitigation: The organization tries to reduce the chance of an event occurring or the consequences the event has. If an organization spends thousand dollars to reduce the chance of a risk that will cost a million it is called mitigation.
- Retention: An organization can also retain the risk and accept it. This might be the case when a risk is not very likely to happen or does not affect the business in a negative way. Positive effects play a significant role in deciding whether to retain a risk or not.

Information security risk management should be applied to all aspects of how information is created, processed, stored and disposed (Broderick, 2001). This is done by the lifecycle pictured in figure 18. First thing to be noticed is that this lifecycle is continuous. In the most mature organization policies and controls to reduce risk are always revised and re-implemented. From that point onwards, the lifecycle follows the arrows in figure 18 again.

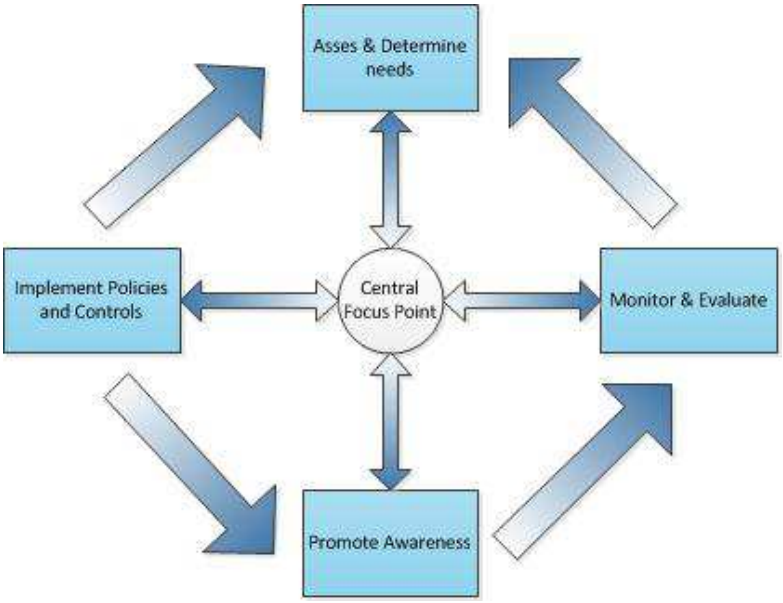

Figure 18: Risk Management Lifecycle (Broderick, 2001)

For every cycle there are new requirements. When starting with information security risk management the implemented policies might be very basic and the steps taken to promote awareness and determine the needs might be high level. When performing this cycle again, the requirement and expectations are improved and other aspects become thereby also more in-depth.

Risk Management, besides being part of the ISO27k standard, is also a standard itself. ISO/FDIS 31000 (ISO, 2009) is the international standard for risk management. The standard helps making risk management as effective and efficient as possible for an organization.

5.1.1. Risk management maturity

Hillson (1997) made a four staged maturity model for risk management called the Risk Maturity Model (RMM). Four stages provide an unambiguous way of measuring an organizations risk maturity. Most organizations fit in this amount of maturity level. Because of this fact, RMM is used as maturity model for the risk management focus area.

Maturity level	Explanation
0- None	Risk is not managed and not though about before starting a project.
A- Naïve	At this level the organization reacts on adverse events. They do not have a structured approach in handling risk and uncertainty and do not learn from past events.
B- Novice	At the novice maturity level the organization knows that risk management has benefits but does not give full attention to it. Organizations appoint individuals to cope with unexpected events.
C- Normalized	Risk management is formalized and most/all projects are using the formalized approach of risk management as defined by the organization. It does not necessarily mean that the business gains benefit in every situation.
D- Natural	Risk management is used to control opportunities as well as negative effects. Risk management processes are used to gain competitive advantage and are well-known by the entire organization.

Table 9: Risk Maturity Model stages

Another model is the Risk Management Capability Maturity Model (Yeo and Ren, 2008). This model was not suitable because the model is focused on Complex Product Systems projects. These projects do not have a relation to information security. Other maturity models with respect to information security risk management, or risk management in general, have a comparable focus to the Risk Management Capability Maturity Model or have a broader scope then necessary. Useful metrics found in the unused maturity models are used to strengthen the maturity model of Hillson.

5.1.2. Risk management maturity metrics

To determine the risk management maturity level the statements in table 10 are used.

Capability /level	Statements	Reference(s)
A	1. The organization has an informal risk management program, OR B1, C1, D1. 2. Individuals in the organization are aware of the importance of risk management, OR B3, C3. 3. Risk Management is supported by individuals within the organization, OR B4.	Hulett 2001
B	1. The organization has defined a risk management program on a strategic level, OR C1, D1. 2. Someone has been made formally responsible for risk management, OR C2. 3. The organization is aware of the importance of risk management, OR D2. 4. Risk management is supported by proactive management that allocates sufficient resources for it.	Hulett 2001
C	1. The organization has defined a detailed risk management program based on a standard, OR D1. 2. Risk management roles have been defined organization wide. 3. The organization measures their risk management level with defined metrics. 4. Risk management processes are formalized	Hulett 2001
D	1. The organization has defined a risk management program involving their customers and suppliers 2. The organization is maintaining their risk management awareness level. 3. Risk management processes are continuously improved. 4. Risk management is an integral part of the decision making process.	Hulett 2001

Table 10: ISFAM assessment statements for information security risk management

5.1.3. Evaluation

To evaluate the initially proposed statements based on risk management literature, an expert having several years of experience in risk management evaluated this model. Since he worked for a large oil company and now works for a financial institution, he is known with a large variety of risks. I explained the purpose of the final model and why risk management is part of the model. Explaining the model, he saw that level 0 was included in capability A and that some of the statements had to be removed: Roles are not defined, there is no risk management training given and the organization has no metrics in place to measure their risk management level. Inherent to this change is the

change of the amount of levels included in this model. Since three statements are dropped at the first level, a closer look was taken at the other levels to see whether they could be replaced to be left with three levels. At the end, we decided that four levels would be better than 3 to cover risk management in a more detailed manner.

The original statements considering training and awareness at capability B can be combined into one new statement: The organization is aware of the importance of risk management. Training is thereby removed from the model, because training is a way to increase the awareness and not a goal in itself. At capability C the statement considering training is for the same reason also removed. Capability D stated that "employees should receive refresh trainings". However, this also has to do with maintaining the risk management awareness level of an organization and therefore a choice had to be made to put the statement of maintaining risk management awareness in capability C or D. Referring back to the previous paragraph where the amount of maturity levels were discussed and the maturity model in chapter 5.1.1 it was decided to place it at capability D.

At capability D, he suggested a small change. The last statement has been changed from: Risk Management is involved in every decision made into Risk Management is an integral part of the decision making process. Risk Management is even in the most mature organization not used in every decision. A simple example is the decision whether you take coffee or tea in the morning. It is a decision, but no one uses Risk Management for that.

Action	Result
Remove	Roles are not defined There is no risk management training given The organization has no metrics in place to measure their risk management level
Change	Combining two statements (training & awareness) to one new statement: The organization is aware of risk management
Remove	Training statement in capability C
Remove	Refresh training at capability D
Add	Awareness statement at capability D
Change	Risk management is involved in very decision made has been changed to risk management is an integral part of the decision making process

Table 11: Overview of changes risk management

5.2.Policy development

The foundation for information security within an organization is the information security policy. The security policy document is the most important document considering information security. It provides the directions an organization should follow regarding information security. The document defines two aspects important to the development of a good policy (Höne & Eloff, 2002):

1. Management's commitment to and support of information security.
2. The role of information security in reaching and supporting the organization's mission and vision.

Creating this document is often seen as the hardest part of information security. Organizations have difficulties with how it should look like, how many pages it should count, and so forth. These difficulties often result in "copy paste" policies constructed from examples found on the internet. Information security policies, however, require a different approach in each organization and should

not be copy pasted from examples on the internet. Using standards is not the same as copy pasting and a better way of dealing with this problem. When making a policy, one should always take into account the goals/purpose of the policy. In case of an information security policy the next seven points are indicated as goals (SANS, 2007):

- Protect people and information
- Set the rules for expected behavior by users, system administrators, management, and security personnel
- Authorize security personnel to monitor, probe, and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation.

If an information security policy is made with these seven points as a basis, the document reveals what information security areas need attention. In other words, in what an organization is doing great and in what areas it is performing below average or worse.

5.2.1. Information security policy maturity

Writing and developing an information security policy should be a continuous process within an organization. Wood (2011) has 30 years of experience in the field of security policies within more than 110 organizations as a consultant, especially the financial and high-tech sector. He suggests three stages of maturity, excluding the zero stage. At the zero stage there are no roles defined and there are no security policy documents. Improving from the zero stage to the maximum level (3th stage), employees get roles, an Information Security Officer is designated and security policy documents are created and reviewed on a regular basis probably based on a standard.

The first stage Wood mentions is an ad-hoc stage. The organization has a document in place primarily focused on Internet Acceptable Use. This document states what is allowed and what is not allowed to be done on the internet (i.e. playing computer games, personal use, etc.). Other documents that are part of the document at this stage are reporting documents. If an unwanted situation occurs within the security of their systems, they may report this. This report includes the incident and the person to whom it is directed. These documents are in many cases made because management wants them. They do not have a clear purpose because management does not identify why they need the documents. Result is the copying of existing policies or examples of policies to finish it quickly. The policy is thereby not specific to the companies' situation and may contain several mistakes (i.e. references to other places in the document that do not exist).

At the second stage, the organization becomes more mature by really thinking about their information security policy. Typically, organizations at this stage have a data classification policy, defined their information security architecture, the document of that architecture, and have formed teams for different parts of information security like incident handling.

At the last stage, the organization is expected to have a document management system for their policies. The policy document is viewed as a dynamic document and should be updated over time. All roles have been defined, standard frameworks are used and the documentation is done in the same style. Besides the look and feel of the document, the document also goes further in depth on

automated controls as encryption. Every information security measurement and implementation is likely to be included in the information security policy. It is recommended to let an auditor check the validity, accuracy and relevancy of the document on a regular basis (e.g. half a year is a best practice).

The three maturity steps described differ from organization to organization. Hence, a small organization might not need a disaster recovery plan in their policy and could therefore decide not to include it. Overall problem of an information security policy is that it needs to be understandable for every person within the organization and not only in terms of words but also in terms of usability. The question why they want a certain person in their organization to follow a certain policy should be clear to that person and the alignment between restrictions and workability needs to be taken into account. Nonetheless, this division in three maturity stages gives a general basis that can be used in organizations as a guideline.

Maturity level	Description
0- Not defined	The organization is not aware of laws and regulations that cover their organization.
A- Ad hoc	The organization's information security policy document is made ad-hoc and often consists of policies found on the internet. The organization is familiar with laws and regulations.
B- Defined	The organization has some organization specific information security policies in place, but the policies are not fully integrated into the organization. The high level policies are well defined, but operational policies are not yet or ill defined.
C- Developed	The organization has an integrated, in detail described information security policy document in place. The development of the information security policy document is seen as a continuous process supported by reviews.

Table 12: Information Security policy maturity model

5.2.2. Information security policy maturity metrics

The policy development maturity is measured by metrics gained from literature. The following table states these and explains to which maturity level they belong.

Capability/ level	Statements	Reference(s)
A	1. Laws and regulations are part of the information security policy 2. Information security policy development is supported by management	Höne & Eloff (2002), Wood (2011), SANS (2007)
B	1. Every policy addresses at least the following: • Introduction • Purpose • Scope • Roles and responsibilities • Sanctions and violations • Revisions and Updating schedule • Contact information • Definitions/glossary • Acronyms 2. Policies are set up taking into account the	SANS (2007), Höne & Eloff (2002), Wood (2011)

	organization's culture and strategy 3. All roles and responsibilities regarding information security are defined 4. There is a formal style for writing information security policy documents	
C	1. The policy documents are reviewed on a regular (e.g. 6 month) basis 2. The policy documents are understood by the whole organization 3. The policies are based on standards (ISO2700x, ISF's standard of good practice, etc.) 4. Information Security policy documents are maintained in a document management system	Höne & Eloff (2002), Wood (2011), British Standard institute (2005)

Table 13: ISFAM assessment statements for information security policy development

5.2.3. Evaluation

To evaluate the initially proposed statements based on literature, I spoke to an expert of Deloitte. With over three years of experience in policies he knows how policies are written and what is seen as most important within companies. He suggested putting an accent on three different policy levels: strategic, tactical and operational. Strategic is on a high level, defined by management. One level lower is tactical. Tactical policies are more on an organizational level and define the differences between business units. Operational is how individuals look at the policies and how they are included in the policies. This is done by going more and more in depth each maturity level. Another remark on the initial conceptual maturity model was the use of compliance to laws and standards. Compliance is something else then policy development and therefore organizations should take into account and be aware of the laws and standards at capability A but not necessarily compliant. Although it might sound incorrect to not have policies in place that comply with the laws and regulations, it is still possible and an organization can be unaware of the laws and regulations. This does not implicate that they do not have an immature policy in place. The policy might still be well developed for the whole organization on each of the three levels. That they do not comply with the laws and regulations should be part of the compliance focus area. Furthermore he confirmed the stages of maturity as mentioned in this chapter and said that what is stated here happens in practice, exceptions excluded (i.e. part of an organization has no policy in place or the company builds his own standard instead of re-using an existing standard.

Action	Result
Remove	Compliance related statements

Table 14: Overview of changes policy development

5.3.Organization of information security

Management plays an essential role in establishing a solid information security program. Organizing information security is not only about your own business, but about the whole value chain. Confidential information travelling from point A to B should also be threatened as confidential if it moves to point C afterwards. Pfleeger (2007) stated in *Managing Organizational Security* that key similarities exist between several companies when talking about organizing information security. Most of the organizations divide information security tasks over different business units. Reporting happens in most cases to the CIO, being it indirectly through an IT executive or directly. However,

not one way of organizing your information security is proved to be best. Therefore, this focus area is looked upon from a general point of view. E.g. who reports to who is not important but the fact that someone is reporting to management level or the board does make a difference in maturity. A large part of the organization of information security is the assignment of roles and responsibilities. How these are defined differs per organization dependent mostly on their size. Really small organizations for example don't have one person full time on managing information security. In those organizations, information security might be part of the IT-manager or might not even be part of the organization at all. Large organizations have multiple FTE's on information security. A Chief Information Security Officer (CISO) and Information Security Officers are a commonality in such organizations. In case of a large organization it is as well usual to report upstream to the CIO or someone similar to a risk committee. Since these do not exist in a small organization, reporting does not happen or is oriented directly towards the CEO.

5.3.1. Organization of information security maturity

Organizing information security in an organization consists of different parts. It all starts with management commitment. If management is not committed to necessary changes or the whole program, information security remains a concept known by few in the organization and applied by even less. Even more, it is applied by an individual for his/her own benefit. Management, in this, should play the role of initiator. Other aspects that influence the maturity of organizing information security are the assignment of roles, the assignment of coordinators, and authorization process for new information security initiatives and how to deal with external contacts.

Maturity level	Description
0- Not defined	Information security is not organized within the organization
A- Management awareness	Management wants to improve their information security and makes resources available.
B- Structured	Managements defines roles and responsibilities to get information security more structured throughout the organization
C- Pro-active	The organization takes other practices into account and gets involved into special interest groups to gain knowledge
D- Optimizing	The organization is part of special interest groups to share knowledge. Their organization concerning information security is updated and reviewed on a regular basis and external parties are taken into account for that.

Table 15: Organizing information security Maturity

5.3.2. Information Security Organization maturity metrics

It is hard to measure the maturity of organizing information security. However, there are some objectives that can be met or thought about if you want to organize information security throughout your organization. Level 0 is not depicted in this table, because any organization starts at this level. It does not require any action for an organization to be level 0.

Capability/ level	Statements	Reference(s)
A	1. There is senior management commitment to information security 2. Management makes sufficient resources available to address information security 3. Management is formally responsible for all policies	British Standard institute, 2005

B	1. Information security aspects are coordinated throughout the organization 2. Information security roles and responsibilities have been defined on a high level 3. All employees have signed a confidentiality agreement	British Standard institute, 2005
C	1. There is an authorization process for information processing in place (from inside to outside the organization) 2. There is contact with authorities about laws and regulations 3. The organization gains knowledge by passively participating in special interest groups	British Standard institute, 2005
D	1. The organization gains knowledge on information security by actively participating (e.g. also sharing information) in special interest groups 2. The organization's information security status is reviewed on a regular basis 3. Risks related to external parties are identified and regularly updated	British Standard institute, 2005

Table 16: ISFAM assessment statements for Information Security Organization

5.3.3. Evaluation

To evaluate the initially proposed statements based on literature, I spoke with an employee working for a big oil company. With over three years of experience in developing and maintaining policies related to information security he has enough knowledge to evaluate the maturity model for organizing information security.

During the conversation three questions were asked. In the first part of the conversation we discussed whether this maturity model consists of the right amount of maturity levels. Since I only showed the maturity model containing the statements, his first remark was that is looked like the CMM standard model without the initial level. I explained that at the initial level nothing is in place and that therefore there was no use of including the initial phase in the maturity model with statements. He agreed upon that and we moved on to the second question: *Are any controls/*statements *important to this maturity model missing?* At first sight he said that there might be something missing. He mentioned thereby the policies. Since policy development is already a focus area, I explained him why this is not included in the model. However, a policy also needs to have an owner. A real important aspect, apart from all other roles and responsibilities, is that management is owner of the information security policy. He suggested reading the requirements of security governance in the CISM (Certified Information System Manager) documentation to get some other insights that can be included in the model. This review led to the inclusion of a separate role for management that should own the information security policy. Other topics were too specific for this maturity model or were already included in other statements.

Action	Result
Add	Management is formally responsible for all policies

Table 17: Overview of changes information security organization

5.4.Asset Management

For organizations it is important to keep important information inside to avoid sabotage, fraud and espionage. The purpose of Asset Management in general is to protect assets from falling into the wrong hands. Information assets are objects holding information useful for the business. This could be a computer, a hard disk, but also an employee. Since asset management has a different meaning in every sector and business unit, the following definition is only applicable for this thesis. For the same reason, a new definition for Information Asset Management is proposed. Information Asset Management in this thesis is defined as:

Asset Management:
"The process of guiding an information asset during its lifecycle in order to gain maximum benefit from the asset"

The focus area Asset Management deals with protecting information from inside as well as outside threats. In the ISO27k series there is no distinction made in physical or logical security. Physical assets are computers, papers, etc. Logical assets are files, passwords, usernames on computers, etc. Both physical and logical are involved in this focus area.

The lifecycle of an information asset is a process of three phases (Ouertani, Parlikad and Mcfarlane, 2008). Beginning of Life (BOL) is the specification, design and creation of the information asset. Middle-of-life (MOL) is the phase where the information asset is used, maintained and provides the intended services it is created for and End-of-Life (EOL) is the disposal or storage of the asset when it is not needed anymore.

