Laurea University of Applied Sciences
Prime Mover

Developing an Information Security Management System

Karjalainen, Mika

2014 Leppävaara

Laurea University of Applied Sciences
Leppävaara

Developing an Information Security Management System

Mika Karjalainen
Degree Programme in
Security Management
Bachelor’s Thesis
May, 2014

Laurea University of Applied Sciences
Leppävaara
Degree Programme in Security Management

Abstract

Mika Karjalainen

Developing an Information Security Management System

Year	2014	Pages	36

The purpose of this thesis was to study development of an information security management system and study the resources and components, which combined create a functional information security management system. To reach the target objective, the thesis first examines the international and international legislation regarding information security. Secondly, the information security related international and national standards and frameworks are analyzed and compared. Finally the outcome of thesis is presented as a reflection of previously studied components of information security management systems.

This thesis was carried out as a basic research to expand the knowledge of the phenomena and develop current practices. Literature overview was used as the research method, as it is the most eligible method to explore the aims of this study. Literature overview was selected to collect in-depth data of the phenomena.

The results of this study indicate that the national legislation related to information security in Finland is not one unified entity, but is fragmented in various regulations. It requires plenty of expertise to gather relevant parts of the legislation in a company to form a functional information security management system. The study also indicates that there are various information security management standards. The international standards and frameworks are wider and can be applied to various organisations as is. The national standards are intended for a specific purpose and require more expertise in order to be applied in an organisation.

Keywords: Information security, Information security management system

Laurea-ammattikorkeakoulu
Leppävaara
Degree Programme in Security Management

Tiivistelmä

Mika Karjalainen

Tietoturvallisuuden johtamisjärjestelmän kehittäminen

Vuosi 2014 Sivumäärä 36

Tämän opinnäytetyön tarkoituksena oli perehtyä tietoturvallisuuden johtamisjärjestelmän kehittämiseen, sekä tutkia sen vaatimia komponentteja ja resursseja, jotka yhdessä luovat toimivan tietoturvallisuuden johtamisjärjestelmän. Tavoitteen saavuttamiseksi opinnäytetyössä käydään ensimmäiseksi läpi kansallista ja kansainvälistä lainsäädäntöä liittyen tietoturvallisuuteen. Toiseksi, opinnäytetyössä tutkitaan ja verrataan kansallisia ja kansainvälisiä tietoturvan standardeja ja viitekehyksiä. Lopuksi opinnäytetyössä esitellään lainsäädännön, standardien ja viitekehyksien vaikutuksia tietoturvallisuuden johtamisjärjestelmiin.

Opinnäytetyö toteutettiin perustutkimuksena, jonka avulla pystyttiin laajentamaan tietämystä ilmiöstä, sekä kehittämään nykyisiä käytäntöjä. Opinnäytetyön tutkimusmenetelmänä käytettiin kirjallisuuskatsausta, koska se tarjosi parhaiten tavoitellun tietoaineiston keräämisen. Kirjallisuuskatsauksen avulla oli mahdollista kerätä syvällistä tietoa tietoturvallisuuden johtamisesta ja muista siihen liittyvistä ilmiöistä.

Tämän tutkimuksen tulokset osoittavat, että tietoturvallisuuteen liittyvä kansallinen lainsäädäntö ei ole Suomessa yksi yhtenäinen kokonaisuus, vaan se jakautuu useisiin eri asetuksiin. Toimivan tietoturvallisuusjohtamisjärjestelmän laatiminen vaatii huomattavasti asiantuntemusta, jotta osataan ottaa huomioon organisaatiota koskevat osat lainsäädännöstä. Tutkimus osoitti myös, että on olemassa useita tietoturvallisuuden hallintaan tarkoitettuja standardeja. Kansainväliset tietoturvallisuuteen liittyvät standardit ovat sisällöltään laajempia ja niitä voidaan hyödyntää sellaisenaan useaan organisaatioon. Kansalliset standardit ovat tehty tiettyjä tarkoituksia varten ja vaativat laajaa osaamista, jotta niitä voidaan soveltaa organisaatioissa.

Asiasanat: Tietoturva, tietoturvallisuuden hallinta, tietoturvallisuuden hallintajärjestelmä

Table of Contents

1 Introduction

Information is a key resource for all organisations from the time it is created to the moment it is destroyed. To manage the confidentiality, integrity and availability of this information is crucial for organisations in order to succeed in the fast paced environment of today. To ensure that the life cycle of the information is guaranteed from the security point of view, organisations must be able to track the information flow through the whole life cycle. To help with this organisations are recommended to create and manage an information security management system.

This thesis describes the different components of information security management systems and different frameworks that can be used as guidelines when creating information security management system for an organisation. The thesis starts by laying down the reasons why this subject was chosen and how it was approached. It then clarifies the research methods and theoretical background of this thesis. This thesis describes the laws and regulations affecting the information security environment of today and provides the reader with a good selection of information security management standards and frameworks that can be used to create an organisation specific information security management system. The research also provides different managerial approaches on handling the management system. In the later parts of the thesis the different methods of handling and creating information security management systems are compared and analyzed.

2 Problem domain

Topic for this thesis was chosen on the basis of the needs of the organisation in which the author did his internship. The need to develop information security came in particular from the requirements of the Decree on information security in central government. The target organisation also had an urge to be compatible with the ISO/IEC 27001:2013 standard in the future, which obligates the certified organisation to maintain the requirements of the standard. For this reason the need for an information security management system (ISMS) was obvious. However during the thesis process it became clear that a fully functional ISMS for such a small organisation was not the practical option. This thesis was originally meant to be an action research to develop the information security practices in the organisation, but morphed into a literature overview on what kind of options there are for organisations to develop their information security management systems and what kind of standards can be used to do it.

According to Network and Information Security Agency ENISA (2006), security experts and statistics have confirmed that "information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness". Therefore this thesis concentrates on the administrative side of information security management, and does not take a wider look at the technical aspects of information security.

2.1 Research problem

To research how an effective information security management system is established the literature of information security and management systems were studied. The focus was to understand what kinds of resources must be allocated to information security management, based on what criteria, and what kind of information security practices are used to meet the goals set for information security management systems.

Therefore, the aim of this research is to understand the following topics. First, what kinds of information security management systems are there? Second, what kind of information security practices are used and for what reason? Third, what kinds of resources are allocated to these information security management systems and what do they result in? Following this, the attempt is made to explain how an effective information security management system can be created, and how it can support the overall business strategies of an organisation.

This research is focused on the governmental point of view on creating an information security management system. The theories and findings of this research can also be applied to privately held companies. The reason for selecting a governmental point of view over privately held companies is that the client for this research was a governmental organisation. Governmental organisations are also guided by legislation that does not concern privately held companies and therefore presenting the requirements of those laws adds value to this research. One of the products of this research is a development plan for the target organisation to develop their information security management system in the future.

To study the research problem structured above, a research question has been compiled to clarify the direction of this study. The research question of this study is formulated as:

What are the components of an effective information security management system?

The sub-research questions of this study are:

1. *What is information security management*?
2. *What kinds of resources does information security management involve*?