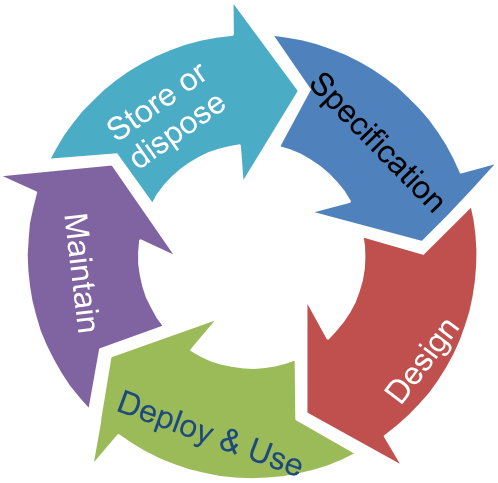

Figure 19: Asset Management Lifecycle

5.4.1. Asset Management Maturity

Since little literature is available on the field on Asset Management and Information Asset Management there is also little scientific information available about the maturity of this focus area. Websites from companies and blogs in combination with the CMM standard for defining maturity models are used to propose an Asset Management Maturity model. A CMM maturity model consists of five stages:

- Initial is a chaotic, non-structured level where problems are solved when they occur
- repeatable is the level where organizations start to re-use the information of previous events

- Defined is the level where processes get standardized
- Managed is the level where the process quality gets measured and therefore can be improved
- Optimized is the level where the continuous improvement is the key word. New technologies are used to stimulate business.

One maturity model in the field of Asset Management Maturity is made by an organization called Oarisk. This English organization provides Operational Asset and Risk solutions. The model (Oarisk, 2010) is used a basis for the focus area maturity model of this thesis. The model as described by Oarisk is more detailed than needed for this thesis. The original model consisting of five stages and twelve areas ensures a mature asset management process. However, several areas are already taken care of in other focus areas (i.e. training and development, risk management, information management) or are not in scope for this thesis (i.e. health and safety). Therefore, the Oarisk asset management maturity model has not been completely used.

In case of Information Asset Management this results in the following levels:

Maturity level	Explanation
0 – Initial	The costs of Asset Management are unknown, no roles are defined and no reports are made. Typically Asset Management is chaotic and unstructured.
A – Repeatable	Senior Management knows the importance of Asset management but no concrete plans exist. Though there are some structured operational processes in place.
B – Defined	There are processes in place that help Business objectives and individuals get training. Thereby, these individuals also get roles in the change management process.
C – Managed	Processes are cross departmental, Roles are well defined and Asset Management is coordinated across functions. Asset Management in this stage is well thought of.
D - Optimized	Every single part of Asset Management is documented, aligned and known organization-wide.

Table 18: Information Asset Management Maturity Model

5.4.2. Asset Management Maturity Metrics

In order to determine the maturity level of an organization regarding Asset Management the following statements have been identified:

Capability /level	Statements	Reference(s)
A	1. Senior Management within departments takes responsibility for Asset Management. 2. Senior Management within the organization recognizes the importance of Asset Management.	Oarisk (2010)
B	1. There is a formal Asset Management policy in place that takes into account the asset management lifecycle phases. 2. All Asset Management roles and responsibilities are defined. 3. Asset inventory is created based on status, connectivity,	Oarisk (2010)

	classification and proximity.	
C	1. All assets have been assigned to an owner 2. All stakeholders are familiar with Asset Management procedures and processes 3. Asset inventory is maintained. 4. Safe disposal, handled, processed, stored in line with the classification	Oarisk (2010)
D	1. Asset Management policies are periodically reviewed and updated 2. The Asset Management process is continuously reviewed and updated 3. An asset management system is in place to increase performance capacity 4. The classification is based on the asset's lifecycle	Oarisk (2010)

Table 19: ISFAM assessment statements for *Asset Management*

5.4.3. Evaluation

To evaluate the initially proposed statements based on asset management literature, I spoke to an expert with more than five years of experience in the field of ISO27K and advising herein. He performed ISO27K assignments at a variety of companies and this experience can be well used for the evaluation of this model.

The first part of the conversation was about the role of asset management in the final model. He liked the inclusion of dependencies in the model because that is not incorporated in other models he knows. His concern was the determination of dependencies. I explained that the dependencies are made following the three steps in chapter 6 and additionally evaluated at an organization to verify if the model represents the current information security level of the organization in a correct way.

Next was the maturity model of asset management. Showing the model led to the explanation of the asset management lifecycle as described in the first paragraph. In his opinion, a maturity model can be set up using the different stages of the lifecycle. I agreed, and asked whether the maturity model is represented according to this lifecycle as it is now. He recognized some kind of CMM structure which is recognizable to the business and very usable. Five stages make sense and is the right amount to map the lifecycle on. Because he was referring to the lifecycle again, I asked him if the model as proposed represented the lifecycle correctly. In general it does, but there are some changes that need to be made.

Starting with the first capability, we discussed who ideally should recognize the importance of asset management. Initially the model stated that individual employees do so, but after the discussion I changed it to senior management because ideally all ideas should be supported by senior management before it can be effective. At the second capability he made one comment. Since I only addressed the importance of asset inventory, he mentioned it would be better to also include what should be stated in the asset inventory. B3 is extended to cover this. At the third capability also some changes were made taking into account the lifecycle. C3 was added and instead of mentioning all employees at B2, it became all stakeholders. At the fourth stage two changes were made. Instead of leveraging an asset to the maximal benefit he suggested to include using a system that increases performance capacity. That should be the ultimate goal for asset management and is more concrete than what was in the model before. As a second change, I added that classification should be based

on the lifecycle of an asset. Different assets are of different importance to the organization. The invocation of applying the lifecycle varies thereby as well. If an organization operates at an optimized level, classification should be done based on the lifecycle of that asset.

Action	Result
Change	Senior Management instead of single employees should recognize the importance of asset management
Add	B3 is extended with information that should be mentioned in an asset inventory
Change	All employees in B2 became all stakeholders
Add	Asset inventory is maintained
Change	The statement *asset management should be leveraged to the maximal benefit* changed to *an asset management system is in place to increase performance capacity.*
Add	Classification should be based on the lifecycle of an asset

Table 20: Overview of changes asset management

5.5.Human Resource Security

Human Resource Security is nowadays one of the most important focus areas within information security. People are a critical factor in making or breaking the information security of an organization. 80 to 90% of organizational accidents happen due to human factors (Reason, 1997). On the one hand organizations can make their personnel aware and train them to prevent data leakage and loss, but on the other hand the same people can use the security information of their organization to gain personal benefit. Employees using inside information to breach the security of their organization is not something unusual. Even more, most of the attacks on an organization actually happen from the inside (Humphreys 2008; Theohariduo et al. 2005). This indicates how important screening, training and other Human Resource Security related subjects are.

In this thesis Human Resource Security is divided into two separate parts. One part is the process a person goes through within an organization and the other is training and awareness. Both together form the focus area Human Resource Security for this thesis.

The process a person follows during his or her career in an organization starts with everything needed prior to employment. This first phase makes sure that the person or the third party (in case of outsourcing a project) understands his responsibilities. The potential employee gets screened and the terms and conditions are discussed. Second phase is employment. The person is now an employee and in this phase it is more important to create and maintain awareness by making the employee familiar with the policies and procedures in place. Last phase occurs when an employee leaves the organization or changes job. This last phase includes activities of the focus area Identity and Access Management where accounts need to be deleted and/or rights require adaptions. Besides these technical oriented actions, there are also organizational actions to assure Human Resource Security. Former employees should always return all assets belonging to the organization and keep in mind the terms & conditions still in place after leaving the organization (i.e. do not start an organization in the same sector for x years).

Training and Awareness are necessary to reduce the chance of data loss. During the time an employee is working at an organization he/she must be aware of the policy. This process is comparable with phase two of the first aspect of Human Resource Security. However, this is an

essential part that requires more attention than the first and last phase. Hence, potential employees have less chance to steal critical information from the inside if they are not an employee yet. During the time they are really working for the organization, they have access to several systems from which valuable data can be extracted.

5.5.1. Human Resources Security maturity

Human Resources Security maturity is built from the two separate parts discussed in the last section. There are many Human Resource related maturity models. Flynn (2010) developed a maturity matrix containing four stages ranging from initial to integrated people strategy. Flynn defines what characteristics show up at what maturity level. For example, at the initial stage you typically observe ad hoc reporting, poor communication and little training. This Human Resource maturity matrix is highly detailed and only useful characteristics are used for the final model.

Another model also uses four stages and is called the People Capability Maturity Model. Although this model addresses more then only Human Resources, it holds valuable information regarding Human resources Security. Since both maturity models define four stages of maturity, excluding the initial stage, the model for this thesis also distinguishes four stages.

Maturity Level	Explanation
0- Nothing	There is no attention paid to the security of Human Resources.
A – Repeatable	The organization knows that Human Resource Security is necessary and is formalizing processes. Human Resources Security policies and processes are however not implemented.
B – Defined	At level 2 the organization wants to gain a competitive advantage by standardizing their practices across business units. Knowledge about Human Resources Security gets shared among employees.
C – Managed	Where level 2 defined the core of Human Resources Security, level 3 is about gaining strategic advantage by using Human Resources Security.
D – Optimized	The organization is optimizing their Human Resources Security. Personal development is important and the whole organization is continuously reminded of the policies.

Table 21: Human Resources Security Maturity Model

5.5.2. Human Resources Security maturity metrics

The IS18 standard (QGEA, 2010) states that at a minimum an organization needs the following:

- Training and security awareness program
- Security roles documented and defined
- Procedure development for employee changes

This represents the first stage of maturity in the maturity model. Statements used for this level and the next three levels are stated in table 22.

Capability/ level	Statements	Reference
A	1. Formal Human Resource policies are in place OR C2, D1. 2. All roles and responsibilities have been defined considering Human Resource security.	QGEA (2010)
B	1. Human resources security policies are known organization	QGEA (2010)

	wide, OR C2, D1. 2. Human resource security processes are defined, OR C3, D2. 3. All employees signed a document stating their roles and responsibilities to the organization.	
C	1. New hires get screened before employment 2. Human resources security policies are fully implemented in the organization, OR D1. 3. Human resource security processes are fully implemented, OR D2. 4. There is a paragraph in the contract which elaborates on post-employment restrictions.	QGEA (2010)
D	1. Human resource security policies are regularly reviewed and updated. 2. Human resource security processes are being optimized continuously.	QGEA (2010)

Table 22: ISFAM assessment statements for *Human Resources Security*

5.5.3. Evaluation

To evaluate the initially proposed statements based on human resources security literature, an internal expert with over 10 years of experience as security officer has been asked a couple of questions mentioned in Appendix B. Considering the model, he suggested the following:

There is no need to change the amount of levels. Following CMM, the levels correspond to the human resources security structure.

Capability A is good, but two statements need to be changed. It is important at the start of employment to face them with their roles and responsibilities. However, those roles and responsibilities are defined at capability B. A switch between the two statements has been done. Second in the process is retaining that awareness and therefore it is rightly placed at capability B. One statement has been removed, because it overlaps with the initial first statement of capability B: There is introduction training available to generate information security awareness. Since the purpose of this is creating awareness and statement B1 is more generic, B1 stays. The same holds for capability C. One statement has been removed: There are regular training sessions on information security developments. At capability C, one statement has been added considering employees leaving the organization. It is an integral part of coping with leakage of confidential information. Capability D requires no changes, since it perfectly matches with the highest CMM level.

Action	Result
Change	*All roles and responsibilities have been defined considering Human Resource security* has been moved from capability B to capability A
Add	B3 is extended with information that should be mentioned in an asset inventory
Remove	There is introduction training available to generate information security awareness has been removed
Remove	There are regular training sessions on information security developments
Add	There is a paragraph in the contract which elaborates on post-employment restrictions.

Table 23: Overview of changes human resources security

5.6.Physical and Environmental Security

Whereas Identity and Access management is on a technical level, Physical and Environmental Security is on a physical level. Instead of talking about passwords, it is now about human attackers that want to enter a building holding sensitive information. Physical and Environmental Security is not only about human attackers, but also about the protection against natural disasters and every other external or environmental event (i.e. fire, earthquake) that might harm the organizations physical assets with as result the loss of information. Physical Security is defined as:

Physical security:
"Physical security describes measures that are designed to deny access to unauthorized personnel (including attackers) from physically accessing a building, facility, resource, or stored information; and guidance on how to design structures to resist potentially hostile acts."
(Structural Engineering Institute, 1999)

Environmental Security in literature is a concept that often deals with sustainability and nature. This is not the case for information security. Environmental security in literature is defined, in its most general sense, as "a concern with human vulnerability to natural resource scarcity created by human and/or natural processes" (Carr, 2005). In case of information security, Environmental Security has nothing to do with scarcity of natural resources, but with the protection of information.

Environmental Security for this thesis is defined as:

Environmental Security:
"Environmental security is, in its most general sense, a concern with organizational vulnerability to information loss created by human and/or natural processes"

Difference in this definition is that human has been changed in organizational, since the organization is responsible to secure their vulnerabilities and not a human. Their risk is losing information and not scarcity.

The goal of Physical Security and Environmental Security is, according to ISO27002, the same and they are therefore combined in one focus area. Main objective of both is "to prevent unauthorized physical access, damage, and interference to the organization's premises and information" (British Standard Institute, 2005). This includes three concepts: hardware, environmental infrastructure and humans and the information they possess (Michael, 2006). Carlson (2001) states that the focus area Physical and Environmental Security addresses the risks inherent to the organizational premises. Security in this case means securing business information inside a building by physical measures. This could in an easy case be fortified walls and in a more advanced situation fingerprint recognition. This focus area shows overlap with Identity and Access management in a way that it could both be about access control. However, in terms of how to deal with access control, Identity and Access Management is about the technical aspect (applications) and Physical and Environmental Security about the physical part (implementing measures such as a fingerprint device).

An example of Physical Security is Tamper Resistant. This concept is comparable to securing a bank vault (Weingart, 2000). The protected device has many protection layers and it is hard to penetrate these. Hard Barriers is a way to protect your information by steel, bricks, etc. Weingart (2000) describes more ways of Physical Security in his paper.

5.6.1. Physical and Environmental Security maturity

Literature does not have a maturity model for Physical and Environmental Security. The CMM standard is used to create a maturity model for this focus area. CMM consists of five stages: initial, repeatable, defined, managed and optimizing. Making those five stages applicable to Physical and Environmental Security leads to the following maturity model:

Maturity level	Description
0- Initial	Problems are handled when they occur. i.e. if someone enters the premises without permission that person is removed but no formal systems or procedures are in place.
A- Repeatable	If events reoccur several times, this knowledge is used to form an informal process of how to handle with that event. The organization becomes more professional in dealing with environmental uncertainty and harming physical attacks.
B- Defined	Processes that help solving a problem triggered by an event are documented and become standardized.
C- Managed	At this stage, the organization starts measuring if they improve their Physical and Environmental Security. This can for example be done by dividing the amount of successful attacks over the amount of unsuccessful attacks. In this way the organization creates knowledge on where to improve.
D- Optimizing	The organization is improving their Physical and Environmental Security continuously and checks/updates their security on a regular basis.

Table 24: Physical and Environmental Security Maturity Model

5.6.2. Physical and Environmental Security maturity metrics

The maturity level of Physical and Environmental Security within an organization is determined by metrics and actions found in literature. All metrics are bound to a certain maturity level. The result is shown in table 25. The metrics take into account the decisions management might make from a financial point of view. Hence, the most mature organization is expected to be an organization taking all natural disasters into account. However, an organization not geographically situated on a fault can decide from a financial point of view not to take any precautions. This should not make the organization less mature, because they did consider the precaution. The most mature stage should thus be the continuous consideration of what could happen if they do not take the precaution and if they would dare to accepts the consequences if the, in this case, earthquake happens or not. More in depth metrics can be found in the NoticeBored technical briefing on datacenter security (2004).

Capability /level	Statements	Reference
A	1. There is a formal Physical and Environmental Security policy defined 2. Access to Key facilities is limited to a certain amount of persons.	NoticeBored (2004)
B	1. All roles and responsibilities considering physical and	NoticeBored

	environmental security are defined 2. The organization uses multiple security zones 3. Key facilities are protected from theft 4. Access to key facilities is logged	(2004)
C	1. All ICT assets that store or process business information located in secure areas 2. Access to key facilities is actively monitored 3. The physical and environmental measures are tested and audited on a regular basis 4. The appropriate personnel receives training in preventing physical breaches	NoticeBored (2004)
D	1. Policies and procedures are periodically reviewed and updated 2. All facilities are protected from theft and severe weather.	NoticeBored (2004)

Table 25: ISFAM assessment statements for Physical and Environmental Security

5.6.3. Evaluation

To evaluate the initially proposed statements based on physical and environmental security literature, I spoke to Trajce Dimkov who received his Dr Title in 2012 in the field of social engineering. During his research at the University of Twente he let students try to steal laptops from colleagues. This study is related to the physical security the University of Twente had at that moment of time. He gained a lot of knowledge on social engineering and physical security and therefore I asked him if he would be willing to evaluate this maturity model.

Considering his background at the University of Twente, I took the opportunity to show him the whole model and ask him about his opinion. While explaining the model, he posted questions on the validity of the model. These questions covered both capabilities as well as dependencies. I told him that the different models are derived from literature and that all models are evaluated by an expert to add business value. He agreed upon the method and the thoughts behind the model.

Next we discussed the role and interpretation of the physical and environmental security maturity model starting with the following question: “Do you know any maturity model for physical and environmental security”? He answered that he does not know any maturity model in that area, but that he does know how to improve physical and environmental security in an organization. The model of NoticeBored is not known to him, but it seems to be a good model to start with.

The maturity model is built up as a CMM. Five stages and four to define statements on in his opinion do make sense. Reviewing the statements within the model strengthens this decision. However, some statements need to be added or changed. Most of his changed can be referred back to the concept of security zones. The security zones concept can be compared to building a castle with different layers and zones of defense. Some places in your organization require better defense than others. In the least mature stage you would probably see organizations that can be matched to the egg stadium; it is hard to get inside the building, but once you are in, you can do anything. The concept of security zones led to the inclusion of B4: The organization uses multiple security zones. Another point of attention is testing and training. Originally, both were not in the model. However, humans are the weakest link in the security of an organization and can make or break the security. training the right people to prevent criminals from stealing valuable information and testing whether the training has effect is a way of improving the awareness of your personnel.

Action	Result
Add	The organization uses multiple security zones
Add	The appropriate personnel receives training in preventing breaches

Table 26: Overview of changes physical and environmental security

5.7.Change Management

All organizations change over time. This can be a decision by the organization or an event from the outside. What is sure is that change is needed to remain relevant (Queensland Government, 2009). Change Management helps to align the organization with those changes.

Evergreen conducted a research in 2006 to extract the reason that organizations implement Change Management processes. Although service quality is mostly recognized by organizations (66,7%) in their decision to start implementing Change Management processes, reducing risk is with 32.4% also an important factor (Casson, 2006). For this reason, Change Management is a focus area of information security.

Leopoldi (2002) defines Change Management as:

Change Management:
"Change Management is the process of planning and coordinating the implementation of all changes (any planned alteration or addition to the operating environment including application systems) into the production environment in a logical and orderly fashion. It does not develop changes, nor does it implement them."

Tthe goal of the Change Management process is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the organizations.

Change Management is responsible for managing the change process for hardware, communications equipment and software, system software, and all documentation and procedures associated with the running, support and maintenance of live systems. (Sanli, 2010). ISO27002's definition of operations and communications management domain shows similarities with this definition of Change Management. Therefore, this focus area is not called Operations and Communications Management, but Change Management.

A lot of theories and models are known in the field of Change Management. Kurt Lewin (1951) made the three step model consisting of the phases: Unfreeze, Change, And Freeze. These three phases represent the preparation for change, the change itself and getting the change stable. This three step model of Lewin has been slightly changed by Prosci (2004). According to Prosci, Change Management consists of an individual part and an organizational part. Prosci defined both and states that the first step is changing the individual. The individual learns to understand change by ADKAR (Awareness, Desire, Knowledge, Ability, and Reinforcement). The organization gets more support for managers and supervisors in this way.