2.2 Theoretical background and methodology

This thesis was carried out as a basic research to expand the knowledge of the phenomena and develop current practices. Literature overview was used as the research method, as it is the most eligible method to explore the aims of this study. Literature overview was selected to collect in-depth data of the phenomena.

Basic research is systematic study to expand the knowledge and understanding of the fundamental aspects of phenomena. It seeks to collect information of the phenomena, but avoids changing the subject into another. The research mainly describes what the subject is or has been, and possibly explains why it is as it is. (Routio 2007) Data about information security and management systems was collected through basic research from various publications and other academic sources through literature overview. These sources include various widely accepted international and national standards and legislation. As this thesis started with a focus on central government, various regulations affecting central government are explained.

2.3 Central government authority

Defined by the decree on information security in central government (Finland 2010) central government authority is "a State administrative authority, another government agency or body, a court of law or another authority for administration of justice". There are approximately a hundred central government agencies and public bodies of various sizes in Finland, performing various tasks.

Many government agencies and public bodies carry out administrative tasks, whereas some have extensive information management and registration duties. Many agencies and public bodies are responsible for developing a specific sector and producing related information for the society as a whole. The central administration also encompasses several research institutes, the largest of which include the Technical Research Centre of Finland (VTT), Geological Survey of Finland and the Finnish Forest Research Institute. Case agency of this study, The Governing Body of Suomenlinna, is explained in more detail in the next chapter. Diagram below shows the positions of State administration in the structure of the public administration. (State Treasury 2013)

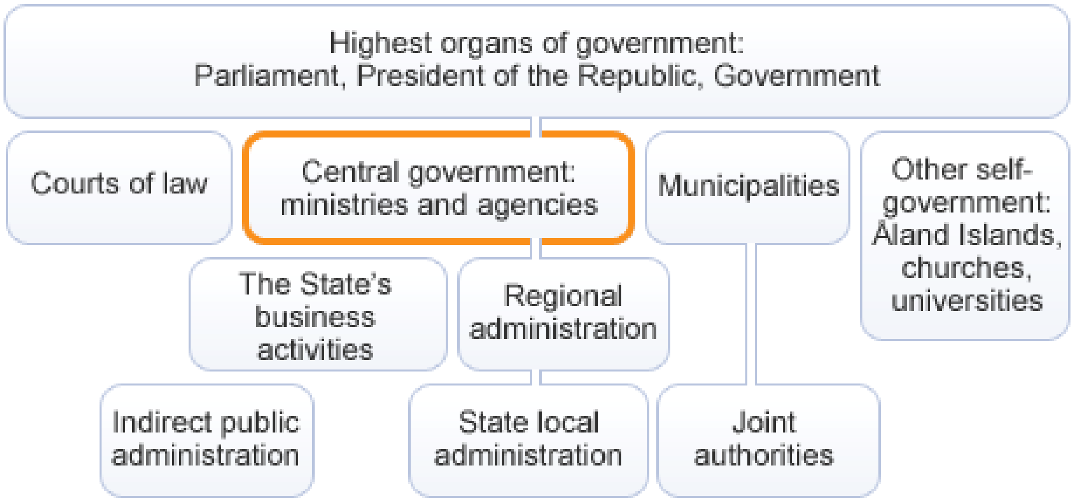
Highest organs of government:
Parliament, President of the Republic, Government
Courts of law
Central government: ministries and agencies
Municipalities
Other self-government: Åland Islands, churches, universities
The State's business activities
Regional administration
Indirect public administration
State local administration
Joint authorities

Figure 1 Position of central government in the public administration.

3 Analytical framework

Requirements, recommendations and frameworks for information security come from different sources. In this thesis those sources are divided to international requirements, national legislation, and to proven standards for information security and management. As the perspective of this thesis is a central governmental organisation, the VAHTI (The Government Information Security Management Board) instructions are explained in more detail, even though the requirements in it originate from national legislation.

3.1 International requirements

International requirements for information security are based on binding directives from the European Union (EU), General Security Agreements between parties and voluntary recommendations from different organisations, such as Organisation for Economic Co-operation and Development (OECD). General Agreements however are part of the Act of international information security responsibilities and are described in national legislation chapter. Other important international requirements are described below.

3.1.1 OECD

In 1992, the Organisation for Economic Co-operation and Development (OECD) published the first version of their guidelines on the Security of Information Systems. These guidelines introduced nine principles to ensure the security of information systems and recommendations regarding their implementation. Ten years later, in 2002, the OECD reviewed the Security Guidelines. The revised version addressed the security implications of the open Internet and the generalisation of interconnectivity. (OECD 2012)

The 1992 Security Guidelines concentrated on avoiding the risks by closing the systems with strict perimeter security. As the openness and interconnectivity of information systems was forced by the business needs, the reviewed guidelines of 2012 switched from risk avoidance to risk management. The guidelines also state that all of the participants can be considered to be a joint society as they operate in shared environment and the security of information processes is the responsibility of all parties from the government to individual organisations. (OECD 2012)

The OECD Security Guidelines are voluntary, but all the member states are recommended to implement the requirements. According to the Ministry of Finance (2011, 42), in Finland the OECD recommendations are taken into account in VAHTI instructions provided by the Government Information Security Management Board (VAHTI) operating under the Ministry of Finance. VAHTI-instructions are described in detail in a later chapter. In 2012 the OECD initiated a review of the 2002 Security Guidelines, but as of writing this thesis the new guidelines have not been published. (OECD 2012)

3.1.2 EU Legislation

European Union (EU) has established directives that directly and indirectly affect the information security processes of its member countries. This chapter is not meant to be a full overview of these directives, but describes the two directives that can be seen as the most important. These directives are the data protection act, and the directive on privacy and electronic communications. The other EU directives concerning information security are addressed in their national implementations in a later chapter.

Data protection directive 95/46/EC on protection of personal data was introduced on 24 of October 1995. The objective of this directive is to set up a regulatory framework seeking to find a balance between protection of the privacy of individuals and the free movement of personal data within the EU. It applies to data processed by automated means. The directive also demands each member state to set up an independent national body responsible for the protection of such data. The Finnish implementation of this directive from information security perspective is addressed in the later chapter. (European Union 1995)

On 25 of January 2012 EU introduced a proposal for a directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Main purpose of this directive is to unify the information protection legislation in all the member countries. As of writing this thesis no new proposal has been published nor a final directive been approved.

Act on the Protection of Privacy in Electronic Communications 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector was introduced on 12 July 2002. The directive required all the member states to amend and harmonize their legislation to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy in electronic communications sector. The Finnish implementation of this directive from information security perspective is addressed in the later chapter about Act on the Protection of Privacy in Electronic Communications. (European Union 2002)

3.2 National legislation

There is no common information security act that includes all the information security requirements in Finland. The requirements are integrated into the other legislation. The requirements start from the constitutional law and end at the decisions of ministries and guidelines originating from agencies, such as the Communications Regulatory Authority, that only affect a specific industry.

Recognition of national legislation is especially important in governmental organizations, as the management of specific organization must ensure that the organization has identified the key information security legislation, and that the organization fulfils the information security requirements. Especially the recognition of requirements based on the Decree and information security levels on the basis of that Decree. The following chapter describes the most important information security related laws from the Finnish legislation.