Instead of unfreeze, change and the freeze phase, Prosci's Change Management for organizations or projects knows three process phases (Prosci, 2004):

- Preparing for change – This phase includes activities to prepare the organization for Change Management. A Strategy is defined at this stage.
- Managing change – This phase is about designing and implementing Change Management plans and activities.
- Reinforcing change – All activities and implementations are checked on performance. Where gaps or negative feedback occurs, alternative actions are taken to improve Change Management.

Those three steps are used as a basis for the maturity model discussed in the next section.

5.7.1. Change Management Maturity

Besides the three phases, Prosci also made a maturity model on the field of Change Management. This model is pictured in figure 20. The Prosci maturity model uses the same five levels as the original CMM and is based on ADKAR and the three phases. The maturity model of Prosci is therefore well-suited as starting point.

The research behind this model states that 85 % of the 160 organizations placed themselves lower than level 3. Besides this finding, the model is not 'one-size-fits-all'. However, it is still possible to move to level 4 or 5 when looking at an organization specifically and exclude superfluous factors.

Level 5	Organizational Competency	Change Management competency is evident in all levels of the organization and is part of the organization's intellectual property and competitive edge	Continuous Process improvement in place	Highest profitability and responsiveness
Level 4	Organizational Standards	Organization wide standards and methods are broadly deployed for managing and leading change	Selection of common approach	
Level 3	Multiple Projects	Comprehensive approach for managing change is being applied in multiple projects	examples of best practices evident	
Level 2	Isolated Projects	Some elements of change management are being applied in isolated projects	Many different tactics used inconsistently	
Level 1	Adhoc or Absent	Little or no change management applied	People-dependent without any formal practices or plans	Highest rate of project failure, turnover and productivity loss

Figure 20: Prosci's Change Management maturity model

The levels are comparable to the levels of CMM. The names are different but the meaning is for almost every level the same. The only difference is made in level 4. Level 4 in CMM is about making your processes measurable so you can track the performance. In Prosci's Change Management maturity model level 4 is about standardization. Nonetheless, this difference is not significant enough to question the model. The model shows stages of improvement and has clear definitions that indicate the process an organization should follow to actually improve their Change Management process.

5.7.2. Change Management maturity metrics

Prosci (2004) provides a couple of measures an organization could take to move their Change Management to the next level. The following table addresses the metrics and measurements. Level 1 is not included in this table because at level 1 there is basically nothing related to Change Management. Level 1 could thus also be seen as level 0. All levels have been translated to A-D to suit the design of the focus area maturity model.

Capability /level	Statements	Reference
A	1. Management is aware of the importance and existence of Change Management 2. Change management is used in large projects 3. Change Management is used to react on negative events.	Prosci (2004), Queensland Government (2009)
B	1. There are formal roles and responsibilities defined for Change Management 2. Change Management is used in all projects 3. The Change Management process is structured	Prosci (2004), Queensland Government (2009)
C	1. There is a formal Change Management procedure designed 2. The Change Management process is standardized and the changes documented. 3. Change Management is used to track configuration and other small changes to the organization's IT environment. 4. Senior Management is responsible for Change Management	Prosci (2004), Queensland Government (2009)
D	1. Change Management is an organization wide integrated process 2. There is a formal Change Management procedure implemented. 3. The Change Management procedure is supported by information systems. 4. Emergency change procedures are covered in the Change Management procedure	Prosci (2004), Queensland Government (2009)

Table 27: ISFAM assessment statements for *Change Management*

5.7.3. Evaluation

To evaluate the initially proposed statements based on change management literature, I interviewed an IT auditor with around one year of experience. Part of his function as an IT auditor is to review the change management process of an organization. The interview started with an explanation of this thesis, the final goal and what the role of change management is in the final model.

He agreed that change management is part of information security and explained how a change management process should work in practice. This explanation covered this focus area, but also the secure software development area. I therefore asked him whether secure software development is the more technical part of change management where the content of the change management process is covered. He said that it is the more technical part and that my division is a justified decision.

Next we started to review the model, the amount of levels it has and whether the right statements are at the right place in the model. His first remark was about change management training. Training is almost never given around change management but more on a higher level like awareness on information security. All training statements can therefore be removed. In addition he mentioned that awareness is important and that he would change the awareness training statement at

capability A to M*anagement is aware of the importance and existence of change management.* Having done that we discussed the awareness around change management and when would an organization become aware and is that due to large or small projects. Since there was an assumption in the original model that organizations would first try out change management on smaller projects before using it on cross-departmental projects, it turns out to be the other way. Employees only start seeing the urgency of change management while they are in a large project where they are not able to oversee all activities going on.

At capability D two suggestions were made, namely the addition of emergency changes and the movement of "*The board is responsible for Change Management"* to capability C. Since nothing about emergency changes was mentioned in the model, I added this to capability D. The movement of "*The board is responsible for Change Management"* was justified because when you want to implement a procedure, it makes sense to make a high person in the organization responsible for it. Since implementation is part of capability D, the responsibility of the board is moved to capability C.

The last correction made to the model dealt with the documentation of changes. There was no statement mentioning that changes should be documented. It has been added to capability C, because it is not yet an information system that supports the change management procedure, but there should be some other way of documentation.

Action	Result
Change	Replace statements about training with one new statements at capability A: *Management is aware of the importance and existence of change management*
Change	First change management is used in large projects and afterwards change management is also used in smaller projects
Add	Emergency change procedures are covered in the Change Management procedure
Change	*The board is responsible for Change Management* is moved from capability D to C
Add	The Change Management process is standardized and the changes documented at capability C

Table 28: Overview of changes change management

5.8.Identity and Access management

Identity and Access management (IAM) consists of two concepts: 1) identity and 2) access. To understand IAM better the two smaller concepts are elaborated on first.

A digital identity contains 1) data that uniquely describes a subject/entity (i.e. a person) and 2) information about the relationships to other subjects/entities (windley, 2005). Identities always follow the lifecycle pictured in figure 21 during their existence. This lifecycle is the process called identity management.

Figure 21: The identity lifecycle

The identity lifecycle starts with registering an identity. The administrative processes for registering an identity establish the relation between the entity and the registration. An important part of the registration is assigning attributes to the identity. Trust plays a key role in this process because trust determines what functions or procedures an identity is allowed to access/change. From a technical point of view this process involves creating an account with the proper rights. Securing these accounts is done by using credentials (e.g. passwords, digital certificates) for authorization. Typically, this step in the lifecycle handles the procedures concerning creating and issuing the right credentials to the right identities. The second step is the usage of the identity. An entity (i.e. person) can log on to an information system and gains the rights from its identity. Third step is the maintenance of the identity. An entity might change over time (i.e. a person getting promotion, a password that needs to be changes, etc.) what can lead to changes to their identity. If so, the maintenance step should update this identity accordingly. Last is the deregistration step. If an entity does not have any interest anymore in a certain information system, the identity should be discarded. This could be the case when a person leaves the organization. All access rights to information systems should be deleted from a security point of view. Hence, companies do not want that a fired employee is allowed to access data when he is not working at their company. If this happens, it could lead to date leakage which could end up in competitors having critical information which could give them competitive advantage.

Access is the ability to use features in an information system. The permissions an identity is access defined in functional terms. The association of permissions with identities can, just as with identity, be described as a lifecycle with various processes. The lifecycle containing four steps is pictured in figure 22.

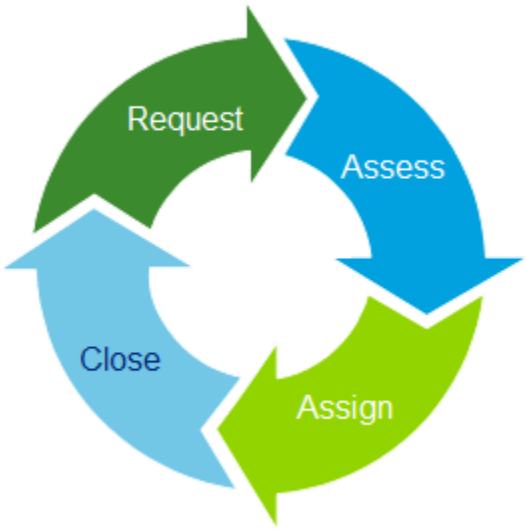

Figure 22: Access lifecycle

During the request stage information is collected to support the assessment, assignment and closure of access. This information includes the reason for the request, the approvals needed, the identity of the requestor, etc. The next step is to assess the request. Why does the person need access to it and what does the person want to do with it. The assessment of this request can be done more structured by for example a RBAC system as defined in the information security history section. RBAC systems can be useful when an organization has a lot of the same type of users for which they can create a standard role. This standard role can then be assigned to employees who fulfill this role within the organization. Third step is the assignment of the access to the person. Hard part is to align the permissions a person is granted with the privileges a system has. I.e. a person who has permission to register a bank account in the system needs the privilege to enter data in the database. Last phase is the closure of access. Access is granted for a specific function a person has within the organization. When changing jobs within the organization it might be that that person requires different permissions. In this case the old permissions need to be removed to prevent fraud.

Now that the concepts identity and access have been explained, a definition for identity and access management can be given. Koelewijn (2009) defines identity and access management as the activities and tools that manage identity and access through their lifecycle. Examples of activities can be the deletion/creation of an account and granting permissions to persons. Tools can be any system that supports or automatizes those activities. IAM plays a significant role in securing an organization and is therefore one of the focus areas for the ISFAM. Hence, data leakage and high annual costs are a significant risk when nothing is done to implement IAM features.

5.8.1. Identity and Access Management maturity

An organization can develop their identity and access management over time by implementing systems and changing policies. In order to do so the organization can follow a maturity model that indicates what steps to take to become more mature. Such a maturity model has been made by Forrester (2010) and Gartner (2009). Forrester and Gartner both define a 5 staged maturity model for IAM based on the CMM. The Forrest model uses exactly the same stages as in the original CMM

and is therefore straightforward to understand and process for the IAM maturity model and capabilities.

Gartner uses the same stages as Forrester's model. The difference with Forrester's model is the interpretation of the stages. Where Forester makes a division into three areas of interest within identity and access management, Gartner identifies six. Within the maturity model for the IAM focus area for this thesis no divisions are made because the goal is to describe the maturity on a high level and not to go into depth too much. Nonetheless, every metric within the areas of interest is looked at to see whether they could provide useful information for the final information security maturity model. An important point of attention in using the models of Gartner en Forrester is dependency. Gartner and Forrester average the values gained from the questions and metrics they address in their survey. This is maturity wise incorrect because an organization that has not everything in place for reaching level 1, could never reach level 2 until the requirements for level 1 are fulfilled. In case of the Gartner and Forrester model this is possible and additional attention considering dependency is thus needed.

Maturity level	Description
0- Initial	IAM has no business value and happens ad hoc. Roles, if they are there, emerged informally. Management has some awareness of IAM.
A- Developing	IAM becomes a separate discipline. IAM is performed per project or business unit but not organization wide.
B- Defined	The CISO identified the need for a standard way of handling IAM. Roles and process become defined and an IAM strategy is put into place. IAM now gets some business value.
C- Managed	IAM has proved business value and IAM is integrated throughout the whole organization. IAM supports the strategy and vision of the organization.
D- Optimized	IAM programs are continuously optimized and reviewed. IAM is now an enabler for the business.

Table 29: Gartner maturity model for IAM.

This thesis uses the Gartner maturity model for IAM because this model has been defined on a more generic level. The model of Forrester took a more technical view regarding identity and access management and included Single Sign On, cloud-based solutions and commercial tooling. the model of both models to address the whole field of IAM.

5.8.2. Identity and Access Management maturity metrics

In order to determine the maturity level of the IAM process in an organization metrics are needed. The following table defines the statements per maturity level.

Capability /level	Statements	Reference(s)
A	1. There is a formal IAM policy in place 2. User Management is done on an ad-hoc basis OR C2, 3. Individuals take responsibility for IAM OR C4. 4. IAM is IT oriented and does not support Business OR C1, D2	Gartner
B	1. Access to applications and buildings is logged 2. A formal IAM program and process is in place 3. The IAM policy contains a password policy which is business unit oriented OR C3, D1.	Gartner

	4. Roles and responsibilities considering IAM have been defined	
C	1. The IAM policy/documentation supports the vision and strategy of the company OR D2 2. User Management is done periodically (every month/year) OR D4. 3. The IAM policy contains an organization wide password policy OR D1. 4. Senior Management is responsible for IAM. 5. Access to applications and buildings is logged and reviewed on a periodical basis.	Gartner
D	1. The IAM policy contains a password policy that is system/role oriented 2. IAM improves the business and generates new opportunities. 3. The IAM program and processes are periodically reviewed and updated 4. User Management is a continuous process supported by an IT system	Gartner

Table 30: ISFAM assessment statement for measuring IAM maturity

5.8.3. Evaluation

To evaluate the initially proposed statements based on identity and access management literature, I conducted an interview with an expert of Deloitte on the field of access control. With more than 5 years of experience in this field he knows how organizations arrange their access control and what the best practices are.

One of the questions, as stated in Appendix A is about Single Sign On (SSO) and how it might affect the security of the organization. Although my initial thoughts were that SSO is not more secure than a normal system of gaining access, it appeared not to be through. Employees only in the need of remembering one password are more likely to pick a difficult password. This secures the entrance to other applications better than having employees storing easy passwords for a lot of applications. Besides, I thought it might affect the maturity of an organization's IAM process. This is not necessarily true. If SSO is not implemented in the right way, it becomes even easier for hackers to comprise the organization's systems. Therefore SSO can be left out of the maturity model. On the other hand, adding the support of an IT system throughout the process does affect the maturity of an organization because the process becomes more structured and easier to manage. Another statement that is removed handles the use of a governance model to support IAM. This is, although important for IAM, more a statement for organizing information security than it is for IAM. A statement added to the model is: Access to applications and buildings is not only logged, but also reviewed periodically. Logging itself does not display suspicious activities, once you start reviewing the logs, additional actions can be taken.

Action	Result
Remove	Statement about using SSO within the organization at level C
Change	"supported by an IT system" has been added to statement D4
Change	Access should be logged but the log should also be reviewed. This has been added to C5

Table 31: Overview of changes identity and access management

5.9.Secure Software Development

This focus area is mainly technology based. An organization always uses information systems. The use of these information systems varies in criticality. For a financial institution, for example, the transaction systems are of great importance. No client of a bank would want to lose their money because of a security issue. According to Daud (2010), who refers to the statistics of CERT, the amount of vulnerabilities is increasing significantly over the last years. This figure indicates that secure software development is a key factor in becoming more mature with respect to information security. If your information systems are not well programmed it is vulnerable to hackers who might find confidential information in your system. For this reason, secure software development is part of the final model.

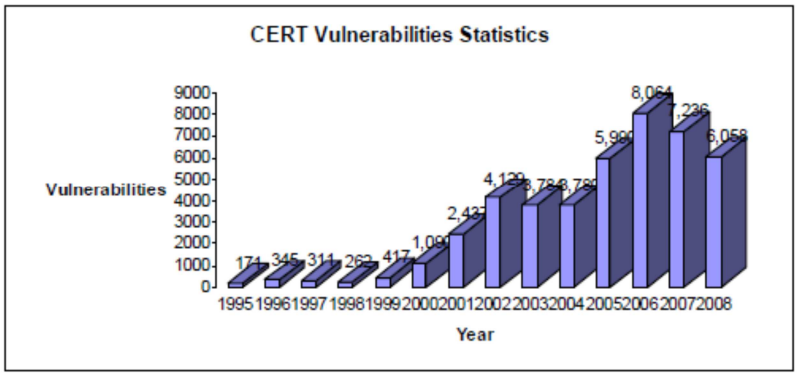

Figure 24: CERT vulnerability Statistics

To secure the organization against vulnerabilities a lot of secure software development lifecycles have been made over the past years (Khan & Ambedkar, 2011; Daud, 2010; Mahizharuvi & Alagarsamy, 2011). For this thesis, the lifecycle of Daud (2010) has been chosen because of the use of iterative steps. Figure 25 shows the lifecycle as mentioned by Daud. Like all other lifecycles, the first step is requirements gathering. This is the phase where the piece of software gets its functional and non-functional requirements. Additionally, in secure software development, there are security requirements. Second phase elaborates on the feasibility and possible misuse of the software. Based on this phase requirements can be adjusted. Next, the software is designed in a secure way using security use cases and threat models that identify possible vulnerabilities. Fourth is the coding or implementing step. Coding needs to be done using best practices and standards wherever is possible to prevent vulnerabilities. After the coding has been done it is very important to test the code both on functionality as well on security. Trying to hack the piece of software is not a big issue in the test phase, but once it is in production a real hacker could do exactly the same. Extensive testing is a must in the software development lifecycle. Last is the deployment of the software. This does not only include the migration of the code to production but also the maintenance of the software afterwards. This can be done by audits, pen-testing, code reviews or regular scheduled maintenance. This last phase is discussed in more detail in the lifecycle of Khan and Ambedkar (2011).

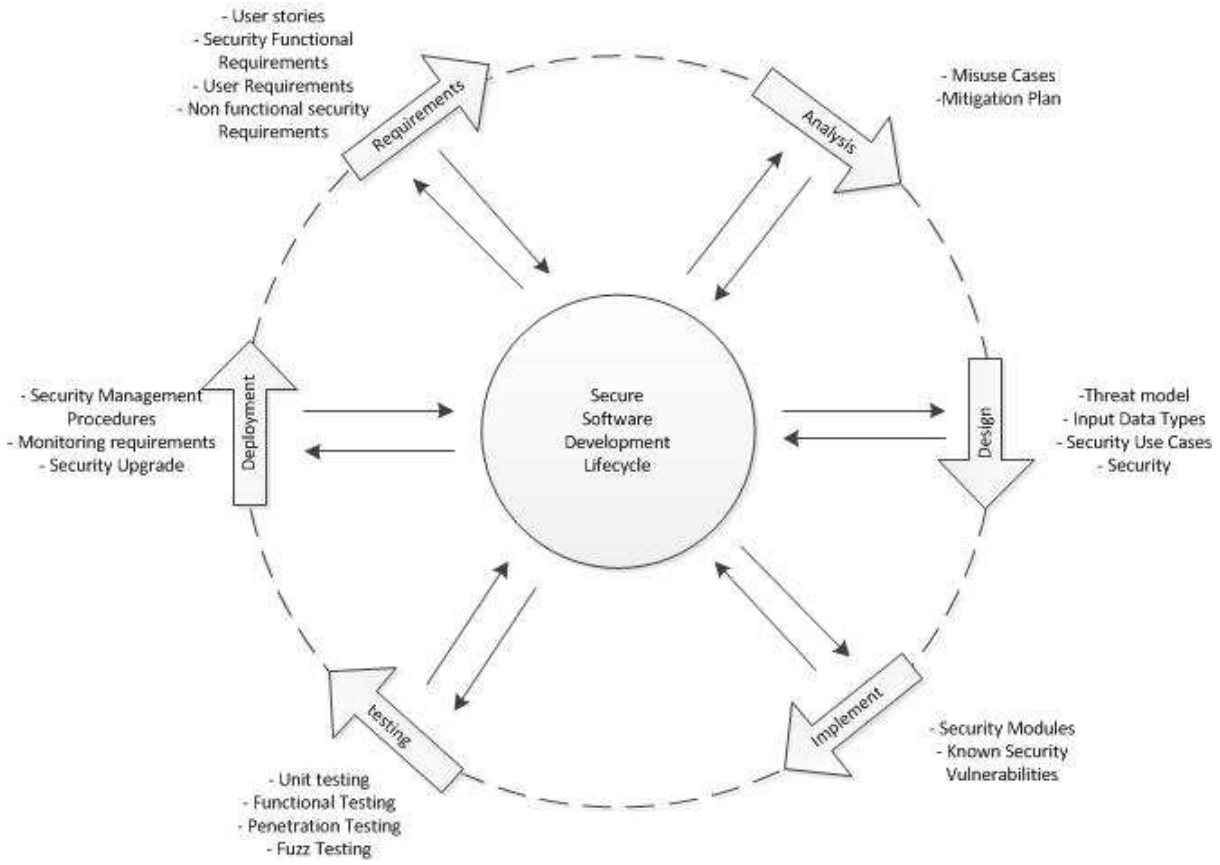

Figure 25: The software development lifecycle (Daud, 2010)

5.9.1. Secure Software Development maturity

There are several maturity models for secure software development. None of them could be copied one on one onto the ISFAM model. The combination of three of the maturity models led to the following maturity model:

Maturity level	Description
0- Initial	The organization does not have a secure software development policy, does not update their software, etc.
A- Developing	An idea of how to develop their software is in place, but security is not the main point of attention. Functionality is.
B- Defined	Security becomes part of the development lifecycle and code gets reviewed on an ad-hoc basis.
C- Managed	Software is built around the security requirements
D- Optimized	Software is regularly reviewed on updates and vulnerabilities

Table 32: maturity stages for Secure Software Development

The first maturity model used to create this maturity model is Building Security In Maturity Model (BSIMM3, 2011). BSIMM differentiates 109 activities divided over four domains: Governance, Intelligence, SSDL Touchpoints, and Deployment. Within these areas numerous activities have been defined considering secure software development. Although this model is way to extensive, it holds activities like establishing procedures and policies considering secure software development that can be used for the ISFAM model. BSIMM has been used as basis for the development of the secure software development maturity model for this thesis.