Premise for all information security is the *Constitution of Finland* (Finland 1999) and notably the section 10. It defines that “everyone’s private life, honour and the sanctity of the home are guaranteed” and continues later “the secrecy of correspondence, telephony and other confidential communications is inviolable”. These sections are expanded in more detail in other laws and some limitations are also introduced. Limitations concern mainly situations involving crime and therefore the absolute inviolability can be differed from. In practice these definitions already require a number of actions in order to ensure the requirements from the law are met.

Act on the Openness of Government Activities (Finland 1999) defines that “all official documents must be in the public domain, unless otherwise provided in this or another act. It defines the right to access official documents in the public domain, officials’ duty of non-disclosure, document secrecy and any other restrictions of access that are necessary for the protection of public and private interests, as well as on the duties of the authorities for the achievement of the objectives of the Act”. Objective of the Act is to “promote openness and good practice on information management in government, and to provide individuals and corporations with an opportunity to monitor the exercise of public authority and the use of public resources”. The act also includes a list of information that must be classified. The Act uses the three levels of classifications from level IV (Restricted) to level II (Top Secret). These levels are directly linked to the information security levels that are described in later chapters of this thesis.

Decree on Information Security in Central Government (Finland 2010) contains provisions on the general information security requirements applicable to the handling of the documents by central government authorities, on the grounds for classifying documents, and on the information security requirements corresponding to the classification and applicable to the handling of documents. A central government authority is responsible for the planning of information security pursuant to good practice on information management, based on inquiries and the assessments conducted by it, regarding documents in its possession, and the significance of their contents. According to the act, in order to implement the basic level of information security, a central government authority shall ensure that:

1. Any information security risks connected with the activities of the central government authority are identified;
2. The central government authority has sufficient expertise for ensuring information security, and the related duties and responsibilities are defined;

3. The duties and responsibilities related to the handling of documents are defined;
4. Access to and availability of information in different situations are safeguarded, and procedures are created to overcome exceptional situations;
5. The secrecy and other protection of documents and the information contained therein are safeguarded by granting access to documents only to those who need secret information or personal data recorded in a personal data file for performing their work duties;
6. Unauthorised modification and other unauthorised or inappropriate processing of information is prevented by access rights management, access monitoring, and appropriate and sufficient security arrangements concerning information networks, information systems and information services;
7. The premises for data processing and storage of documents are sufficiently monitored and protected;
8. The reliability of personnel and other persons performing tasks related to the handling of documents is ensured, if necessary, by means of a security clearance procedure and other means available by virtue of law;
9. The personnel and other persons performing tasks related to the handling of documents are provided with instructions and training for the appropriate handling of documents and the information contained therein;
10. Compliance with given instructions is monitored, and the need to revise the instructions is assessed regularly.

In addition to these, the information security measures shall be planned and implemented so that they cover all stages of handling a document, ranging from the preparation or reception of the document to the filing or destruction thereof, including the provision and transfer of the document and the supervision of the handling. In the planning, compliance with data processing obligations shall be ensured also when data processing tasks are carried out on commission of central government authorities.

Act on international information security obligations (Finland 2004) defines the provisions on the measures of the authorities required to implement the international information security obligations. This law is also applied to a company and its employees when the company is party to a contract or subcontractor in a classified project defined in the Act on public defence and security procurement (Finland 2011), or participates in competitive bidding preceding such contract, or when company asks for security clearance or estimate to be made in order to participate as a party to a contract or subcontractor or in a competitive bidding of such contract with authority of another State or a company established in that State.

Archives Act (Finland 1994) handles national archives service, records and archives management and its organisation, preparation, preservation and use of records, and private archives. It defines the documents that must be archived permanently. National Archive Service is responsible for ensuring the preservation and availability of records, to promote research and to guide, develop and study archives and records administration.

The objectives of *Personal Data Act* (Finland 1994) are to implement, in the processing of personal data, the protection of private life and the other basic rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practices. This Act is applied to the automatic processing of personal data. It also applies to other processing of personal data where the data constitutes or is intended to constitute a personal data file or a part of such. It does not apply to the processing of personal data by a private individual for purely personal purposes or for comparable ordinary and private purposes, nor does it apply to personal data files containing, solely and in unaltered form, data that has been published by the media. The Act also defines the general rules on the processing of personal data, which are duty of care, defined purpose of processing, exclusivity of purpose, general prerequisites for processing, principles relating to data quality, and description of file.

The purpose of the *Act on the protection on privacy in working life* (Finland 2004) is to promote the protection of privacy and other basic rights safeguarding the protection of privacy in working life. The Act lays down provisions for the processing of personal data about employees, the performance tests and examinations on employees and the related requirements, technical surveillance in the workplace and retrieving and opening employees' electronic mail messages. In short, the employer is only allowed to process personal data directly necessary for employment relationship of the employee, which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arise from the special nature of the work concerned.

The objective of the *Act on Electronic Services and Communication in the Public Sector* (Finland 2003) is to "improve smoothness and rapidity of services and communications as well as information security in the administration, in the courts and other judicial organs and in the enforcement authorities by promoting the use of electronic data transmission". Chapter two of the Act defines the information security responsibilities of the authorities. Authorities must ensure an adequate level of information security both in their services to customers and in the communication between themselves. They must also ensure that the services are accessible to the customers and other authorities also outside the office hours.

Chapter 38 of *The Criminal Code of Finland* (Finland 1889) contains some of the oldest information security related legislation in Finland, the confidentiality of correspondence. Data and communications offences (secrecy offence, secrecy violation, message interception, interference with communications and computer systems, and computer break-in) require intent, thus intentionality, but it is possible to be guilty of these unintentionally, for example in situations of unauthorized reading of email without the correct procedures or jurisdiction. Data protection offence is the only one of the data and communications offences that may be punished for intent, but also of negligence.

As we can see from the previous chapter the information security legislation in Finland is divided into multiple different laws and regulations. There is no one information security law that describes the requirements. Because of this it can be problematic for organisations to create from scratch information security management systems that cover the complex requirements of the law. Therefore it is recommended to use previously generated standards as a checklist to ensure that all legislative requirements are met. On top of that, organisations must note industry specific legislation and regulation in their own information security management systems.

3.3 Information security levels

Information security levels specify administrative and technical requirements for organisations and information processing environments. Every central governmental organisation must implement the requirements relating to information security activities and processes described in the information security levels. There is no statutory requirement for the implementation, but the fulfilment has been carried out in other ways. Some of the requirements are already included in obligations for public administration to follow good IT governance practices. For example, some organisations may demand the fulfilment of the requirements set in information security levels before participating in information exchange or providing services. (Ministry of Finance 2010)

Administrative and technical information security levels are classified into three levels: base level, increased level and high level of information security. The minimum required level for central government agency is currently the base level of technical and administrative information security. This level allows the handling of level IV classified information. Increased level allows the handling of level III classified information and the high level handling of level II classified information. (Ministry of Finance 2010)

3.4 VAHTI

The Government Information Security Management Board (VAHTI), established by the Ministry of Finance, is responsible for the steering, developing and coordinating of central government information security. All significant central government information security policy and guidance matters are handled by VAHTI. They also support the Government and the Ministry of Finance in decision-making as well as in the preparation of decisions relating to central government information security. Ministry of Finance (2010) defines the objective of VAHTI as "improve the reliability, continuity, quality, risk management and contingency planning of central government functions and to promote information security so that it becomes an integral part of central government activity, steering and performance management." As a part of promoting the information security, VAHTI publishes instructions for governmental organisations to help them to implement good information security practices. (Ministry of Finance 2010)

3.4.1 VAHTI instructions

VAHTI publications have been issued since 2000 and currently there are 47 effectual information security guidelines and regulations. These publications are divided into eight areas of information security, these being physical, administrative information, personnel, operations, equipment, software, information material, and data-communications security. VAHTI information security instructions are described to be one of the most comprehensive sets of information security instructions in the world. Along with public administration these instructions are used in the international information security and co-operation, business, companies, communities as well as in education and civil activities. (Ministry of Finance)

One of the most important publications for the central government organisation is the Instructions on Implementing the Decree on Information Security in Central Government, which covers the topics needed to ensure the continuity and quality of official activities as well as the implementation of due process of law. This publication is intended for the management of organisations and for those responsible within organisations for security, information services and information management. Other publications are for more specific systems and processes, e.g. guidelines for logging and protection of internal networks. (Ministry of Finance 2010)

3.5 Cyber security strategy

Finland, as an information society, relies on information networks and systems and, consequently, is extremely vulnerable to disturbances, which affect their functioning. For this reason, the Finnish Government gave a resolution on cyber security strategy on 24 January 2013. The Strategy defines the key goals and guidelines which are used in responding to the threats against the cyber domain and which ensure its functions. By following the strategy it is possible to manage deliberate or inadvertent disturbances and also respond and recover from them. The Cyber Security Strategy is an element in the implementation of the Security Strategy for Society, which defines the principles of ensuring the functions vital to society.

The Security Committee approved the first national implementation plan for the Cyber Security Strategy on 11 March 2014. According to the Security Committee (2014) the plan will speed up the implementation of the Cyber Security Strategy by proposing concrete methods to improve cyber security. The plan includes a total of 74 measures, compiled from various administrative branches and the security of supply organisations. The central development targets for the plan are to create the Cyber Security Centre to provide round-the-clock information security status reports, to start the integration project of encrypted data transfer and administrative security network, to provide police with action-taking capacity in combating cyber crimes, to develop the cyber domain and cyber security related legislation, and to start research and training programmes to strengthen cyber security and other competences. (The Security Committee 2014)

3.6 Management frameworks and tools

This chapter explains the main frameworks and tools used in information security management. For the tools that can also be used in other contexts than information security, the basic way of usage is explained with examples from information security management. Frameworks chosen for this chapter are mainly used in information security management, IT governance, and management. First two chapters introduce decision making and development tools that can be used with the frameworks introduced in the later three chapters.

3.6.1 PDCA

In the traditional sense, PDCA (Plan, Do, Check, and Act) is a fundamental tool to implement continual change. It helps to continually change and tweak your processes, achieve higher quality results and processes, and it helps to gain continual increases in work efficiency. It is also a tool to assist in working logically and systematically. In other words, it is a problem solving and development model. PDCA concept was originally made popular by Edwards Deming.

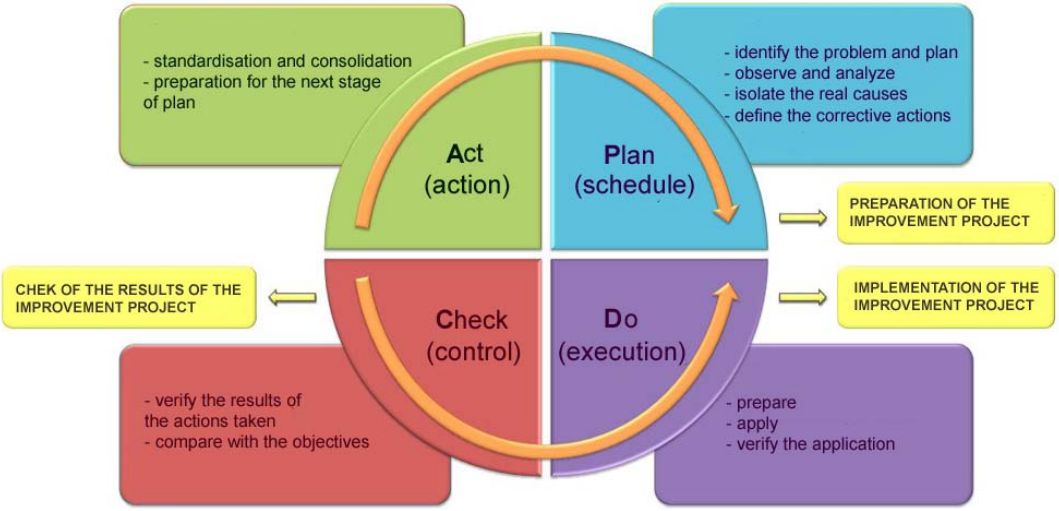
- standardisation and consolidation
- preparation for the next stage of plan
Act (action)
Plan (schedule)
- identify the problem and plan
- observe and analyze
- isolate the real causes
- define the corrective actions
PREPARATION OF THE IMPROVEMENT PROJECT
CHEK OF THE RESULTS OF THE IMPROVEMENT PROJECT
Check (control)
Do (execution)
IMPLEMENTATION OF THE IMPROVEMENT PROJECT
- verify the results of the actions taken
- compare with the objectives
- prepare
- apply
- verify the application

Figure 2 PDCA model. (Work Life Management)

To carry out a process according to the PDCA model you have to systematically follow the four stages and then repeat the process. In the first stage you create a detailed plan that identifies the goals, delegates work and sets a clear action plan for the different milestones. Each state must be documented in order to analyze the effectiveness of the actions later. Once the plan has been created it is time to put it in action. In the do stage, the plan is executed and all problems encountered are documented. Documentation also includes responses to the problems. After the project has been finished, it is time to check the results of the actions and the encountered problems. The aim in the check stage is to go through each step, identify what happened and why the problems were encountered. In this stage is it also important to come up with solutions to each encountered problem, because in the last act stage the aim is to correct all the problems identified in earlier stages. After all the stages have been cleared you end up back to the planning stage, where everything is evaluated once again and a new plan is created to further enhance the operations and processes.

3.6.2 OODA-loop

The OODA loop is a decision cycle, developed by John Boyd. This cycle is often applied to strategic military operations, but recently it has also been applied to information security. (Tipton & Krause 2009, 66) The OODA loop by Boyd, compared to the more traditional PDCA model, provides more effective methods to react to information security incidents and proactively fight against them. The diagram below illustrates the cycle of the OODA loop.