The second maturity model is the Software Assurance Maturity Model (opensamm, 2011). This model also recognizes four different areas in secure software development: Governance, Construction, Verification and Deployment. Last three areas can be traced back to the software development lifecycle and are simple to translate to a CMM like model. This model has been used especially for translating the BSIMM activities onto the secure software development lifecycle. If activities were the same in both models, it has been mapped 1 on 1. Else, the decision has been made whether the activity of the BSIMM would be too technical for inclusion in the final model.

Last model is the Secure Software Engineering CMM. This model is already a CMM based model. Just as BSIMM3, this model is very extensive. It distinguishes 22 areas with each area covering over twenty statements. SSE-CMM has a lot of information inside and is very valuable to this model when viewing it on a high level. This model has been used to verify the model already made after the combination of the first two models and checked whether the statements initially set up can be found in the SSE-CMM model. For all statements this was the case, which made the statements in the model presented in the next section more reliable.

5.9.2. Secure Software Development maturity metrics

The following table gives substance to the maturity model as proposed in the previous section.

Capability /level	Statements	Reference(s)
A	1. The System Development Lifecycle consists at least of: • Requirements Gathering • Development • Testing • Migrating to production 2. There is a formal System Development policy in place. 3. Development, Testing and the Production environment are separated 4. There is a formal System Development Lifecycle in place.	Opensamm 2011, BSIMM3 2011, SSE-CMM 2011, ISF 2011
B	1. A formal deployment plan is used for migrating changes or new systems to production 2. Roles and responsibilities have been defined throughout the whole System Development lifecycle 3. Business requirements are based on standards, policies and procedures 4. Risks are identified for every project.	Opensamm 2011, BSIMM3 2011, SSE-CMM 2011, ISF 2011
C	1. Test results are documented. 2. Quality review is a step at the end of the System Development Lifecycle, OR D2 3. Staff is trained to know how to use the System Development Lifecycle 4. There is a formal sign off procedure at the end of each stage of the System Development Lifecycle	Opensamm 2011, BSIMM3 2011, SSE-CMM 2011, ISF 2011
D	1. A post implementation review is done on every change or new system 2. Quality Review is a continuous process in the System Development Lifecycle 3. Business Requirements are reviewed at each step of the	Opensamm 2011, BSIMM3 2011, SSE-CMM 2011, ISF 2011

System Development Lifecycle

Table 33: ISFAM assessment statements for Secure Software Development

5.9.3. Evaluation

To evaluate the initially proposed statements based on software development literature , I spoke with an expert having over 3 years of experience in the field of Secure Software Development. He has been involved in the Secure Software Development lifecycle, but also has experience in writing policies in this area.

The interview started with explaining the goal of the research and that Secure Software Development is one of the focus areas in the final model. After showing the Maturity Model for Secure Software Development and explaining how the division was set up we talked about the most important parts of Secure Software Development. Or, in other words, it is the first statements that an organization should be able to answer with "yes we have" in becoming more mature.

He suggested dividing the Secure Software statements over the four levels by looking at the CMM methodology. This implicates that the first level is 'Do', the second is 'Document', the third is 'Do what you document', and the last is 'Monitoring and optimizing'. Monitoring and optimizing normally should be two separated levels, but in the case of Secure Software Development he agreed that a combination of both levels is a good way to go, because the monitoring and optimizing level are in case of Secure Software Development overlapping and more or less the same.

The statements in place cover the maturity stages of Secure Software Development in a good way. There is no need to add statements. Changing associated levels of statements is necessary because of the change of view on the maturity model described in the previous paragraph.

Action	Result
Change	*Risks are identified for every project* has been moved from capability C to B because of the new approach mentioned by the expert
Change	*Test results are documented* has been moved from capability B to C

Table 34: Overview of changes secure software development

5.10. Incident management

A Computer network can be attacked in many ways. These attacks can also be mixed and therefore the threat enlarges. To prevent loss and destruction of data of an organization, the organization must be able to handle such incidents in a fast and effective way (Kalbande, Singh and Thampi, 2009). Two automated ways of preventing and detection these incidents have already been mentioned in the literature study: Intrusion Detections Systems and Intrusion Prevention Systems. However, attackers are always improving their strategy and tools and therefore a well-defined incident process should be in place.

Many methodologies for incident management (also called incident response or incident handling) have been developed. NIST (2004), and West-Brown et al. (2003) have all written a method to minimize the impact of security incidents and to identify and improve vulnerabilities in the systems. A typical Incident Response method contains six steps as depicted below.

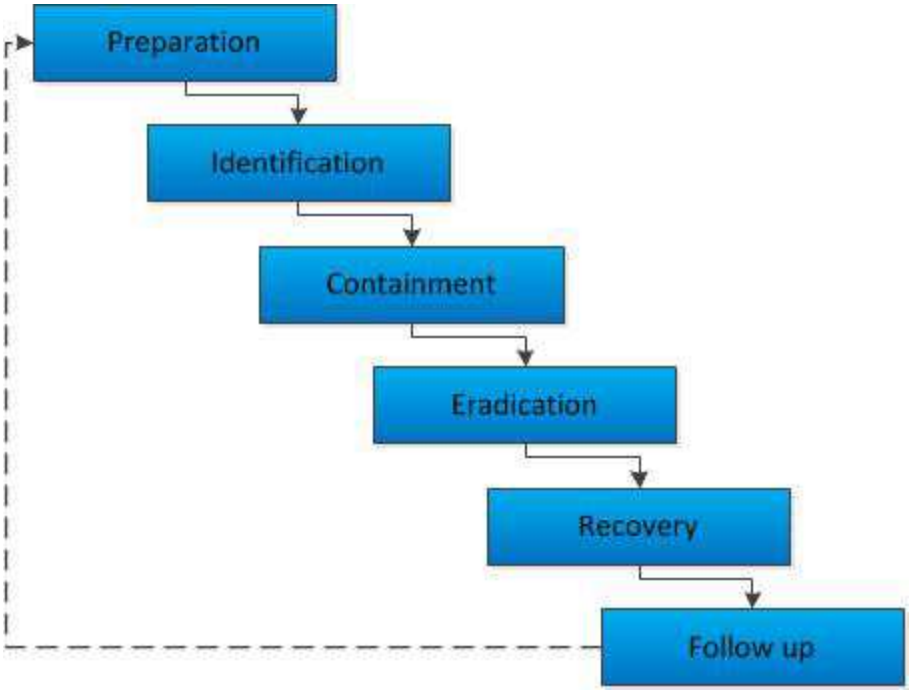

Figure 26: Incident Response Method (Mitropoulos, Patsos and Douligeris, 2006)

Preparation: The first step in the method is the preparation phase. This phase should make sure that back-up procedures are in place and that back-ups are made. Besides the ability to recover and patch systems, it is also important to keep an audit trail. An audit trail enables an organization to trace back issues that have taken place to prevent such events from happening again.

Identification: The next step is the identification phase. In this phase decisions about categorizing events have to made and therefore identification is a crucial step in the method. After the identification of an event, evidence gathering should start immediately to later assist in solving the incident. After the incident has been identified, it needs to be classified. In most organizations this means that incidents can be categorized as high impact, medium impact or low impact. This impact is based on the criticality of the program or service to the business and the costs made while the program or service is down and what it costs to recover the system.

Containment: Now the incident has been identified and classified, the appropriate actions should be taken to prevent the attack from spreading and causing more damage to the organization. Actions involved might be shutting down the compromised services or the restoration of compromised systems by putting in place a back-up.

Eradication: This phase makes sure that the incident happened will be solved for a long time. This might include hardening, reinstalling or rebuilding the system dependent on the nature of the incident.

Recovery: Recovery of the systems should make sure that the system is in production again without security holes open. This can be done in the eradication phase by rebuilding the system from scratch, but recovery should also make sure the data is recovered from trusted back-ups, the system is configured in a secure way and that the system is reviewed on its security level.

Follow up: Last, all actions taken to recover from the incident should be documented to improve the incident response time and procedure

To make sure this process is effective, the process should be tested. Tests can be done on paper or in real-time. Paper tests are safe and represent a walk-through when an incident happens. However, testing an incident in real-time provides a better overview of the awareness of the organization, the cost of the incident and thus the effectiveness of the incident response procedure. Most of the times, this procedure is the guideline for the appointed security incident response team, who are responsible for solving incidents in a timely manner.

5.10.1. Incident Management Maturity

Following the process described in the previous section, incident management is divided over five different maturity stages. The first one being the stage where they did not even think of incident management and the best practice level as the level where they continuously try to optimize their incident management process. The model used for this thesis is based on the PPBI Incident management maturity model. (Mura, 2012)

Maturity level	Description
0- Initial	The organization does not have anything in place to handle incidents in a structured way.
A- Inadequate	There is a policy and a process for the classification of systems, but no formal roles or processes are defined
B- Marginal	Formal processes and roles are defined. Effectiveness is however unknown
C- Acceptable	Audit trails and tooling is used to support the incident management process
D- Best practice	The incident management process is tested and optimized using the test results

Table 35: Incident Management Maturity Model

5.10.2. Incident Management Maturity metrics

Based on the maturity model, the following statements can be identified per level.

Capability /level	Statements	Reference(s)
A	1. A formal Incident Management policy and process have been defined. 2. Formal process to assess and classify systems based on the business criticality in place.	
B	1. There is a formal incident management implemented. 2. Roles and responsibilities have been defined in order to respond in a timely manner on incidents. 3. Systems are assessed and classified based on their criticality to the business.	
C	1. The systems provide an audit trail to trace back the incident. 2. The incident management process is tested using a walkthrough to validate its implementation. 3. The Incident management procedure is supported by tooling	
D	1. The organization documents incidents as an when they	

occur. 2. The organization learns from previously occurred incidents and updates the process accordingly 3. The incident management process is tested for operational effectiveness in real time by executing periodic exercises.

Table 36: ISFAM assessment statements for Incident Management

5.10.3. Evaluation

To evaluate the initially proposed statements based on incident management literature, an expert in the field of business continuity and incident management evaluated the model. Four questions were asked to evaluate the model. First question handled the amount of levels in the maturity model. The expert said that four levels, excluding the level 0 would be sufficient and covering the area of incident management.

Secondly, he identified a missing statement which influences the maturity. The maturity of incident management is also determined by the way they use automated tooling to log, detect and monitor the status of the incidents. He suggested adding the use of an incident response system at capability C, since it is not the first thing you would do when willing to adopt an incident management procedure, but also not the most mature stage. Choosing between capability B and C led to C because the procedure should be covered in B and this statement is the implementation of the procedure. This can only be done when this statement is added in C. Other statements were correct and only minor changes were proposed considering wording.

Next, the statements were judged on the level they are placed. The expert would like to see the procedure statement divided over two capabilities. This implicates that putting in place or developing the procedure is in capability A, and implementing the procedure in capability B. Last question addressed if there are any other issues considering the model. He said that the other questions covered the whole model and that he had no additional comments.

Action	Result
Add	The Incident management procedure is supported by tooling
Change	*A formal incident management policy and process have been defined* is placed at capability A, the implementation of the process has been located at level B

Table 37: Overview of changes incident management

5.11. Business Continuity Management

Since the Y2K threat (Oud, 2000) Business Continuity Management (BCM) attracted the attention of organizations. Followed by the 9/11 event, BCM gained worldwide attention. Organizations need to be prepared for disasters like these. Assuring business continuity is the goal of thinking about the prevention of or recovery from these events. Adverse events should not affect the business or at least as less as possible. BCM is there to take care of this wish. Smit (2005) uses the definition of Verdonck, Klooster and associates to define Business continuity management:

Business Continuity Management:

"Business Continuity Management encompasses the management process that aims to prevent severe disruptions in the business and to protect critical processes against the consequences of disruptions or disasters."

Smit (2005) agrees that this is the right definition for BCM because it encompasses the following four aspects:

- The aim of BCM is to ensure the continuity of the business at a certain minimum level
- BCM initiatives should be directed towards the critical business processes
- BCM encompasses both the prevention of disasters or disruption and limiting the damage to business in case of a disaster or disruption, so it has preventive, corrective and repressive characteristics
- BCM is a continuous management process, not a single project.

BCM covers nine sub domains that as a whole cover the focus area BCM. Organizations involved in BCM typically have a list of contact points in case of an adverse event. Hence, when a server has downtime, it is convenient to call the person responsible for the up-time of the servers right away instead of calling a help desk that puts you through. The other eight subdomains are: roles and responsibilities, risk levels, continuity and recovery service levels, business continuity reviews, business continuity processes, incident reporting and documentation, testing and training (Lam, 2002). How an organization deals with all nine points together determines their maturity (e.g. how the processes concerning these nine subdomains are organized).

BCM is one of the focus areas of information security, because the business needs to assure to their clients that every system works properly. I.e. A server having unexpected downtime can result in loss of money due to unsatisfied customers and/or data not available to personnel. Business always should be able to continue working, generating money and satisfying customers. BCM takes this into account and suggests, for this example, to have back-up servers in place at another building using a different connection. BCM takes care of this aspect of information security and is therefore not only part of the ISO27K standard but also part of this thesis as a focus area. The next section elaborates on the maturity levels of BCM.

5.11.1. Business Continuity Management Maturity

There are several ways to define a maturity model for BCM. A model by Getronics (De Ruiter, 2009) for example, uses the plan, do, check, act cycle. All phases in this cycle can be compared with maturity stages.

Plan	1.Scope 2.Goals 3.BCM policy 4.Communication 5.Resources 6.Training 7.Inbedding 8.Documentation 9.Control mechanisms
Do	1.Business impact analysis

	2.Risico assessment 3.BCM Strategy 4.BCM organization 5.Testing 6.Maintenance 7.Audit
Act	1.Internal audit 2.Research input 3.Research output
Check	1.Continuous improvement 2.Corrective actions 3.Preventive actions 4.Based on feedback!

Table 38: De Ruiter (2009) BCM maturity model

Another model is included in the BS 25999-1:2006 standard (British Standards institute, 2006). This standard also distinguishes four steps in a BCM lifecycle. First of all, an organization must understand their organization and wishes. Second, they need to formulate a BCM strategy that fits to their organization's strategy. When this is in place, the organization can start implementing and developing their Business Continuity Program. To guarantee business continuity over a longer period of time, the final step is continuously practicing, maintaining and reviewing the business continuity plan.

The last model discussed is of Smit (2005). Smit identifies six stages of maturity.

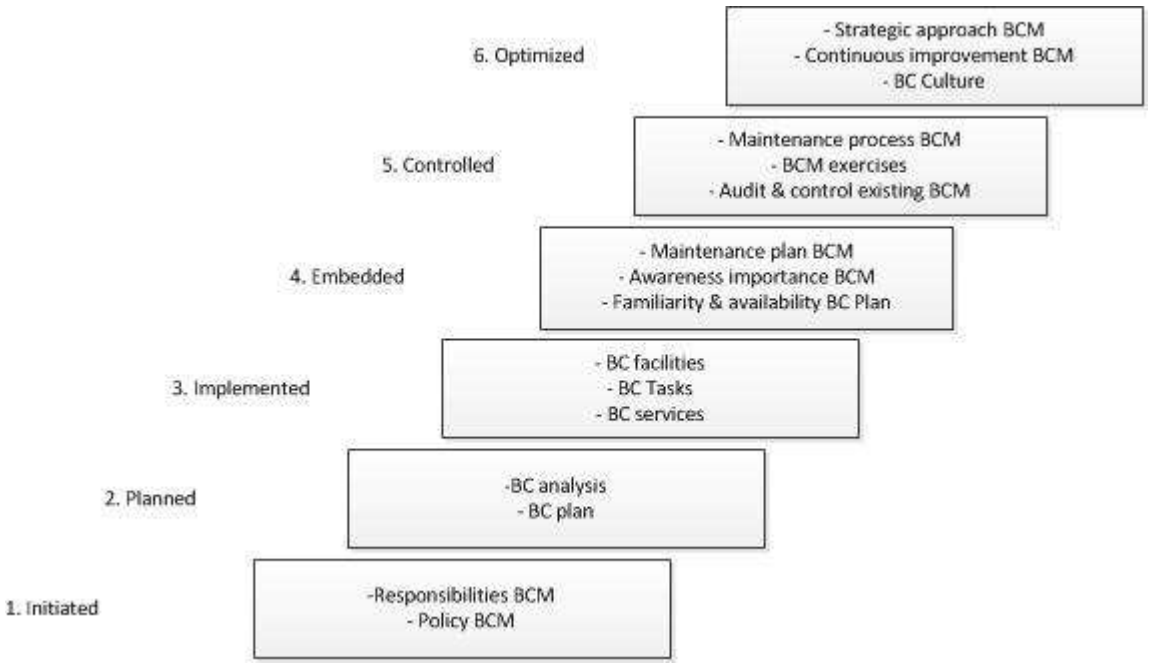

Figure 27: Business Continuity Management Maturity Model of Smit (2005)

Initiated: The first stage of the maturity model of Smit (2005) states that there needs to be formal management commitment of BCM within the organization. High roles are defined and a special BCM policy is in place.

Planned: An organization in the second stage has written all necessary Business Continuity plans. Before writing the plan, typically a Business Continuity Analysis has been performed. Critical applications and processes and consequences on failure are identified during this analysis.

Implemented: All plans written in the previous stage are implemented at this stage. BCM on paper is not satisfying and therefore BCM responsibilities are known by the employees and measures are used effectively to gain insight in their performance.

Embedded: BCM develops from a project into a process at this stage. A maintenance plan is made and there exists a small amount of awareness covering the whole organization.

Controlled: Organizations in level 5 are controlling their BCM by means of their maintenance plans. For most organizations this is seen as the most desired stage.

Optimized: BCM at this stage is a strategic instrument that can create commercial and competitive advantage. The organization seeks continuous optimization of their BCM.