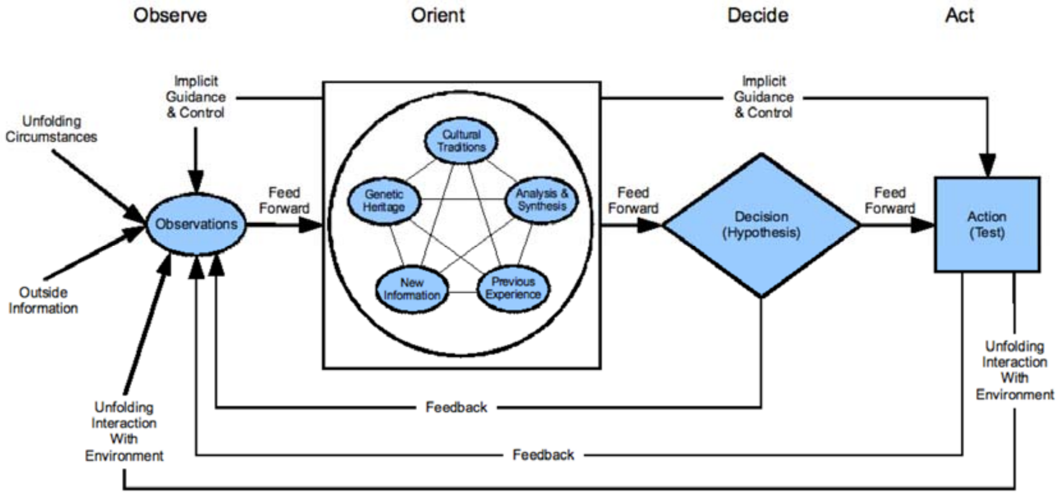

Figure 3 OODA Loop. (Alleman 2011)

The OODA loop can be seen as a simple, yet complex overview of how human brain processes information and how it reacts to it. At the observation stage you observe your surroundings with your senses. In information security we can see this as an activity of actively monitoring or scanning networks. In the next stage you orient on what is happening around you and apply information from your long-term memory to put it all into context. When looking at this from an information security perspective, we can see this stage of analysing the data from our scanning and comparing it to previous activities. After we have gathered and analysed the information it is time to decide what we do with this information. In the decide stage we choose one activity from all the activities we have at hand. In the information security context this could be, for example, to make a decision to start filtering connections coming to a specific port. When we have observed the situation, oriented to it, decided what we want to do about it, the final stage is to act. We put our plans into action and return back to the observer stage to see the effects of our actions. At any stage it is possible to fall back and return to the observe stage. For example, this might happen if the other side makes a decision before us, which then affects our decisions or actions. (Stephens 2013)

The OODA loop requires fast decisions and actions. Therefore it might not be the best decision making cycle for slow phase situations. Threats in information security happen fast and therefore the possibilities of preventing incidents through an OODA loop might be better than by using the traditional PDCA model. Support for this claim can be obtained when we look at the new ISO 27001:2013 Information Security Management System standard. Although the conventional PDCA model has been excluded from the new standard, it is still present between the lines. However, it is not actively brought out.

3.6.3 ISO 27000

ISO/IEC 27000:2013 refers to the ISO (International Organization for Standardization) standard family which provides organizations with a standard for information security management and general structure for the management system. This standard is created by a wide variety of organizations and compiled by the International Organization for Standardization. Organizations involved in this process are national operators such as the BSI (British Standards), European level actors such as the CEN (European Committee for Standardization) and international actors such as IEC (International Electrotechnical Commission). (ISO 27000 Directory 2007)

The ISO 27000:2013 series currently consists of four individual documents. The first document of this series is the ISO 27001:2013 which is the specification for an information security management system. Second document, 27002:2013, is the code of practices for information security. Third document is the ISO 27003:2010, which is intended as a standard to offer guidance for implementing an information security management system. ISO 27004:2009, the fourth document of the family, covers the metrics and measurements for an information security management system. These measurements and metrics are aligned with the previous version of ISO 27002:2005 controls, but are in process of being updated to correspond with the new ISO/IEC 27001:2013 (ISO 2013)

ISO/IEC 27001:2013 covers the establishment, implementation, maintenance and continual improvement of an information security management system. It also has requirements to assess and treat information security risks. All the requirements set in the ISO 27001:2013 are generic and intended to be applicable to all organizations, regardless of the size or nature. (ISO/IEC 27001 2013) The 2013 version is the first revision of the ISO 27001. According to the BSI Group it has “taken account of practical experience of using the standard.” (BSI UK 2013, 4) The standard no more guides the organizations to use the PDCA model, but gives them more flexibility to choose their own framework. However, it can be seen from between the lines that the PDCA model is still there. The new revised ISO 27001 has also been structured to match the previously updated ISO 9001 standard for quality and ISO 22301 standard for business continuity. The new version is also aligned with the recommendations from the ISO 31000 standard for risk management. (BSI UK 2013, 4)

ISO/IEC 27002:2013 provides the organizations with guidelines for information security standards and practices including the selection, implementation and management of controls the organization should take into consideration in the organization’s information security risk environments. It is designed to help the organization to define the controls with the process of implementing an information security management system based on the ISO/IEC 27001:2013. It also includes implementation of commonly accepted information security controls. ISO 27002:2013 also has guidelines for organizations to develop their own information security management guidelines. (ISO/IEC 27002 2013)

ISO/IEC 27003:2010 is focused on the critical aspects needed to successfully design and implement the information security management system for the organization in accordance with the previous version of ISO 27001:2005. This document is also in process of being updated to match with the requirements of the new revised version ISO 27001:2013. ISO 27003:2010 describes “the process of information security management system specification and design from inception to the production of implementation plans.” It also describes “the process of obtaining management approval to implement an information security management system, defines a project to implement an information security management system, and provides guidance on how to plan the information security management system project, resulting in a final information security management system project implementation plan.” (ISO/IEC 27003 2010)

As mentioned already above, the ISO/IEC 27004:2009 is designed to provide the organization with guidance to develop and define metrics and measurements in order to assess the effectiveness of the implemented information security management system. (ISO/IEC 27004 2009)

As we can see from the previous chapters, the ISO 27000 family of information security management system development is a very mature documentation. It has been refined with one revision to correspond more with the current needs of information security management. This framework will be referenced later in this thesis in the information security management system chapter where it is compared to other frameworks that can be used to implement an information security management system for an organization.

3.6.4 ISF

Information Security Forum (ISF) is a global organization, which has over 300 members worldwide. ISF publishes an annually updated Standard of Good Practices for Information Security publication, which is one of the most important and used publications they publish. It includes a business oriented practice for improving the information security of organizations. The standard provides the best practices for information security based on the studies conducted by ISF. The standard contains 30 chapters and a total of 135 controls. The basic idea is to fulfill all of the controls, if there is no business oriented obstacle for it. Each chapter includes a general overview of the controls in that chapter, control objective or the reason why it should be implemented, and the controls themselves. It is not possible to certify an organization based on the ISF standard, but the standard is a good starting point for an information security management system that fulfills the requirements of the ISO 27001 standard. (Laaksonen et al. 2006.)

3.6.5 COBIT

COBIT (Control Objectives for Information and related Technology) is a framework developed by ISACA (Information System Audit and Control Association). According to Laaksonen et all (2006) COBIT provides organizations' management with tips on how to combine business operations and the objectives of IT operations, and also how to measure these objectives. It also helps organizations to understand, which tasks and functions are included in the IT procedures of the organization. COBIT is a technology independent framework, which makes it a very general framework. It does not provide a view on how operations should be, but provides an overall structure for them. For in-depth guides an organization should use standards and other information security related frameworks such as VAHTI instructions. (Laaksonen et al. 2006)

COBIT 5 is the newest version of the COBIT family. Compared to other versions, it includes a new part called COBIT 5 for Information Security, which provides organizations with "a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT." (ISACA 2012) In other words, it tries to keep the balance between realizing benefits and optimizing risk levels and resource use. COBIT 5 for Information Security is built on the COBIT 5 framework and according to ISACA (2012) it "provides more detailed and more practical guidance for information security professionals and other interested parties at all levels of the enterprise".

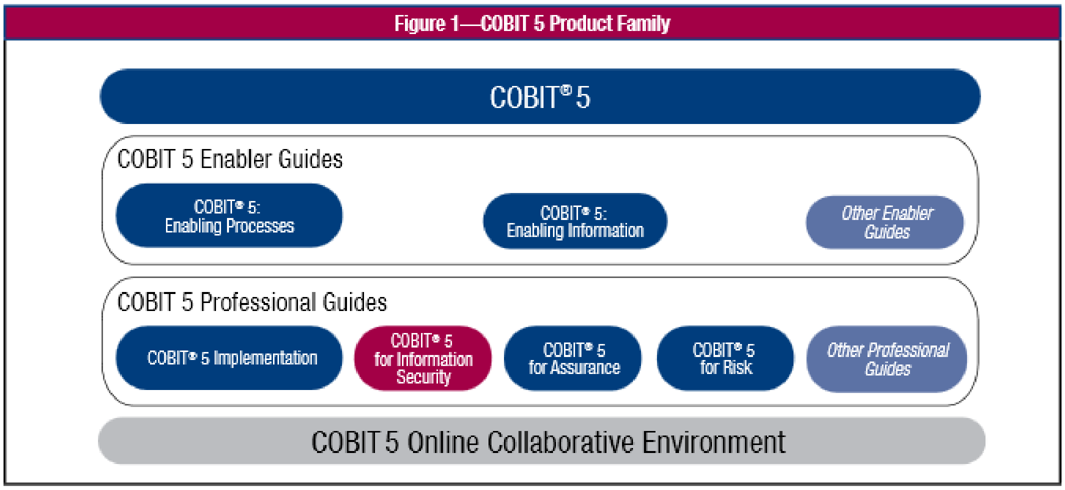
Figure 1—COBIT 5 Product Family
COBIT® 5
COBIT 5 Enabler Guides
COBIT® 5: Enabling Processes
COBIT® 5: Enabling Information
Other Enabler Guides
COBIT 5 Professional Guides
COBIT® 5 Implementation
COBIT® 5 for Information Security
COBIT® 5 for Assurance
COBIT® 5 for Risk
Other Professional Guides
COBIT 5 Online Collaborative Environment

Figure 4 COBIT 5 for Information Security in the COBIT 5 Framework (ISACA 2012)

According Laaksonen et al. (2006), the controls defined by the COBIT include the information owned or held by the company, and also information systems, operating environment, and people handling the information. COBIT has been divided into four different categories, which are called domains. The domains include 34 processes, which can also be called controls. All the processes also include hundreds of activities. Topics covered by COBIT are plan and organize (PO), acquire and implement (AI), deliver and support (DS), and monitor and evaluate (ME).

Plan and organize (PO) includes creating strategy and policies. This topic covers the best ways to achieve the objectives set for the IT procedures. These strategic intents must be communicated to different parties, such as employees and other stakeholders. This step helps the organization to see if they understand the organizations operational environment, and if they have recognized the risks related to information security. In the acquire and implement (AI) phase the organization has to identify the information systems, acquire the possible missing systems or update the existing ones. In this phase the information systems must also be integrated to the business of the organization. This part is crucial for the organization in order to utilize the ITstrategy created in the previous phase. Deliver and support (DS) deals with the topics related to delivering the services, such as information security and business continuity, support functions and other requirements from the users. This phase helps the organization to identify if the systems are used securely and efficiently, are the IT costs optimized and if the information is available. Last phase, the monitor and evaluate (ME) helps organizations to monitor and develop their IT processes to match the needs of the organization. It show the organization if their metrics are measurable, if they have identified all the relevant areas in the metrics, and also helps the organization to concretely measure them. (Laaksonen et al. 2006)

3.6.6 ITIL

The ITIL (Information Technology Infrastructure Library) is a collection of best practices of IT service management. It provides a cohesive set of best practices taken from the public and private sectors. The ITIL provides a model for measuring the effectiveness of information systems and management. The ITIL has a four P model (People, Processes, Products, and Partners) that requires management to combine these factors in the most effective and workable combination. The ITIL is divided into seven different categories. These being Service Delivery, Service Support, Planning to Implement Service, Security Management, ICT Infrastructure Management, The Business Perspective, and Application Management. In the Security Management chapter ITIL defines the principle for information security management to be that information security must be taken into account already in the planning of services. ITIL also requires regular inspections and reporting of the current state of information security. According to Laaksonen et al. (2006) this principle does not differ that much from the requirements of ISO 27001.

According to the ITIL, the management of the organization is responsible for defining the information security principle and ensuring that it is being followed. First the information security policy is compiled. Then the organization must perform a risk assessment and analysis of the current state, from which the needed security controls are planned. The organization must take into consideration the local laws and regulations. The planned controls must be included into everyday activities and the state of them must be monitored with various inspections.

4 Information Security Management System

This chapter introduces the reader to the topic of information security and information security management. First the theories and concepts of information security, then the information security management practices are explained. This chapter also gathers best practices from various information security management systems explained earlier to introduce the reader to the basics of information security management systems.

4.1 Information security

According to von Solms (2000), the so-called first wave of information security was characterized by a very technical approach. Information security was limited to simple identification and authentication forms. As the computing and information handling decentralized to desktops connected by networks, the risk of unauthorized access to information increased. At this point it was realized that the information security needed management and was more and more related to humans instead of purely to technical aspects. Von Solms (2000) calls this reversal the second wave of information security. The third wave, according to von Solms (2000), emphasizes that the information security should be incorporated into everyday processes performed by company’s employees and an information security culture should be cultivated throughout the company. According to Veiga and Eloff (2007), as the information security has evolved over time, the focus has shifted more and more towards a people- and governance-orientated approach.

Decree on information security in central government (681/2010) defines information security as “administrative, technical and other measures and arrangements to comply with secrecy obligations and restrictions on use related to information, as well as to ensure access to information and its integrity and availability.” There are also three widely agreed requirements or components of information security, irrespective of the tradition of information security from which they emanate (e.g. Baskerville 1988; Parker 1998). These requirements are: information must not be disclosed to unauthorized parties (*confidentiality);* information must not be modified by unauthorized parties (*integrity*); information must be available to authorized parties when needed (*availability)*.

By comparing these views on how information security can be perceived, we can see that the basic idea behind all these views is the same. Information security consists of people, processes and technology working together. Only by combining these, educating and protecting the individual parts, we can assure the confidentiality, integrity and availability of information and therefore have effective information security measures.