The maturity model of Smit has been picked as the basis for this maturity model. The model presented in this thesis is a simplified representation of the original. Smit (2005) had her model evaluated by 30 expert consultants in the field of BCM. Therefor it is assumed that all statements within the model are correct and influence the maturity. However, there are statements involved containing more operational factors which are not necessary for the purpose of this thesis. Those have been left out of the simplified version used for this thesis.

5.11.2. Business Continuity Management maturity metrics

Table 39 shows the metrics that determine the maturity level of BCM. The maturity model has five levels due to the fact that a couple of capabilities could be moved to other maturity levels. This is partly due to the evaluation.

Capability /level	Statements	reference
A	1. BCM is performed by IT, OR B2 2. Senior management takes responsibility for BCM, OR C1, E1. 3. A formal BCM policy is developed.	Smit (2005)
B	1. All roles and responsibilities regarding BCM have been defined 2. BCM is performed by Business 3. A Business Impact Analysis is regularly performed	Smit (2005)
C	1. A formal Business Continuity Plan is designed 2. BCM processes and procedures are based on available standards 3. The organization tests the Business Continuity Plan by performing a walk through test.	Smit (2005)
D	1. The organization tests the Business Continuity Plan on a regular basis by simulating real events. 2. The BCM plan is internally reviewed, OR E1 3. A formal Business Continuity Plan is implemented	Smit (2005)
E	1. The Business Continuity Plan is regularly reviewed and changed bases on past events by a third party. 2. The BCM policy is regularly reviewed and updated	Smit (2005)

Table 39: ISFAM assessment statements for Business Continuity Management

5.11.3. Evaluation

To evaluate the initially proposed statements based on business continuity management literature, the Business Continuity Maturity model has been evaluated by an expert having more than eight years of experience in the field of business continuity. During these eight years he worked for several consultancy organizations delivering advice to their clients. As he is being familiar with maturity models and the different steps an organization should take to become mature, he is a knowledgeable person to evaluate this model.

Although the model has already been evaluated in 2005, I wanted to make sure that this is still a recent version and that is supports and reflects the business. The expert did not know the model of Smit and read the six levels and attached statements. Having done that, I explained the final model and the fact that not all maturity models need to be CMM based to create the model. His first remark is that it covers the most important topics of business continuity management, but that it needs some small additions and changes. I suggested walking through a couple of question before posting the other comments related to the model.

The first question addressed the amount of levels needed to represent the model. Although it is not CMM, the expert does agree with the amount of levels looking at the statements inside these levels. It is well structured and it makes sense to put this maturity model into six stages.

Secondly, we discussed whether there are statements missing or superfluous. What was missing in the model is the testing of a business continuity plan. According to the expert this can be done in two ways:

- A walkthrough test: Testing on paper what should happen when an adverse event occurs
- Simulation: Real-life testing of an event where the effect is visible.

As a second change he suggested to split up designing and implementing a formal Business Continuity Plan. In a CMM based model these stages are divided and while this model has more stages than the CMM standard model it makes sense to split this statement.

On the last question if there are any other comments he answered no. All comments he had at the start were covered during the conversation.

Action	Result
Add	C3: performing a walkthrough test
Add	D1: Simulation of a real event
Change	Added *a formal business continuity plan is implemented* at capability D3
Change	C1: removed *"and implemented"* in order to let design stay at capability C and move the implementation to capability D

Table 40: Overview of changes business continuity management

5.12. Compliance

All policies, laws and regulations that are developed following the maturity model for policy development are useful, but useless if you do not comply with them. Compliance is defined by the dictionary as: "The act of complying with a wish, request, or demand; acquiescence". In case of information security the wish, request or demand has to do with the organization's ambition towards maturing their information security and protecting their assets. Existing models and

standards are often used as a basis for improving this maturity level. However, the models themselves do not mature the organization; it is a combination of the models and the compliance with the models that influence the maturity.

The focus area Compliance for this thesis is intertwined with the focus area policy development. First a policy needs to be developed, second it is important to roll out and comply with that policy. Compliance for this thesis is defined as:

Compliance:
"The extent to which an organization meets and follows their information security policy and processes."

This is almost the same definition as given by a dictionary, except for the scope of the definition since this definition only addresses the field of information security.

Gabriel, R., Sowa, S. And Wiedemann, J. (2008) state compliance addresses legal, regulatory, and internal requirements relevant to the organization. In this case, it is a reference to the standards and laws related to information security. COBIT, ISO27K, and ITIL are examples of standards. The SOX law is an example of a law that organizations must follow to avoid fines and be trustworthy to their clients. As can be concluded from this paragraph, compliance does not only have a technical side, but also a socio-organizational (Bulgurcu, Cavusoglu and Benbasat, 2010). Successful compliance within an organization is therefore achieved by addressing both sides. Moreover, the socio-organizational side is more important than the technical side because the weakest link in information security is human behavior (Mitnick and Simon, 2002).

5.12.1. Compliance Maturity

Logically following the maturity model of policy development, this maturity should also have the same amount of maturity levels, since you first do a step forward in policy development and afterwards you comply with the new policies made. Compliance has three maturity stages.

Maturity level	Description
0- None	The organization has no idea about their compliance level. Also laws are not taken into consideration while doing their daily business
A- Ad hoc	The organization complies with laws and regulations and complies sometimes to policies since they are forced by systems or already part of their daily work
B- Defined	The organization complies to policies developed for the whole organization. On business line/department level there is less compliance to their specific policies.
C- Developed	The organization reviews their compliance level and is pro-actively improving it. This also included taking measures against violation of the policies.

Table 41: Compliance Maturity Model

5.12.2. Compliance maturity metrics

The compliance maturity statements are based on the policy development metrics. There is no formal reference available that states that these determine the level of compliance.

Capability /level	Statements	Reference
A	1. The organization complies with all applicable laws and regulations 2. Management complies with the organization's policy	NA
B	1. All employees are aware of their roles and responsibilities concerning information security 2. All policies are written using the formal style	NA
C	1. The organization complies with/is certified based on applicable standards 2. All employees comply with the policies of the organization 3. Employees are timely informed about changes in the policy	NA

Table 42: ISFAM assessment statement for Compliance

5.12.3. Evaluation

During the evaluation of the compliance maturity model I interviewed an expert who has over 3 years of experience at a financial institution with policies and compliancy. Before asking him any further question detailing the model, I explained him the final model and the relationship of compliance with the focus area policy development. He agreed that a policy first has to be developed before an organization can comply with anything. Based on the maturity levels of policy development, he mentioned that it is a good way to look at compliance and policy development as two dependent focus areas. Next he reviewed the relation between the different statements and found that no major changes are needed to the amount of maturity levels or the statements in which the statements are placed. Some small remarks were made about the wording of statements. Having changed that, he agreed upon the model and thought it was a good representation of how it works in practice.

5.13. Information security architecture

Information Security Architecture is part of enterprise and IT architecture. Information Security Architecture addresses the construction and design of computers, communication networks and the distributed business systems that are implemented for information security technologies (Sherwood, Clark & Lynas, 2009). The aim of information security architecture is to increase the effectiveness with which these computers, networks, etc. are implemented (Eloff & Eloff, 2005). To make an Information Security Architecture effective it at least has to take care of:

- The goals that need to be achieved through the systems
- The environment
- The technical statements necessary to control the systems

The focus of the security architect is enforcement of security policies of the enterprise without inhibiting value. Security within architecture is often overseen because it is not visible to the business (The Open Group, 2011a). The purpose of securing your architecture is to protect the value of the systems and the information assets. Most of the times, security architecture does not receive a lot of attention since organizations do not pay attention to it as long as no data has been leaked.

One way to improve this focus area within an organization is inside-out. Starting with the architectural protection of your core assets and improving towards a cross-organizational architecture is a common choice for organizations. As in other focus areas, this is done by deriving

controls from architecture policies. This process can be matured by using specific tooling enabling the organization to review and improve the security status of the architecture. The Open Group (2011a) made the TOGAF framework used for developing enterprise architecture. This process includes security and is therefore used as a guideline for this focus area.

5.13.1. Information Security Architecture Maturity

Defining maturity stages for this subdomain requires a look at enterprise and IT architecture. The US Department of Commerce (The Open Group, 2011b) developed a 5 staged maturity model for IT architecture. IT security, as it is part of information security, is a subdomain within this maturity model. IT security architecture maturity is defined in the following six stages:

0- Not defined
A- IT security considerations are ad hoc and localized.
B- IT security architecture has defined clear roles and responsibilities.
C- IT security architecture Standards Profile is fully developed and is integrated with IT architecture.
D- Performance metrics associated with IT security architecture are captured.
E- Feedback from IT security architecture metrics is used to drive architecture process improvements.

These five improvement steps in Information Security Architecture go along with metrics and activities necessary to reach that maturity level. A focus area maturity model allows having less or more than six maturity levels. Therefore a closer look is taken at the different stages and the need for them.

Not defined – Always maturity level 0 in the focus area maturity model and therefore no need for change.

IT security considerations are ad hoc and localized – This indicates that there is not a structured architecture in place for the whole organization but that there are some local or departmental initiatives for information security architecture.

IT security architecture has defined clear roles and responsibilities – From a more local level of information security architecture now reaches an organization wide arranged level with defined roles and responsibilities. This is a logical step forward and therefore a good second maturity level.

IT security architecture Standards Profile is fully developed and is integrated with IT architecture – This stage is about the full adoption of an IT security architecture standard. It is an addition to the previous maturity level and therefore considered as good.

Performance metrics associated with IT security architecture are captured – This maturity level can be integrated with the previous level. It adds performance metrics which can also be made part of a standard.

Feedback from IT security architecture metrics is used to drive architecture process improvements – This is the optimization step where the architecture supports your organization in an optimized way.

The concept for Information Security Architecture maturity has five stages including the not defined stage. The metrics now presented are combined with the stages to form the final maturity levels for Information Security Architecture.

The metrics are derived from literature covering enterprise architecture, IT architecture and information security architecture.

5.13.2. Information Security Architecture Maturity metrics

To determine the level of Information Security Architecture Maturity the metrics in table 43 have been identified.

Capability /level	Statements	Reference
A	1. On a departmental level someone takes the responsibility for architecture, although that person might not be familiar with security	
B	1. There is a formal information security architect role within the organization 2. A formal policy is in place regarding information security architecture. 3. A defense-in-depth approach has been designed	
C	1. Architectural development is based on a standard or framework 2. Metrics have been defined to monitor the effectiveness of the current architecture 3. A defense-in-depth approach has been implemented 4. The architecture is audited/penetration tested on a regular basis	
D	1. Architecture supports the business in an optimized way 2. The architecture of the organization is continuously updated. 3. The organization uses building blocks in order to set up and change their architecture	

Table 43: ISFAM assessment statements for Information security architecture

5.13.3. Evaluation

An expert performing penetration tests and giving advice on network structures for over five years evaluated this model. Since little literature was available on a maturity model for information security architecture, I did not show any premade model and asked how an organization can develop their information security architecture starting with an organization that has not thought about architecture. The expert explained the process of developing architecture with respect to the development of a maturity model. He therefore referred to the architecture model of The Open Group (2011b).

Capability A is mostly defined by someone picking up architecture as something that needs to be managed and maintained. This person does not necessarily think about providing this architecture in a secure way. Along the way of development (capability B), an information security architect is appointed that needs to take make sure that no hackers or other malicious persons can steal away data. To harden the architecture a defense-in-depth concept, comparable to the security zones concept of physical security, can be implemented. Instead of physical security it is now about IT security and the usage of hardware and software to protect sensitive data. At capability B this

concept is designed for the organization and at capability C this concept is implemented. At capability D it becomes important that the architecture supports the business (e.g. prevent downtime, communicate about issues, etc.). Besides that architecture should be seen as a process and not as a one-time issue.

The expert told that the most mature companies try to manage their architecture using building blocks. Building blocks are part of the architecture that are tested and considered to be secure. Attaching different building blocks to each other makes the final architecture. The only thing that needs testing in this scenario is the communication between the two different building blocks.

6. ISFAM Model

This chapter elaborates on the steps taken to construct the final model, called the ISFAM (Information Security Focus Area Maturity model). To present and combine thirteen maturity models into one model, the first step is to make a categorization. The categorization of the thirteen focus areas has as goal to create a better understandable model than without categorization. For this model, four categories have been identified:

- Organizational: This category comprises focus areas that are organizational oriented and are mostly characterized by organizational statements rather than technical.
- Technical: This category comprises focus areas that are technical oriented. It means that the statements often require a technical implementation or the focus area represents the technical implementation of an organizational focus area. Statements occurring in most of the focus area are left out (e.g. statements dealing with roles and responsibilities, policies, etc.)
- Organizational and Technical: This category comprises focus areas that require both technical as well as organizational statements to become mature.
- Support: This category comprises focus areas supporting the other focus areas in becoming more mature. Focus areas mentioned in this category are part of the defense-in-depth concept. Defense-in-depth means that your organization should be secured on different levels. Defense-in-depth can be explained using a castle as metaphor. A castle has a moat, but when the enemy is able to pass the moat, there is still a thick wall they need to climb over or break through. The same should count for an organization. An attacker can physically enter a building, but when the attacker needs a badge to enter it becomes more difficult. When he succeeds in passing this barrier, there is still the option to secure your network, and even on a lower level the valuable data itself.

Translating the following categorization into the final model results in the model shown below:

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management													
Policy Development													
Organizing Information Security													
Human Resource Security													
Compliance													
Technical													
Identity and access management													
Secure software development													
Organizational and Technical													
Incident management													
Business Continuity Management													
Change Management													
Support													
Physical and environmental security													
Asset Management													
Architecture													

Figure 28: The conceptual ISFAM model

The next two paragraphs each describe one step in the process of mapping the capabilities onto the ISFAM model. The two different steps taken are:

- Identification of dependencies
- Deducible dependencies

Combining these steps led to the conceptual version of the ISFAM model:

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		

Figure 29: Conceptual version of the ISFAM Model

6.1.Identification of dependencies

After defining the focus area, the next step in building the ISFAM model is identifying dependencies and mapping them onto the model. The blue arrows in figure 30 show dependencies found in literature. A table containing all dependencies found in literature can be found in table 44.

Eleven arrows are leaving capability A (#1-11) of Organizing information security. This capability consists out of three statements:

- There is senior management commitment to information security
- Management makes sufficient resources available to address information security
- Management is formally responsible for all policies

According to Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003) the implementation of an information security program starts with management commitment and having sufficient resources available. Therefore, no other capability can be placed before capability A of organizing information security.

Second, there is an arrow moving from risk management capability A and to policy development capability B (arrow #12). This has to do with the so-called risk based approach Discini (2006). As a start, policies involving applicable laws and regulations are important. When moving on, an organization should not only take these into account, but also their risks. Risk management capability A makes sure that you identify risks that might affect your organization. Based on these risks, the policies can be changed (arrow from risk management capability A to policy development capability B). For the same reason, there is a dependency between risk management capability B and policy development capability C (arrow #13).

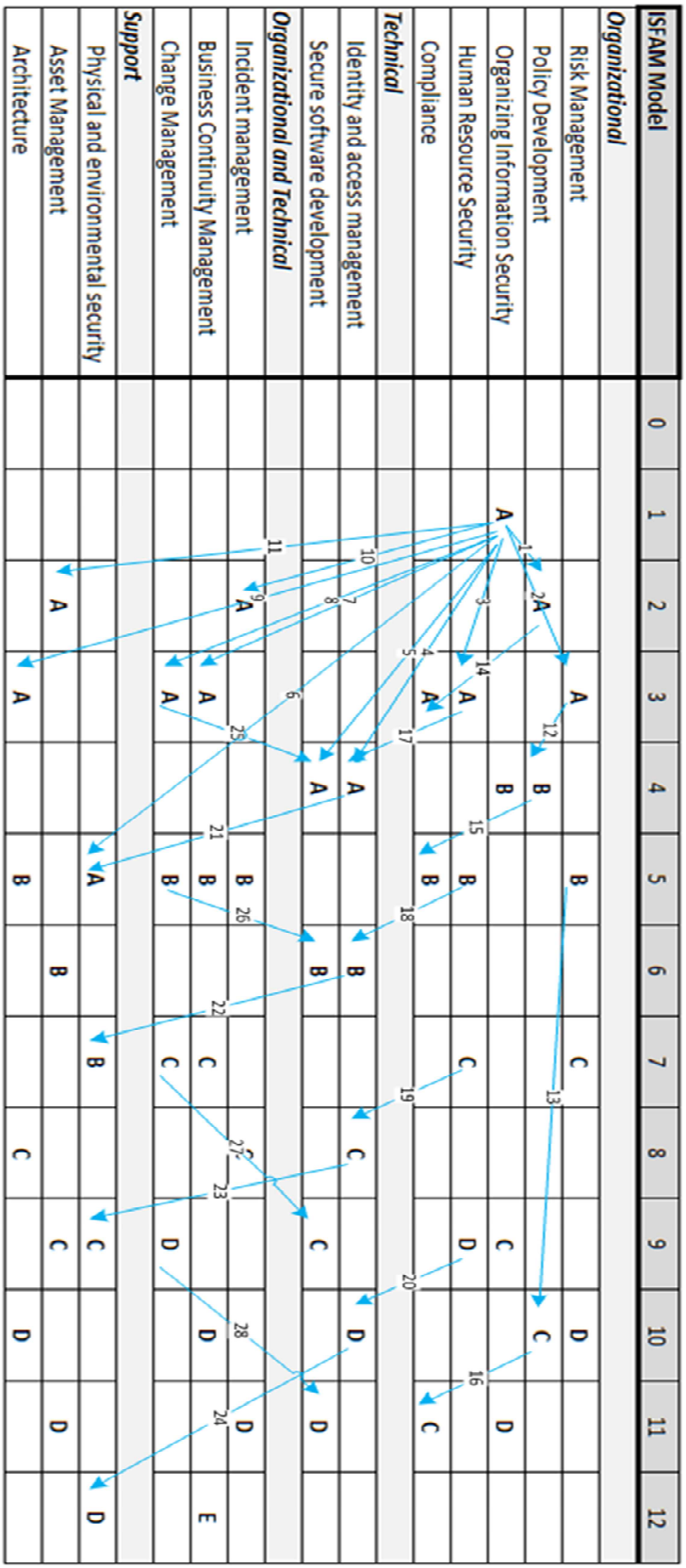

Figure 30: Dependencies in the ISFAM model

Third, there is a dependency between policy development and compliance. A policy needs to be developed before you can comply with something. Höne and Eloff (2002) mention in their paper that most policies are written to comply with applicable laws and regulations. In addition, compliance in a mature state should also include an organization's own policies. This results into three arrows going from policy development to compliance (arrow #14-16).

Fourth, there need to be some organizational implementations before the related technical part can be implemented. In this case, human resource security is related to identity and access management (arrow #17-20) and change management is related to secure software development (arrow #25-28). Since all the involved focus areas are CMM based, the dependency is marked as one on one. Identity and access management can be seen as the technical implementation of human resource security (The institute of internal auditors, 2007). Hence, a person enters an organization and afterwards that employee receives roles and rights for several systems. Change management and secure software development are related in the same way (ISC^2, 2012). Without change management, secure software development cannot exist in a mature manner. In addition, physical and environmental security can be seen as an implementation of identity and access management. Physical and environmental security is partly dependent on identity and access management (arrow #21-25) . The policies written for physical and environmental security should reflect the policies for identity and access management. For example, access to a server room should only be granted to server administrators. This means that the server room has valuable information inside and needs to be protected physically as well as logically (Gergi, 2010). Physically by, for example, needing a fingerprint and logically by having the rights in the system to access the server. In addition, because the information is valuable, the organization should take the right measures to reduce the chance or impact of environmental risks.