4.2 Information Security Management System

As mentioned earlier, the objective of information security is to ensure the data confidentiality, integrity, and availability within information systems. (Smith, M. 1989) Contents of information security management systems vary with different researchers and institutions. According to Tudor (2001), any given information security architecture should contain five components:

- Security organization and infrastructure
- Security policy, standards and procedures
- Security baseline and risk assessment
- Security awareness and training programs
- Security compliance

The most essential of these according to Hong (2003), is the security organisation and infrastructure. ISO 27000 standard families' structure for the information security management systems differ from Tudor views, but still include the same basic idea behind the structure. ISO/IEC 27002 (2013) defines the structure of information security management systems as follows:

Information security policies	Management direction for information security
Organisation of information security	Internal organisation
	Mobile devices and teleworking
Human resource security	Prior to employment
	During employment
	Termination and change of employment
Asset management	Responsibility of assets
	Information classification
	Media handling

Access control	Business requirements of access control
	User access management
	User responsibilities
	System and application access control
Cryptography	Cryptographic controls
Physical and environmental security	Secure areas
	Equipment
Operations security	Operational procedures and responsibilities
	Protection from malware
	Backup
	Logging and monitoring
	Control of operational software
	Technical vulnerability management
	Information systems audit considerations
Communications security	Network security management
	Information transfer
System acquisition, development and maintenance	Security requirements of information systems
	Security in development and support processes
	Test data
Supplier relationships	Information security in supplier relationships
	Supplier service delivery management
Information security incident management	Management of information security incidents and improvements
Information security aspects of business continuity management	Information security continuity
	Redundancies
Compliance	Compliance with legal and contractual requirements
	Information security reviews

When comparing these two approaches it is clearly interpretable that the ISO 27000 approach is more detailed and hands on concerning the risks and issues around the whole information security field, whereas the approach of Tudor is more general and academic. Both have the same underlying principle, but still differ on how the matter should be approached. ISO 27000 approach relies heavily on the Annex A in the ISO 27001:2013, that defines a comprehensive list of controls from which the organisation must choose the ones that might occur in the organisation based on a risk analysis. ISO 27001:2013 recommends organisations to go through the list to ensure that all the aspects of information security are covered. It is also mandatory for organisations to create their own controls to the subject that are not covered in the Annex A.

When we introduce the structure of the information security levels to this comparison we can start to see the similarities of information security management systems more clearly. The structure of the information security level management part includes: (Ministry of Finance 2010)

Leadership	Strategic control
	Resourcing and organising
	Coordination of cooperation
	Reporting and communicating to stakeholders
	Management in special situations
	Reporting to management
Strategies and planning	Impact of operating environment
	Specification of Objectives
	Developing operations through risk assessment
	Operating network management
	Special situation management
People	Developing expertise and awareness, and sanctions
	Management of human resources and tasks
	Actions in special situations
Partnership and resources	Contract management
	Securing operations in special situations
Processes	Information resources management
Measurement	Assessment and verification of operations

In this report the technical information security side of Information security level has been bypassed, as this thesis is concentrating on the administrative side of information security management systems. Information security levels approach to the information security management system structure is simpler and not as heavy looking as the ISO 27000 approach. However it must be noted that the top headings in the table include numerous subtopics that must be taken into account when creating an organisation specific information security management system. (Ministry of Finance 2010)

All of the above frameworks include similar topics covered from different perspectives. ISO 27001 is concerned with the overall protection of information and aims for certification. Information security levels are governmental instructions that must be, according to the Decree on Information Security in Central Government, fulfilled by the central government authorities and is therefore more government orientated. There are multiple other standards and requirement lists that approach the subject of protecting information from different perspectives. For example, the Finnish national security auditing criteria (KATAKRI) is more concerned with the confidentiality of information, rather than the full confidentiality, integrity, and availability circle of information protection. (Ministry of Defence 2011)

Following chapters will describe why organisations need to consider implementing an information security management system, what kinds of resources must be allocated, and which are the crucial parts of information security management systems. Later chapters will also describe how an organisation should start developing their own information security management systems, and what kind of an approach it could take when developing one.

4.2.1 Need for ISMS

For governmental organizations, the need for an information security management system is easily justified. The Decree on Information Security in Central Government is unambiguous so that each central government organisation must fulfil the basic level of information security. The basic level is nowhere near a full and operational information security management system, but it is a starting point. The decree also recommends organisations to make a classification decision, but because of deliberate or negligent writing in the law, there is a loophole that does not force the organisations to make the decision.

In privately held organizations and corporations the need for an information security management system can come from various different reasons. European Network and Information Security Agency ENISA (2006) lists a few of the possible reasons. The reasons can be external, such as providing a competitive edge or a more respected organization image. External reasons can also be legal compliance or a requirement in bidding. Internal factors for implementing an information security management system can be business continuity, minimization of damages and losses, or simply a requirement from a well-informed board member or employee.

ENISA (2006) also notes that the employees of a specific organization are a far greater threat to information security than outsiders, and comes to the final conclusion that “security administration is a managed and NOT a purely technical issue”. These factors themselves should be enough for any organization to start implementing even the simplest information security management system to protect their most valuable information.

4.2.2 Approach to ISMS Framework

As already mentioned in the beginning of this thesis, according to ENISA (2006), security experts and statistics have confirmed that “information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness”. It is also recognized that the security and protection of information depends more on people than on technology. Most important resource an organization has for creating an effective and functional information security management system is the organization’s employees and their support towards the system.

Below is a possible information security management system framework that organizations can use as a support when creating their organization specific system. Most important part to understand from the framework is that information security management is a continuous process that must be developed and maintained at least annually, if not more frequently.