#	From	To	Reference
1	Organizing A	Policy development A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
2	Organizing A	Risk Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
3	Organizing A	Human Resources Security A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
4	Organizing A	Identity & Access Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
5	Organizing A	Secure Software Development A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
6	Organizing A	Physical & Environmental Security A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
7	Organizing A	Business Continuity Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
8	Organizing A	Change Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
9	Organizing A	Architecture A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
10	Organizing A	Incident Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)
11	Organizing A	Asset Management A	Solms (2006) and Kankanhalli, Teo, Tan and Wei (2003)

12	Risk Management A	Policy Development B	Discini (2006)
13	Risk Management B	Policy Development C	Discini (2006)
14	Policy Development A	Compliance A	Höne and Eloff (2002)
15	Policy Development B	Compliance B	Höne and Eloff (2002)
16	Policy Development C	Compliance C	Höne and Eloff (2002)
17	Human Resource Security A	Identity and Access Management A	The Institute of Internal Auditors (2007)
18	Human Resource Security B	Identity and Access Management B	The Institute of Internal Auditors (2007)
19	Human Resource Security C	Identity and Access Management C	The Institute of Internal Auditors (2007)
20	Human Resource Security D	Identity and Access Management D	The Institute of Internal Auditors (2007)
21	Identity and Access Management A	Physical and Environmental security A	Gergi (2010)
22	Identity and Access Management B	Physical and Environmental security A	Gergi (2010)
23	Identity and Access Management C	Physical and Environmental security A	Gergi (2010)
24	Identity and Access Management D	Physical and Environmental security A	Gergi (2010)
25	Change Management A	Secure Software Development A	ISC^2(2012)
26	Change Management B	Secure Software Development B	ISC^2(2012)
27	Change Management C	Secure Software Development C	ISC^2(2012)
28	Change Management D	Secure Software Development D	ISC^2(2012)

Table 44: Dependencies derived from literature

6.2.Deducible dependencies

Deducible dependencies are dependencies that make sense or are derived from a top-down approach. Figure 31 shows these dependencies.

To ensure consistency throughout the organization, policy guidelines have to be established on a high level before policies can be established for every other single focus area (arrow #1-10). Implementing and developing policies in a top-down manner makes sure that, if strategy is included in the high level policy, the strategy of the organization is also drilled down to the rest of the organization. A line of policy development A is therefore linked to other capabilities where one of the statements refers to the development of the policy for that specific focus area.

The other important capability is organization of information security B. This capability is about identifying and defining roles and responsibilities. Following a top-down approach, it makes sense to first define the roles and responsibilities on a high level within the organization (arrow #11-21). After this phase, roles and responsibilities can be defined for every focus area in line with the previously, high level defined roles and responsibilities.

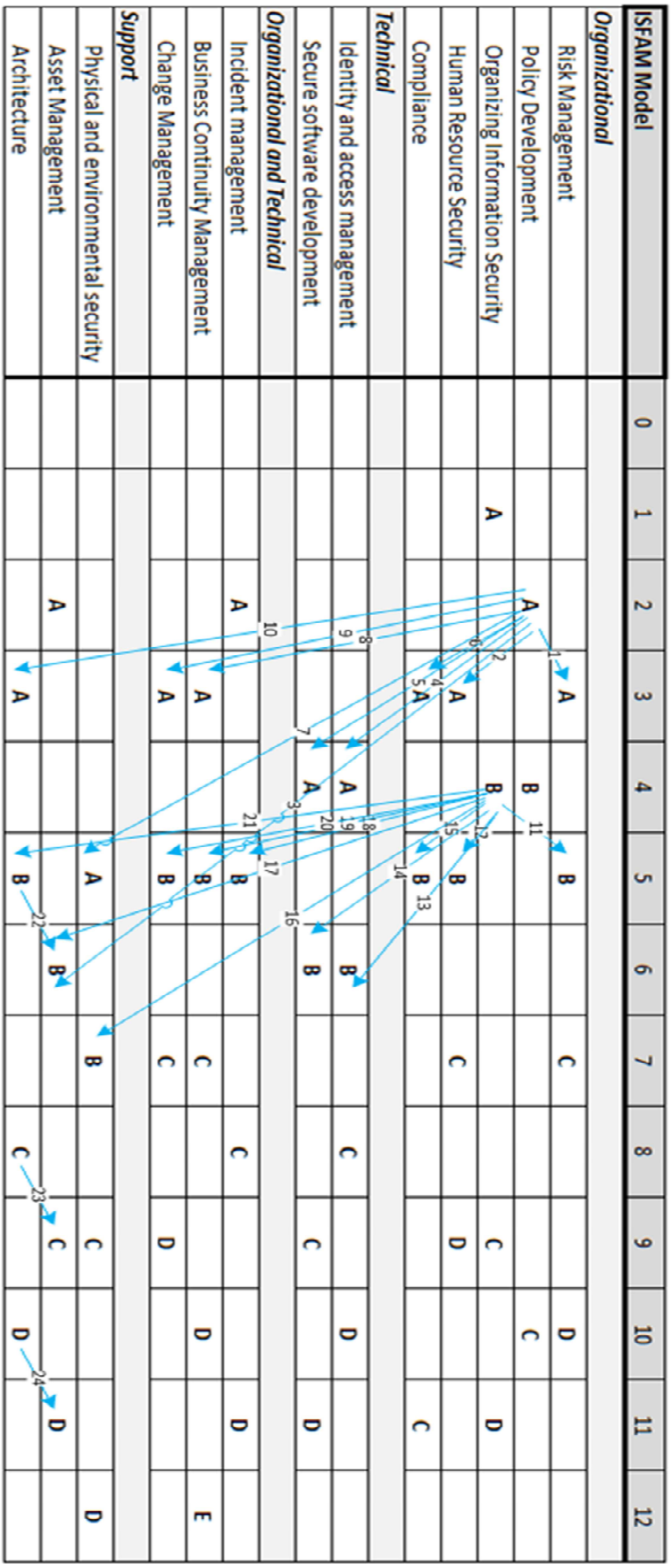

Figure 31: Deducible dependencies in the ISFAM model

The last dependencies shown in this model is the dependency between architecture and asset management (arrow #22-24). Normally, you will first have an architecture or infrastructure in place and then you start thinking about managing your architecture/IT infrastructure in an inventory list. For this reason, architecture is placed before the asset management capabilities. Nonetheless, recognizing the importance of managing your assets is more important than having an employee formally responsible for your architecture because assets directly affect your income statement. Therefore, the relation between the first capability of both focus areas is exactly the opposite of the preceding capabilities. Note, this does not mean that there is a dependency between the two focus areas.

Capabilities that are not addressed by arrows defined in section 6.2 or 6.3 are set up based on common sense and interviews held for every focus area. For example, business continuity management E and physical and environmental security D are not in place for a lot of companies and have been placed at level 12.

#	From	To
1	Policy Development A	Risk Management A
2	Policy Development A	Human Resources Security A
3	Policy Development A	Asset Management B
4	Policy Development A	Identity & Access Management A
5	Policy Development A	Secure Software Development A
6	Policy Development A	Compliance A
7	Policy Development A	Physical & Environmental Security A
8	Policy Development A	Business Continuity Management A
9	Policy Development A	Change Management A
10	Policy Development A	Architecture A
11	Organizing B	Risk Management B
12	Organizing B	Human Resource security B
13	Organizing B	Identity and Access Management B
14	Organizing B	Secure Software Development B
15	Organizing B	Compliance B
16	Organizing B	Physical and Environmental Security B
17	Organizing B	Asset Management B
18	Organizing B	Incident Management B
19	Organizing B	Business Continuity Management B
20	Organizing B	Change Management B
21	Organizing B	Physical and Environmental security A
22	Architecture B	Asset Management B
23	Architecture C	Asset Management C
24	Architecture D	Asset Management D

Table 45: Overview of deducible dependencies

7. Evaluation

The evaluation of the ISFAM model has been carried out using the evaluation method of Yin (2003). Various aspects around case studies are elaborated on in this book. Case studies are used as research strategies to confirm decisions/results derived from research done.

There are four different tests recognized by Yin (2003)

- Construct validity: establishing correct measures that reflect the question
- Internal validity: establishing of a causal relationship
- External validity: establishing a domain to which the study can be generalized
- Reliability: Demonstrate that the study can be repeated with the same results.

For this particular research the construct validity test has been selected since the goal is to evaluate the final model, the statements within this model, dependencies (only the ones touched by the results of the assessment) and the result of the assessment. This implicates that the informants should review the initial case study report.

Beside the type of test, there is also a distinction in two dimensions resulting into four quadrants:

- Single-case or multiple-case: The single case study is an appropriate choice under various circumstances such as unique cases, extreme cases or typical cases. Multiple-case design is often more robust (Herriott & Firestone, 1983) and is often used for comparison or replication.
- Holistic or embedded: the difference between holistic and embedded is that the embedded case studies take into account several subunits whereas holistic takes the global nature of an organization as viewpoint. Using embedded case studies results in one or multiple case studies with embedded units within the case which can all have distinct results.

For this study, the single case study with a holistic view has been selected. The holistic case study design has been selected because the model is evaluated for the whole organization and no distinction has been made between various departments. The single case study design is selected because of the uniqueness of the model. The ISFAM model is evaluated by a small/medium sized telecom organization. Applying the ISFAM model in another industry with a different headcount might result in a different result of the evaluation and therefore a slightly different model. In other words, two case studies might be conflicting in such a way that it is not possible to make one generic model for every organization. Only one organization has been picked for this research with as goal to prove that the conceptual ISFAM model is capable of representing an organization's maturity level, enabling an organization to develop an information security program and to verify whether capabilities are placed in the right order in the ISFAM model.

The relatively young organization operates across the globe but has its headquarters located in the Netherlands. Interesting about this company is that it seriously started improving their information security a couple of years ago. Before, they were also concerned about security, but did not formalize the processes around it. Their reason to join the evaluation is to verify their current status and create an improvement plan for the future.

For the evaluation I sat together with two managers of the company. Together they are responsible for the security within the company and able to answer the questionnaire within the tool. Because they discussed and answered the questions together, the answers are validated and I could observe

if the managers would become more aligned in knowing from each other what they are doing as well as their ability to communicate the final results back to business.

I started with introducing the model and the questionnaire to the managers. I explained them that there are 162 statements divided over 13 focus areas, together forming the maturity model. The statements within the focus areas are attached to a capability and when all statements of a capability are answered with yes, you are on that level for that specific focus area. The capabilities in the final model are placed using dependencies that represent the most ideal situation of setting up your information security roadmap. Level 1 would mean that almost nothing is done and level 12 would represent that you have thought about every part of information security, although it might not be implemented correctly. The model is not on an operational level, meaning that it would tell you what to do on a detailed level), but more on a "have you thought about this" level. For example, it does not state that you need an Information Security Architect, but it would ask whether all roles and responsibilities have been defined which could include an Information Security Architect depending on the type and size of the organization.

The ISFAM model is considered to be successful if the following points can be verified:

- The total analysis can be performed within a four hour timeframe – the model needs to be lightweight and easy to use within organizations. Four hours has been set as a limit for the questionnaire and analysis of the results.
- All questions make sense - questions should unambiguous and easy to understand. This prevents employees from having different opinions about the answer on a question and therefore being unaligned.
- The organization recognizes itself in the result - the most important aspect of the model is its capability to represent the information security maturity level of an organization. Reviewing the results of the ISFAM model should result in recognition.
- Dependencies that influence the result of this model need to be correct –Dependencies can always be changed based on changes over time, differences between industries and size of the organization. Therefore a full evaluation of all dependencies is not necessary for this study. The organization should however agree upon their next steps according to the ISFAM model. For example, the model suggests that they first have to work on incident management and next on identity and access management. The organization looks at the statements within the capability not yet reached and decide whether the improvement steps are placed in the right order or not.

Before they started the questionnaire I wrote down the time to make sure it is still a light weight self-assessment tool and not an intensive, more than four hours requiring, organization analyzer. They started with the questionnaire and answered most questions without discussion. Some questions they had a small discussion and a few questions were not correctly formulated. These questions were mainly about specific roles that do not exist in a small or medium sized company. There is not really a difference between senior management and the board and there might not even be difference between senior management and management. Therefore, they recommended naming all these similar roles to senior management because this is a familiar term to organizations. Next, they also recommended changing the layout of the questionnaire. Every row in the tool had a white background instead of switching colors every row and that makes answering the questions harder (e.g. less readable). This might result in answer and question fields in the tool might not be

corresponding at the end. Further, they liked the questions and saw the similarity with audit questions although audit questions are more detailed.

When they finished the questionnaire, we discussed the results. The results were not surprising to the managers and already on forehand they mentioned that they lack in the documentation of policies. They recognized this in the final result, because policy development was still at capability A and they could not meet the requirements to go to capability B. The same holds for other areas. When they do not meet the requirements for capability A, they do not have a policy in that area or at least it is not formal. However, when reviewing the statements for capability B and C in more detail, they might have answered some questions with yes, because they do have implemented security measures, but did not formally document their processes and policies.

The two managers discussed the result and were wondering how they could refer the results back to the yearly IT audit. Since the model is a self-assessment I answered that this result will never be used by auditors because they need to see and check the controls with their own eyes. A self-assessment is not considered as valid evidence. The question was asked because one of the managers recognized an audit pattern in it. Usually an audit contains four stages of control (Singleton, 2009). First there is design, in which you would set up your policies. Second, there is implementation where the company implemented processes related to the policies. Third stage is the operational effectiveness where the company can demonstrate that there processes work properly. Last stage is monitoring where the organization takes changes of the environment into account to add, change or delete controls. These stages can be mapped onto the maturity model:

- Level 0 – 4: Design
  Most capabilities in this range address developing a policy and cover the stage where an auditor would test on design. When the design is in order, the organization should be at least level 4.
- Level 5 – 6: Implementation
  At this stage you will mostly find capabilities that cover questions covering questions about roles and responsibilities and developing standardized processes. If the organization has all process in place, it should be around level 6.
- Level 7 - 9: Operational effectiveness
  From level 7 to 9 the organization is able to demonstrate that the processes are implemented and work as designed. Typically, an organization would be around level 9 when all processes work according the procedures designed at the existence stage.
- Level 10 – 12: Monitoring
  This stage does not exist for an auditor, because it is an action he is performing on the first three stages. An organization can review their own processes and procedures by performing an internal audit in which they would audit the first three stages. Based on the results the organization can update their policies, procedures and processes.

Concluding, they said they liked the model and are planning to re-assess themselves before the next year-end audit to make sure that all questions behind the A capabilities can be answered with yes. This will be the first milestone for them in the road to becoming a mature information security organization. As a next step one of the managers said it would be nice to include activities behind

every capability. This way it becomes easier for them to get sufficient resources available for the appropriate actions that need to be taken in order to become more mature.

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		
	Design					Implementation		Operationel Effectiveness			Monitoring		

Figure 32: Result of the evaluation

To enhance the completeness and accuracy of this case study I sent the draft version of the case study back to the organization for a review. The two managers agreed upon the results and the draft and did not require anything to be changed.

To evaluate the case study it is not only of significant importance that the organization agrees upon the results but also that the goals previously described are met:

- The total analysis can be performed within four hours – this goal has been met. It took about three hours in total to evaluate the ISFAM model including answering the entire questionnaire
- All questions make sense – with the feedback received from the organization regarding the roles in small to medium sized organizations the model and questionnaire have been changed. According to the organization the questions were easy to understand and with the additional changes made, the questions became unambiguous as well. This goal has therefore been reached.
- The organization recognizes itself in the results – during the review of the results the organization recognized themselves in this result. They know additional effort has to be put in formalizing their processes and policies. According to their maturity level reached (level 1) they are in the design phase which corresponds to their view on their business.
- Dependencies that influence the result of this model need to be – The next point of attention according to the result of the model has to be incident management (see figure 32). Since the organization did not have anything in place for incident management they acknowledged this fact. They also agreed upon the fact that it should be one of the first areas to focus at. While discussing the results they did agree with the order as it is now, although they do think that another organization within a different sector could have different requirements and might not pick the order as suggested by the model. I answered that this indeed can be the case and that every organization will be at a different level requiring different actions which they are likely to perform in a different order. However, with this model they do have a guideline of what is advised to be done first. In this case, it would for example not make sense to bring the organization of information security focus area to level D, while incident management did not even reach capability A.

8. Conclusions and discussion

This chapter refers back to the start of this research where the research questions were defined. First, the sub questions are answered, followed by the two main questions. After elaborating on the final result of this thesis project, the second section of this chapter points out the limitations of this research and possibilities for further research.

8.1.Conclusions

Looking back at the whole research process it is now time to look back at the sub- and main questions defined at the start of this project. The two main questions were separated in a business and scientific objective. For science:

"How and by what means can the gap between business requirements with respect to information security and the actual level of Information security be minimized or closed?"

The objective for the business was:

"Providing a method/tool that enables companies and organizations to increase their information security level in a structured and effective way."

The main research questions were divided into five sub questions stated below.

Sub questions:

1. *"What are the focus areas in the information security domain?"*
2. *"What are applicable metrics to measure the information security focus areas?"*
3. *"Is it possible to define a maturity scale for the different focus areas and if so how are they defined?"*
4. *"How can the maturity of information security be modeled?"*
5. *"What would be an appropriate distribution for the maturity stages?"*

Starting with the first main research questions it was determined in chapter 4 that a maturity model would suit best to minimize or close the gap as presented in the first research question. Based on this information the five sub questions were defined.

What are the focus areas in the information security domain?

This question was used to determine the different focus areas needed for the final ISFAM model. Combining several standards, certificates and methods led to a total amount of thirteen focus areas. 12 translated from the ISO27k standard and architecture as an additional focus area as it was involved in the other models.

What are applicable metrics to measure the information security focus area?

To make sure the model can be used by the business it was important to make every focus area measurable. Besides, the ISFAM model needed to be as simple as possible in order to not take a lot

of time from the business to determine their current status. Combining both requirements led to 161 metrics that are represented as yes/no statements. Answering the 161 statements takes 3 hours at most and fulfills the requirement of an efficient and quick model. The statements have been based on literature, existing maturity models for the different focus areas and the evaluations done with experts that gave the ISFAM model additional business value.

Is it possible to define a maturity scale for the different focus areas and if so how are they defined?

Chapter 5 discusses the 13 focus areas separately. First, the meaning and concept of the focus area is elaborated on. Next, it was possible to find maturity models in literature or define a maturity model taking the CMM levels as a basis for every focus area. To ensure added value for the business one expert interview per focus area has been held.

How can the maturity of information security be modeled and what would be an appropriate distribution for the maturity stages?

The 13 focus areas, their capabilities and the statements within the capabilities needed to be compared and ordered to fit into the final ISFAM model. This was done in three steps. First the capabilities were placed in the model using dependencies found in literature. Secondly, deducible dependencies are identified together with information gathered from the various interviews. To make sure the model could be used by small and medium sized organization an assessment tool has been made. This assessment tool has been evaluated by an organization that recognizes the importance of information security, but did not know where to start improving their information security.

Now the five sub questions have been answered, the two main questions can be answered by combining the sub questions. The scientific research question addressing the gap between information security business requirements and the actual level of information security can be answered with the ISFAM model that has been made during this research. During the assessment two managers sat together and discussed the measures they had in place to ensure the security of their data. They could, by discussing the 161 statements, determine their actual level of information security. They agreed upon the results of the ISFAM assessment and therefore the model can be seen as a good way to determine your information security maturity on a high level. On the other hand, with this result they confirmed that it is easier for them to make budget available for information security. Reason for this is that the model provides high level advice on what to do next. For them it is therefore easier to make a more specific information security program stating what they exactly want to do in the coming years. Thereby it is possible to make more budget available for the right actions that need to be taken in order to become more mature. Over a longer period of time this will result into a smaller gap between the actual level of information security maturity and business requirements.

The business objective was to provide a tool for the business that enables organizations to improve their information security maturity in a structured and effective way. During this research an assessment tool has been made to determine the maturity level of the organization. It the previous paragraph it was already clear that the model makes it easier for management to make more budget available. Inherent to the model and the fact that management is able to make more resources available demonstrates that the model at least is a structured way of improving the information

security maturity level. The expectation is that it will also be an effective way, because the organization will know where to focus at next. However, since there have not yet been any follow-up actions based on the model it is impossible to make this conclusion at this moment.

ISFAM Model	0	1	2	3	4	5	6	7	8	9	10	11	12
Organizational													
Risk Management				A		B		C			D		
Policy Development			A		B						C		
Organizing Information Security		A			B					C		D	
Human Resource Security				A		B		C		D			
Compliance				A		B						C	
Technical													
Identity and access management					A		B		C		D		
Secure software development					A		B			C		D	
Organizational and Technical													
Incident management			A			B			C			D	
Business Continuity Management				A		B		C			D		E
Change Management				A		B		C		D			
Support													
Physical and environmental security						A		B		C			D
Asset Management			A				B			C		D	
Architecture				A		B			C		D		
	Design					Implementation		Operationel Effectiveness			Monitoring		

figure 33 : The final ISFAM model

8.2.Further research and discussion

Based on feedback regarding the model, assessment tool and followed approach there are discussion points that need to be addressed. First of all, it is unclear what will happen to the model in the coming five years. It might be the case that new developments (i.e. cloud computing, mobile security and cyber security) in the domain of Information Technology results in rigorous changes to the model. The model could therefore not be time resistant. Next to that, it is also not sure if the model holds for all organizations. Different organizations in different sectors with different sizes have different issues on their mind at a different moment in time. Although the model worked for a small/medium sized telecom, media and technology organization, it does not have to be the same for financial organizations. Performing more assessments at different organizations and repeat these assessments after half a year will eventually result in a solid model that might even be able to illustrate the differences per sector in addressing information security.

Another point open for discussion is benchmarking versus tailor-made assessments. In this thesis it was decided to keep as much benchmarking value as possible by not adding industry specific characteristics. By doing so, it might be that the guideline and alignment capability of the model is less accurate. Additionally, the benchmarking value of the ISFAM model has not yet been proven. By evaluating the model at only one organization, not many dependencies have been covered. In this thesis, no absolute certainty can be given about the practical applicability of the dependencies situated in the higher maturity levels of the organization.

Third point of attention is the visualization of the results. For now, it is done using the representation as proposed by Steenbergen et al. (2009). However, from a business perspective it is more valuable to represent this model in a spider chart since most managers are familiar with such type of representation.

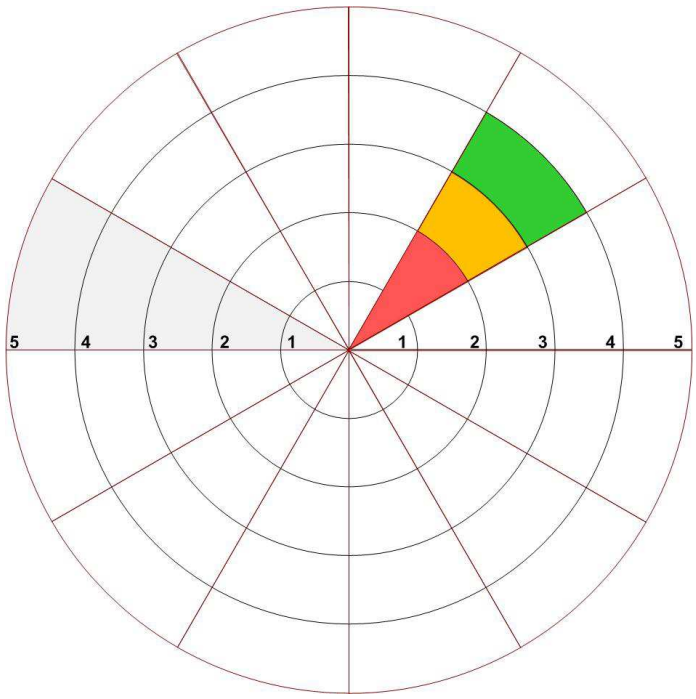

Figure 33: Spider Chart

The spider chart depicted in figure 33 is an example of a representation known to the business. In this particular case there are three levels in the spider chart. For the ISFAM model, twelve levels would have to be made and the thirteen focus areas would be represented by thirteen “pieces of pie”. The grey color can indicate that a certain focus area is out of scope for that company. This might happen if one of the focus areas is not applicable to the company or that they just know that they did not pay any attention to that area so far. The red, orange and green color provide an improvement path: red being the history, orange the level that is current and green the level where you want to be in the future.

Attached to this visualization issue is the availability of follow-up actions given by the model. As further research it would be interesting to give the organization steps they should take in order to increase their maturity level.

Besides the previous discussion points, there is also something to be discussed regarding the scope and extendibility of this model. The model is suitable for a high level assessment. It is less or not suitable for a detailed, more operational analysis that can assist auditors on a daily basis. For further research and discussion it would be interesting to turn this model into several or one larger maturity model that would be able to help auditors. This would also imply that the assessment tool would change from a self-assessment towards an auditor-assessment. The value gained by keeping the model easy and fast would then be lost, because the assessment will probably require multiple employees to deliver evidence. On the other hand it will gain value, because the model will also be usable for larger organizations. Hence, large organizations might have a lot in place in the ISFAM model, but when looking more in depth there might be some small remarks. Second, there is the extendibility of the maturity model. The ISFAM model is easy to extend with new focus areas. However, introducing additional capabilities can require the replacement of other capabilities which eventually can end up in a messy situation.

For further research it would be interesting to look at emerging technologies that might affect security such as cloud computing and mobile security. When the traditional IT landscape is replaced security standards change as well, and so might the model.

Last point of further research and discussion considers the alignment between IT and business. The ISFAM model has been evaluated by two persons from one organization that discussed together whether questions should be answered with yes or no. Although they did not always agree on the answers, they seemed to be on the same page. It is useful that they discovered some points where they did not agree at once; because that implicates that they do not know everything of the organization and need more persons to determine what their current maturity level is. For alignment purposes it would provide additional value if the model is also evaluated at non-IT focused organizations. The organization used for this thesis uses and provides IT services to make profit and are probably better in aligning business and IT. It would be interesting to look at organizations in other industries to see whether they align business and IT to the same extent and if so, how it would reflect in the discussion. Another option would be to let two employees perform the assessment on their own and afterwards compare the results and take that information to a discussion.

9. References

Alger, J.I. (2001). On Assurance, Measures, and Metrics: Definitions and Approaches. *Applied Computer Security Associates Workshop on Information-Security-System Rating and Ranking, 1*(No issue).

Appel, W., 2000. Architecture Capability Assessment. *Enterprise Planning and Architecture Strategies*, *4*(7).

Baars,T., & Spruit,M. (2012). Designing a Secure Cloud Architecture: The SeCA Model. International Journal of Information Security and Privacy, 6(1), January-March 2012, 14–32. Bace, R., and Mell, P.

(2001). *Intrusion Detection Systems*. Washington, DC: US Department of Commerce.

Bekkers, W., Weerd, I. van de, Spruit, M., & Brinkkemper, S. (2010). A Framework for Process Improvement in Software Product Management. Systems. In Riel, A., O'Connor, R., Tichkiewitch, S., & Messnarz, R. (Eds.),Communications in Computer and Information Science 99, Software and Services Process Improvement - Proceedings of the 17th European Conference (pp. 1–12). EuroSPI 2010, September 1-3, 2010, Grenoble, France: Springer. [pdf] [online]

Bell, D.E. and La Padula, L.J. (1976). *Secure Computer System: Unified Exposition and Multics Interpretation (*ESD-TR-75-306). Bedford: The Mitre Corporation.

Biba, K.J. (1977). Integrity Considerations for Secure Computer Systems (MTR-3153). Bedford: The Mitre corporation.

Bishop, M. (2004). *Introduction to Computer Security*. Boston, MA: Addison-Wesley.

Blakley, B., McDermott, E. and Geer, D. (2001). Information Security is Information Risk Management. *Proceedings of the 2001 workshop on New security paradigms,* New York, NY, USA, 97-104.

Bodin, L.D., Gordon, L.A., Loeb, M.P. (2008). Information security and Risk management. *Communications of the ACM, 51*(4), 64-68.

Brewer, D.F.C, Nash, M.J. (1989). The Chinese Wall Security Policy. *IEEE Symposium on Security and Privacy*, 206-214.

Broderick, J.S. (2001). Information Security Risk Management – When Should It Be Managed? *Information Security Technical Report, 6*(3), 12-18.

Bruin, T. de, Freeze, R., Kalkarni, U., and Rosemann, M. (2005). Understanding the main phases of developing a maturity assessment model. *Proceedings of the 16th Australasian Conference on Information Systems*, *Australia*.

British Standard Institute (2005*). ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management.* Londen, UK.

British Standard Institute (2006). *Business Continuity management – Code of practice.*

BSIMM3 (2011). *Building Security In Maturity Model.* Retrieved December 10th, 2011, from http://bsimm.com/download/

Burnett, S. and Paine, S. (2001). *The RSA Security's Official Guide to Cryptography.*New York: McGraw-Hill, inc.

Bulgurcu,B., Cavusoglu, H. and Benbasat, I. (2010).Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly 2010, 34*(2), 523-A7.

Carlson, T. (2001). *Information Security Management: Understanding ISO 17799.* Retrieved September 20th from, http://www.kwesthuba.co.za/downloads/03_ins_info_security_iso_17799_1101.pdf

Carr, E. R. (2005). *Environmental Security*. In the Routledge Encyclopedia of International Development, Tim Forsyth, ed. London: Routledge, 213-214.

Casson, D. (2006). ITIL Change Management Maturity Benchmark Study from Evergreen. *Information-management.* Retrieved June 6th, 2011, from http://www.information-management.com/specialreports/20061010/1064947-1.html

Chapin, D.A., and Akridge, S. (2005). How can Security be measured. *Information Systems Control Journal, 2*, 43-47.

CISSP and ISO27k (2007). Top information security risks for 2008, *ISC2*. Retrieved September 20th, from http://www.iso27001security.com/Top_information_security_risks_for_2008.pdf

Clark, D.R. and Wilson, D.R. (1987). A Comparison of Commercial and Military Computer Security Policies. *IEEE Symposium on Security and Privacy,* 184-194.

CMMI (2002). CMMISM for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing; (CMMISE/SW/IPPD/SS, V1.1) Staged Representation; CMU/SEI-2002-TR-012 ; ESC-TR-2002-012 .

Coates IV, J.C. (2007). The goals and Promise of the Sarbanes-Oxley Act. *Journal of Economic Perspectives, 21*(1). 91-116.

Conrath, E.J., Krauthammer, T., Marchand, K.A., and Mlaker, P.F. (1999). *Structural Design for Physical Security*. USA: ASCE.

Daud, M.I. (2010). Secure Software Development Model: A guide for Secure Software Life Cycle. *Lecture Notes in Engineering and Computer Science,2180*(1). 724-728.

De Ruiter, P. *Business Continuity Management.* Retrieved March 13th, 2011, from http://www.pvib.nl/download/?id=11581169

Denning, D.E. (1976). A lattice model of secure information flow. *Communications of the ACM, 19*(5). 236-243.

Discini (2006). *Developing Security Policies: Rules vs. Risk.* Retrieved March 15th, 2012, from http://www.esecurityplanet.com/best_practices/article.php/3629626/Developing-Security-Policies-Rules-vs-Risk.htm

Eloff, J.H.P., and Eloff, M.M. (2005). Information Security architecture. *Computer Security and Fraud, 2005*(11), 10-16.

ENISA. (2009). *Cloud Computing: Benefits, risks and recommendations for information security.* NISA, Emerging and Future Risk programme. Crete: ENISA.

Fagan, P. (1993). Organizational issues in IT Security. *Computer & security, 12*(8). 710-715.

Ferraiolo, D.F. and Kuhn, R.D. (1992). Role-Based Access Controls. *15th national Computer Security Conference.* 554-563.

Flynn, S.M. (2010). Linking Human Resource Strategy and Practice: An Integrated Framework.

Forrester (2010). *Introducing the Forrester Identity and Access Management Maturity Model.* Retrieved may 13th, 2011, from www.forrester.com

Fuchsberger (2005). Intrusion Detection Systems and Intrusion Prevention Systems. *Information Security Technical Report, 10.* 134-139.

Gabriel, R., Sowa, S. And Wiedemann, J. (2008). Improving information security compliance--A process-oriented approach for managing organizational change. *Multikonferenz Wirtschaftinformatik*

Gergi, R. (2010). *Logical and Physical Security – What the main Major Differences are.* Retrieved May 17th, 2012, from http://ezinearticles.com/?Logical-and-Physical-Security---What-the-Major-Differences-Are&id=3541842

Gartner (2008). *Assessing the Security Risks of Cloud Computing*, Retrieved December 15th, 2012, from www.gartner.com

Gartner (2009). *Toolkit: Identity and Access Management Program Maturity Assessment.* Retrieved May 13th, 2012, from www.gartner.com

Haughney (2008). SMART goals. Retrieved Febrauary 8th, 2011 from http://www.projectsmart.co.uk/smart-goals.html

Herriot, R.E., and Firestone, W.A. (1983). Multisite qualitative policy research: Optimizing description and generalizability. *Educational Researchers, 12*(2), 14-19.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*. Boca Raton, FL: Auerbach Publications.

Hevner, A.R., March, S.T., Park, J., and Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-101.

Hillson, D.A. (1997). Towards a Risk Maturity Model*. International Journal of Project & Business Risk Management*, *1*(1), 35-45.

Höne, K. and Eloff, J. (2002). *Information security policy – what do international information security standards say?, 22*(5), 402-409.

Hulett, D.T. (2001). Key Characteristics of a Mature Risk Management Process. *Paper presented at the Fourth European Project Management Conference*, PMI Europe, London, UK, 6-7 June, page 6.

Humphreys, E. (2008) Information security management standards: Compliance, governance, and risk management, *Information Security Technical Report*, *13*(4), 247-255.

IEEE (1983). *IEEE Standard Glossary of Software Engineering Terminology*. IEEE Std 729.

IEEE (1990). *IEEE Standard Glossary of Software Engineering Terminology*. IEEE Std 610.12.

ISC^2 (2012). *The ten best practices for Secure Software Development.* Retrieved May 23rd , 2012, from https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Certification_Programs/CSSLP/ISC2_WPIV.pdf

ISC^2 (2011). CISSP – Certified Information Systems Security Professional. *ISC2.* Retrieved June 8th, 2011, from https://www.isc2.org/cissp/Default.aspx.

ISO (2009). ISO/FDIS 31000:2009(E), Risk Management – Principles and guidelines.

IT Governance Institute. (2000). *COBIT 4.1 excerpt.* Rolling Meadows, IL, USA.

Jamil, D., and Zaki, H. (2011). Cloud Computing Security. *International Journal of Engineering Science and Technology, 3*(4). 3478-3483.

Jaquith, A. (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* Reading, MA: Addison Wesley.

Jelen, G. (2001). SSE-CMM Security Metrics. *NIST and CSSPAB Workshop*, URL: http://csrc.nist.gov/csspab/june13-15/jelen.pdf

Jones,A., Kovacich, G.L., Luzwick, E.G. (2002). *Global Information Warfare. How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton, FL: Auerbach publications.

Kalbande, D.R., Singh, M. and Thampi, G.T. (2009). Incidence Handling and Response System. *International Journal of Computer Science ànd Information Security, 2*(1).

Kankanhalli, A., Teo, H., Tan, B.C.Y., and Wei, K. (2003). *International Journal of Information Management, 23*(2), 139-154.

Khan, R. and Ambedkar, B.B. (2011). *Computer Fraud & Security, 2011*(8). 12-20.

Koelewijn, G. (2009). *Identity & Access Management.* Retrieved may 13th, 2011, from http://repository.tudelft.nl/assets/uuid:47e228e5-645e-497c-a5e2-ec3b4df5e299/Thesis_-_Identity__Access.pdf

Koomen, T., Pol, M. (1999). Test Process Improvement, a practical step-by-step guide to structured testing. Boston, MA: Addison-Wesley Longman Publishing.

Kruger, H.A., Kearney, W.D. (2006). *prototype for assessing information security awareness, 25*(4), 289-296.

Lam, W (2002). Ensuring Business Continuity. *IT Professional, 4*(3), 19-25.

Landau, S. (2000). Standing the test of time: The Data Encryption Standard. *Notices of the American Mathematical Society, 47*(3), 341-349.

Lee, W., and Stolfo, S.J. (2000). A framework for constructing features and models for Intrusion Detection Systems. *ACM Transactions on Information and System Security (TISSEC), 3*(4). 227-261.

Leopoldi, R. (2002). *IT Service Management: Change Management Methods and Implementation Best Practices.*ITSM. Retrieved June 8th, 2011 from www.itsm.info/ITSM%20Change%20Management%20Best%20Practices.pdf

Leeuw, K. de, and Bergstra, J. (2007). The History of information security: A comprehensive Handbook. Amsterdam, NL: Elsevier.

Lewin, K. (1951). *Field Theory in Social Science*. New York: Harper.

Mahizharuvi, P. and Alagarsamy, K. (2011). *International Journal of Computer Technology and Applications, 2*(2). 253-257.

Maier, A.M. and Moultrie, J. and Clarkson, P.J. (2009) *Developing maturity grids for assessing organisational capabilities: practitioner guidance* In: 4th International Conference on Management Consulting, Academy of Management (MCD'09), 11-13 June 2009, Vienna, Austria.(Unpublished)

Mell, P. and T.Grace, 2009, "The NIST Definition of Cloud Computing", csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

METAgroup (2001). Diagnostic for Enterprise Architecture, META Practice.

Mettler, T., Rohner, P. (2009). Situational Maturity Models as Instrumental Artifacts for Organizational Design. Proceedings of the 4th international Conference on Design Science Research in information Systems and Technology. USA.

Michael, M. (2006). Physical Security Measures. In Bidgoli, H. (Eds.). *Handbook of information security*. (pp. 263-288). Hoboken: Wiley.

Michael, R. (2006). The definition Of Asset Management. Retrieved September 20th, from http://www.eioba.com/a/7vi/the-definition-of-asset-management

Mitnick, K.D. and Simon, W.L. (2002). *The Art of Deception: Controlling the Human Element of Security.* Indianapolis, IN, USA: Wiley Publications.

Moultrie, J. (2007). "Development of a Design Audit Tool for SMEs." Journal of Product Innovation Management 24(4): 335-368.

NASCIO (2003). NASCIO enterprise architecture maturity model.

NIST (2004). *Computer Security Incident Handling Guide.* Retrieved September 10th, 2011, from http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

NIST. (2010). *NIST Definition of Cloud Computing v15.* Department of Commerce. Washington: NIST.

Nolan, R.L. (1973). Managing the computer resource: a stage hypothesis. *Commun. ACM*, *16*(7), 399-405.

NoticeBored (2004). *Securing physical access and environmental services for datacenters.* Retrieved april 14th, 2011, from http://www.infosecwriters.com/text_resources/pdf/datacenter_security.pdf

Oarisk (2010). Oarisk operational Asset and Risk Solutions. Retrieved September 20th, 2011, from http://www.oarisk.co.uk/Asset_Management_Maturity_Model.html

Office of Government Commerce (2007) *IT Infrastructure Library – ITIL.* Norwich, UK.

Opensamm (2011). *Software Assurance Maturity Model.* Retrieved December 10th, 2011, from www.opensamm.org

Orman (2003). The Morris worm: a fifteen-year perspective. *Security and Privacy IEEE, 1*(5). 35-43.

Oud, E.J. (2000). Business Continuity Management; meer dan Contingency Planning. Retrieved September 10th, 2011, from http://www.euronet.nl/users/ernstoud/pdf/ths_jrbk2.pdf

Ouertani, M.Z., Parlikad, A.K., and Mcfarlane, D. (2008). Towards an approach to select an asset information management strategy, *International Journal of Computer Science and Applications, 5*(3b), 25-44.

Payne, S. C. (2006). *A guide to security metrics.* SANS Institute. Retrieved January 19th ,2011, from http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55?show=55.php&cat=auditing

Pfleeger, S. (2007). Managing Organizational Security. *IEEE Security & Privacy.*

Pham, N., Baud, L., Bellot, P.,Riguidel, M. (2008). Towards a Security Cockpit. *International Conference on Information Security and Assurance.* 374-379.

Mura, L. (2012). The PPBI Incident Management Maturity Model. *PPBI.* Retrieved February 3th, 2012, *from http://www.ppbi.org*

Prosci (2004). Prosci's Change Management Maturity Model*. Change-Management.* Retrieved June 7th, 2011, from *www.change-management.com/**Prosci**-CM-**Maturity**-**Model**-writeup.pdf.*

Queensland Government (2009). *Change Management Best Practices Guide.* Queensland, UK.

QGEA (2010). *Information Standard IS18*. Retrieved May 26th, 2011, from www.qgcio.qld.gov.au/.../Architecture%20and%20Standards/Information%20Standards/.../is18_print.pdf

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Hants, UK: Ashgate Publishing Ltd.

Sandhu, R.S. and Samatari, P. (1994). Access control: Principles and Practice. *IEEE Communications magazine, 32*(9). 40-48.

Sanli (2010). Management Issues In Information Technology. *E-leader Budapest.*

SANS (2007). *Information Security Policy – A development guide for large and small companies*, Bethesda, MD: SANS institute printing office.

SANS Institute. (2008). *Data Loss Prevention.* Bethesda, MD: SANS Institute printing office.

SANS Institute. (2008). *Host intrusion Prevention Systems and Beyond.* Bethesda, MD: SANS Institute printing office.

Sherwood, J., Clark, A., and Lynas, D. (2009). *Enterprise Security Architecture.* Retrieved December 12th, 2011, from http://www.alc-group.com/sabsa_enterprise_security_architecture.php

Singleton, T.W.(2009). What every auditor should know about controls: The CDLC. *ISACA Journal, 3.* 1-2

Smit, N. (2005). *Business Continuity Management*. Retrieved November 11th, 2011, from http://www.pvib.nl/scripties

Software Engineering Institute (2010). *Smart Grid Maturity model.* Retrieved November 22nd, 2011, from http://www.sei.cmu.edu/library/assets/brochures/SGMM-1010.pdf

Solms, B (2006). Information Security – the fourth wave. *Computers & Security, 25*(3), 165-168.

Steenbergen, M. van, Bos, R., Brinkkemper, S., Weerd, I. van de & Bekkers, W.J. (2010). The design of focus area maturity models. In R. Winter, J. Zhao & S. Aier (Eds.), Global Perspectives on Design Science Research Lecture Notes in Computer Science (pp. 317-332). Berlin, Heidelberg.

Steenbergen, M. van, Brinkkemper, S., van den Berg, M. (2007): An Instrument for the Development of the Enterprise Architecture Practice. *Proceedings of the 9th International Conference on Enterprise Information Systems*, 14-22.

Steenbergen, M. van, Schipper, J., Bos, R, Brinkkemper, S. (2009). The Dynamic Architecture Maturity Matrix: Instrument Analysis and Refinement. In Asit, D., Gittler and Toumani, F. (Ed.), Service-Oriented Computing. ICSOC/ServiceWave 2009 (pp. 48-61). Stockholm: Springer Berlin/Heidelberg.

Structural Engineering Institute (1999). *Structural Design for Physical Security: State of the Practice*. United States of America: ASCE

Symantec. (2010). W32.Stuxnet. Retrieved November 15th, 2011, from http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling Design Processes. A*I Magazine , 11* (4), 37-48.

The Institute of Internal Auditors (2007). *Identity and Access Management.* Retrieved May 23rd, 2012, from http://www.aicpa.org/interestareas/informationtechnology/resources/informationsecuritymanagement/downloadabledocuments/gtag9identaccessmgmt.pdf

The Open Group (2011a). *Security Architecture and the ADM.* Retrieved February 11th, 2012, from http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap21.html

The Open Group (2011b). *Architecture Maturity Models.* Retrieved Februaty 11th, 2012, from http://pubs.opengroup.org/architecture/togaf8-doc/arch/chap27.html

Theohariduo, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, *24*(6), 472-484.

US Government. (2002). *Sarbanes Oxley Act of 2002* (Publication No. 15 USC 7201). Retrieved June 8th, 2011, from www.sec.gov/about/laws/soa2002.pdf

Weerd, I. van de, Brinkkemper, S. (2008). Meta-modeling for situational analysis and design methods. In M.R. Syed and S.N. Syed (Eds.), Handbook of Research on Modern Systems Analysis and Design Technologies and Applications (pp. 38-58). Hershey: Idea Group Publishing.

Weingart, S.H. (2000). Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses. *Workshop on Cryptographic Hardware and Embedded Systems*, *1965.* 302-317

Westbrock, T. (2004). Architecture Process Maturity Revisited and Revised. METAgroup Delta 2902.

West-Brown, M.J. et al. (2003). *Handbook for Computer Security Incident Reponse Teams (CSIRT).* Retrieved September 10th, 2011, from http://www.cert.org/

Whitman, M.E. and Mattord, H.J. (2009). *Principles of information security.* Boston, MA: Thomson Course Technology.

Windley, P.J. (2005). *Digital Identity*. Sebastopol, CA: O'Reilly Media

Wood, C. (2011). *Levels of maturity in The Security Policy Development Process.* Retrieved November 19th, 2011, from http://www.informationshield.com/security-policy/2011/01/levels-of-maturity-in-the-security-policy-development-process/

Yeo, K.T., Ren, Y. (2008). Risk Management capability maturity model for complex product systems (CoPS) projects. *Systems Engineering, 12*(4), 275-294.

R.K. Yin(2003). *Case Study Research: Design and Methods (*3rd ed.*).* London, UK: Sage publicationss

10. Appendices

Appendix A: interview Identity and Access Management

How can Single Sign On (SSO) be more secure and thus more mature then organizations not using SSO?

Answering this question, expert #8 also used a figure to explain why and where the security is improved using SSO. This figure is pictured here:

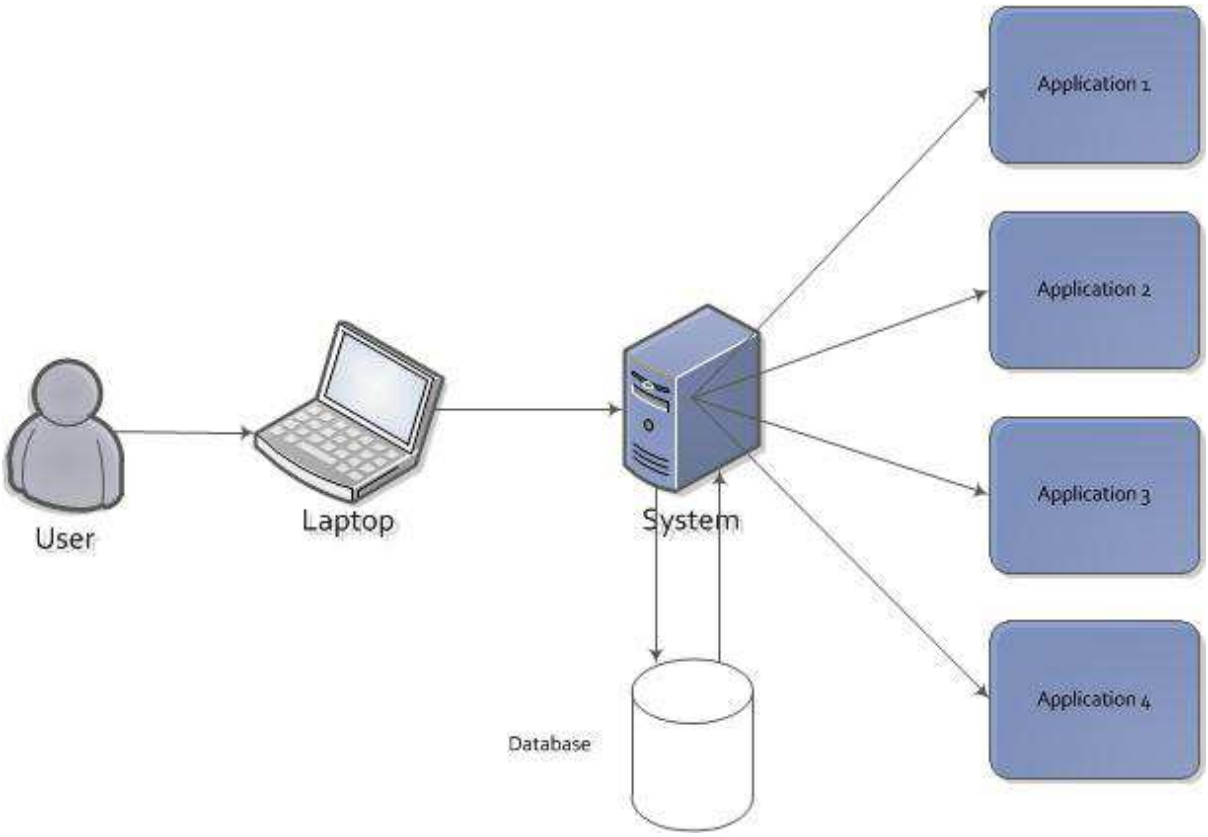

Figure 43: Single Sign On mechanism

Single Sign On is the term used to describe that a user can access all applications Figure 34 starts with a user logging on to his/her laptop. A strong password (>8 characters, not only letters, etc.) is recommended. The system behind this laptop now knows that the person is authenticated. When the person needs to access one of the applications where normally an additional authentication (userid/password) would be needed, the system in between now handles this task by asking a database for this data. The system forwards this data to the application with as result that the user does not have to remember another password to log in. If a user utilizes a lot of applications and those applications all need some form of password that the user has to remember, the user is more likely to pick simple passwords like his name. With SSO, the user has to remember only one password and all other passwords can be randomly generated and encrypted, since the user doesn't need to know them. Advantage is now that the only password of the user can be a stronger password because he only needs to remember one. On the other hand, since the applications are secured by a randomly generated password, hackers can't access the system by hacking the applications because those applications also have a strong password. The only point of attention is

the security of the database. The database must be well encrypted to assure that the passwords can't get stolen by hackers. Besides the advantage of the increasing security, the user friendliness also increases.

What is the relation between Human Resource Security and Identity and Access Management?

This question was posted to make a clear distinction between both terms for the thesis. Thereby duplicate metrics can be avoided. Expert #8 draws a figure (see figure 35).

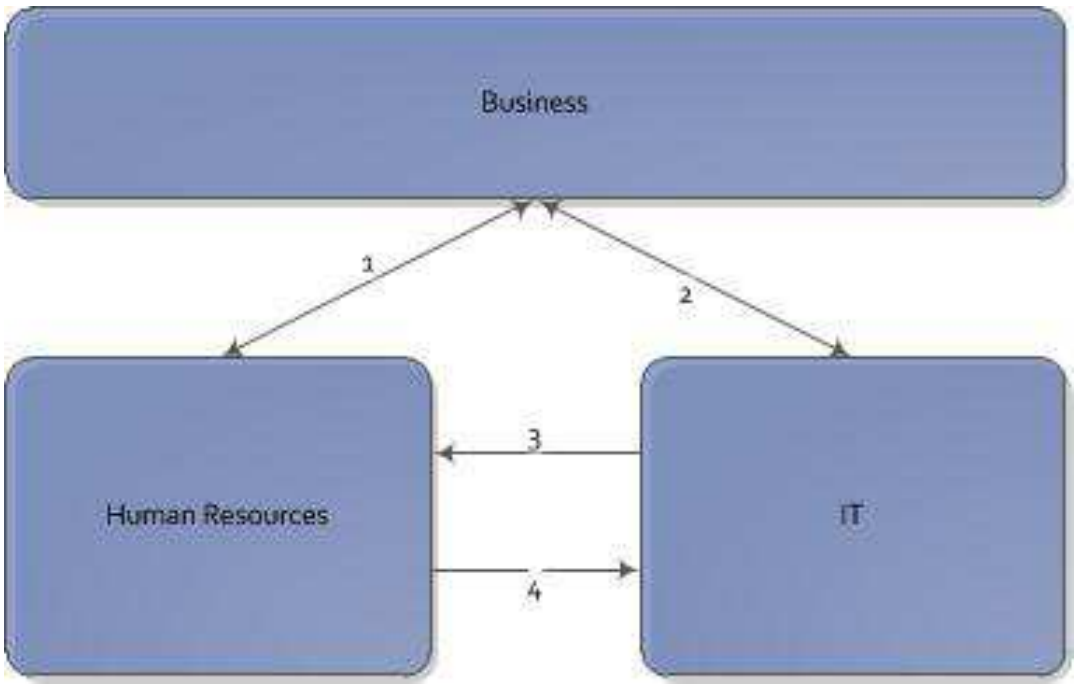

Figure 35: relation between Human Resource Security and Identity and Access Management

Identity and Access Management in this figure is part of IT. First of all there is the business. Second you have supporting functions of the business, in this case Human Resources and IT. Take the example of a person hired by the organization. The business delegates to Human Resources to set up a contract, arrange a car and perform HR checks (such as verification of certificates, background check, etc.). At the other hand the business also informs IT to create an account for, and give the appropriate rights to the new employee. This model of handling IAM is depicted by arrow 1 and 2 in the figure. However, this in that case it is done in an immature way. Better would be to inform Human Resources (arrow 1) and let Human Resources trigger the process at IT to create and arrange all needs for the new employee. The request is done by arrow 4 and the answer and services are represented by arrow 3. In this way the business does not manage two departments for the same job (e.g. in the picture arrow 2 is not used anymore). The relationship between Human Resource Security and Identity and Access Management is as follows: Human Resource Security is the trigger for Identity and Access Management. This definition means that Human Resources should let IT know what to do regarding accounts and personnel. Human Resources keep track of the employees hired, fired and left and IT should then perform the supporting role in terms of bringing and getting

back the assets. Moreover, Human Resource Security can be seen as the organizational role and Identity and Access Management as the IT-role that supports the organizational role.

What do you usually see when entering a company as consultant? Is it structured, is there documentation, etc?

Most of the times companies have a suboptimal access control system. They do not use Role Based Access Control, but assign rights and grant access to employees when needed. This is not documented in most cases, and for larger organizations it becomes unmanageable. It would be more effective to assign all employees to roles and those roles to rights. The roles are then managed by a role manager that obviously has a lot to do, but is still better than giving rights to employees on request. Central documentation (on paper or in a system) of access rights is then the next step of maturity. Employees who leave the organization no longer need an account or rights. When the rights and accounts of this employee are documented, it is easy to remove or disable them. Additionally this could be automated by running a script on a periodic basis (i.e. monthly) that automatically checks the employee's rights with his role. This could either flag violations or even adjust violations to bring them in line with policy. However, most of the times IAM is not really structured, but there is some awareness at management level. IAM also starts with management commitment, because IAM needs to be driven from a strategically perspective. Most of the times individuals take the first steps by doing small things like documenting rights. However, if it needs to get organization wide, the implementation starts at management level. An IT-driven IAM strategy only results in suboptimal solutions as IT is usually not capable to get the business onboard for such a large project.

Can Identity and Access Management create additional business for your organization and do you have an example of such a case?

Yes, it does. By implementing IAM there is a lot to gain. Not only regarding cost savings, but also regarding new business ideas. By implementing IAM it is also possible to use the identities for marketing purposes (keep in mind to remain compliant with privacy regulation though). This is for example done with loyalties at supermarkets. Companies can use the data on the card to customize their marketing to a single person.

Appendix B: Interview HR Security

What does Human Resources Security consist of?

Expert #5 answered this question by first telling me about his experience with HR security within the organizations he worked for. During this conversation he pointed out a couple of HR security aspects. As already known by me, background screening is an important part of getting the right people into your organization and more important: preventing the 'bad' people to get into your organization. Such background screenings are divided over three levels ranging from a simple screening (e.g. screening former employers, criminal records, etc.) on the applicant to an extensive check on the whole family. An extensive screening on the family is necessary for high governmental functions to make sure that you are not related or seduced by criminal personal contacts. Another aspect of HR Security is reporting of security incidents. As an example he referred to an unsafe lock on the door. All employees in the building know that the building thereby is not sufficiently secured and need to be obliged to report this to the security officer or at least someone responsible for this issue. However, in most organizations this does not happen. Employees are selfish and care about their own tasks. A solution to this could be the hiring of an external facilitating company (i.e. Johnson controls). However, in their portfolio security and their related risks is still an underappreciated. Making a single employee responsible for reporting the incidents is another option. At first thought this could solve the problem immediately, but taking a closer look also brings a disadvantage. Employees care about their status within an organization. If assigned the task of incident reporter, the employee could become less appreciated because he/she is always looking at what others are doing and if that is considered legal or not. The most ideal situation would be that the whole department/organization and individual within warn others when violating the policy. The third aspect of HR security is the security travel policy. This policy is not mentioned a lot in literature but is an important issue within HR Security. For small organizations it might be less applicable, but for large organizations travelling has to be taken into account. Employees feeling uncomfortable in immigrant neighborhoods should not be allowed to travel to a middle-east country with threat for terrorism. Hence, when they don't feel comfortable in their own country because of those persons, how would they feel in their country? From a business point of view it would be best to keep them in their own country and do not risk any negative impacts on that person. The guideline should be: An employee is only allowed to fly if the employee returns in an equal or better condition.

Finally, there is awareness. Is does not matter what you want to change or implement in your organization, awareness of consequences caused by human actions is always necessary. The same holds for HR Security awareness. Employees need to be aware of the HR Security policy to comply with it. The policy encompasses all aspects mentioned earlier in this paragraph.

Where does HR Security start with?

HR Security starts already with signing the contract and making employees aware of what their security responsibilities are. Employees, however, see their security responsibilities as a secondary task and therefore pay little or no attention to it. Establishing a security culture from the start of someone's employment is a good start. Next step is to retain and expand the awareness of the employees by posters, events, etc. These help to remind the employee of his duty to comply with the HR policy. The hardest part of this is making sure that employees tell each other when they are

violating the policy. Last but not least, the person will leave the organization with a lot of knowledge. This knowledge is confidential and should not be spread across the globe. Including additional paragraphs about this in the contract solve this issue and are nowadays often applied.