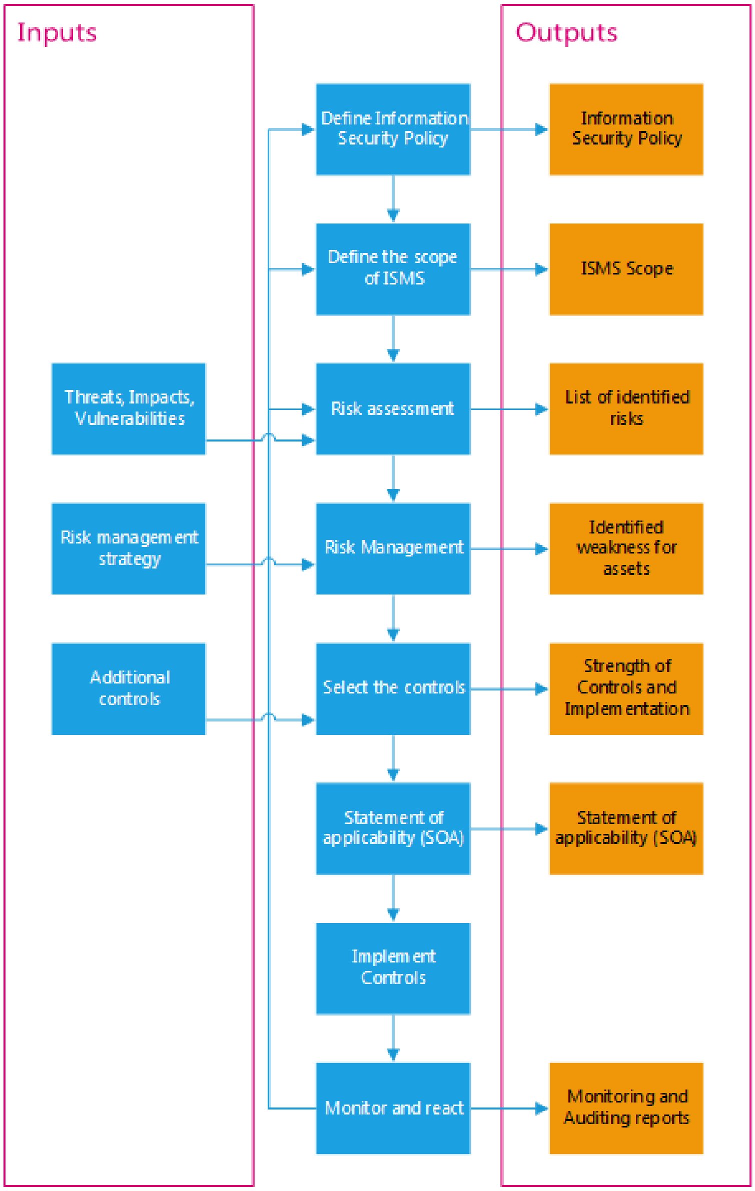
Inputs
Outputs
Define Information Security Policy
Information Security Policy
Define the scope of ISMS
ISMS Scope
Threats, Impacts, Vulnerabilities
Risk assessment
List of identified risks
Risk management strategy
Risk Management
Identified weakness for assets
Additional controls
Select the controls
Strength of Controls and Implementation
Statement of applicability (SOA)
Statement of applicability (SOA)
Implement Controls
Monitor and react
Monitoring and Auditing reports

Figure 5 Possible ISMS Framework approach (Based on ISO 27002 and ENISA)

The framework starts with the most important part of any information security management system, the upper management must create the information security policy, which is the base of everything that is done in the organization about information security. According to Kadam (2007), an information security policy should identify the key resources of the organization. The policy should also explain why these resources must be protected and who are responsible for the protection of the resources. It is also important to include if the policy is implemented throughout the company or if it is only for a specific branch or office. The policy should not include specific instructions, but serve as a top level document answering the questions of what, how, who, where and when.

After the information security policy has been accepted by the board, the organization must create the scope for the information security management system. The scope can already be defined on a general level in the policy itself, but the information security management scope document should have clear instruction on which operations or divisions of the organization the management system applies to.

Identifying the information related risks is one of the key steps in defining an effective information security management system. Risks can be effectively identified through risk assessment, which is a systematic process that includes identification of the risks, determining the consequences of the risks, and managing risks. (Aagedal *et al.* 2002) Inputs for the risk assessment can be previously identified threats, impacts and vulnerabilities. There are multiple ways for executing the risks assessment, but they are not covered in this thesis as the topic is in general the development of information security management systems.

According to Bojanc (2013), an effective risk management process is based on a quantitative analysis of identified security risks "that enable organizations to introduce optimum security solutions." After the organization has identified the risks, the organization identifies the possible controls to mitigate the risks. These controls can be selected from previously introduced standards. After selecting the controls, the organisation creates the statement of applicability document, that is a document which identifies controls chosen for your environment, and explains how and why they are appropriate. (Kosutic 2013) Last step in risk assessment and management process is to implement the chosen controls.

The basic information security management system should now be operational. However the process does not stop here. Organizations must implement a monitoring program to monitor the results of implemented controls. Results of this monitoring needs be used to update the existing policies, plans, scope, or controls.

Based on ENISA's research (2006) there are some critical success factors for a functional information security management system. First of all, the information security management system must have "the continuous, unshakeable and visible support and commitment of the organization's top management." It has to be managed centrally, based on common strategy and policies, and adopted across the entire organization. Most importantly, the information security management system has to be a never ending process.

5 Conclusion

This thesis sought to answer the question of what are the components of an effective information security management system. The first part of the thesis process opened this from the perspective of international and national laws and regulations. Second part focused on international and national standards and frameworks that can be utilized to create effective information security management systems.

During the writing of this thesis it came clear that Finland does not have a uniformed information security legislation that could be followed to guide to process of creating information security management system. The newly released national implementation programme of the cyber security strategy clarifies the responsibilities of national information security by assigning roles to various actors. It does not however provide support for those not working in the critical infrastructure, and therefore effectively leaving out great number of Finnish organisations. The cyber security strategy is a great start to improve the national information security, but is not enough alone. Therefore, the first suggestion of this thesis is for national actors to unify the legislation related to cyber and information security, and therefore making it more accessible to a wider audience.

Currently there are multiple international information security standards, which organisations can choose to adopt into their own processes. On a national level the VAHTI instructions and KATAKRI provide good start for the standardisation process for small and medium size organisation. However, these standards are created for a narrow special purpose and are not applicable to all situations. International standards can be with some effort modified to support the needs of Finnish organisations. The second suggestion of this thesis is to start developing a national standard for information security, which can be used as a guideline in creating an information security management system for any size organisation and which is specified for the needs of Finnish organisations.

During the writing of this thesis it came clear that information security management systems can be applied to an organisation of any size, but they easily grow to be too large to be effectively managed and follow. Therefore, it is critical for companies to carefully plan the information security management system, before starting to adopt it to cover all the processes of the organisation. Most important requirement for all these systems is the support from the upper-management and employees who are part of that system. The support must be visible and continuous in order for the system to stay functional.

References

Aagedal, J. et al. (2002), "Model-based risk assessment to improve enterprise security", Proceedings of the Fifth International Enterprise Distributed Object Computing Conference (EDOC 2002), Lausanne, Switzerland, 17-20, September.

Alleman, G. 2011. Wanna See Agile in the Real World? Accessed 11 April 2014. http://herdingcats.typepad.com/my_weblog/2011/06/wanna-see-agile-in-the-real-world.html

Baskerville, R. 1988. Designing information system security. United Kingdom: John Wiley Information System Series.

BSI UK. 2013. Moving from ISO/IEC 27001:2005 to ISO//IEC 27001:2013. Accessed 11 April 2014. http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

Bojanc, R. & Borka, J. 2013. A Quantitative Model for Information-Security Risk Management. Rolla: American Society for Engineering Management.

ENISA. 2006. Risk Management: Implementation principles And Inventories for Risk Management/Risk Assessment methods and tools.

European Union. 1995. Directive on the protection of personal data 95/46/EC. Accessed 16 December 2013 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF

European Union. 2002. Directive on privacy and electronic communications 2002/58/EC. Accessed 16 December 2013 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

Finland. 1889. The Criminal Code of Finland 19.12.1889/39. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

Finland. 1994. Archives Act 23.9.1994/831. Accessed 16 December 2013. http://www.arkisto.fi/uploads/Arkistolaitos/Teht%C3%A4v%C3%A4t%20ja%20toiminta/The-Archives-Act-831.pdf

Finland. 1999. Personal Data Act 22.4.1999/523. Accessed 16 December 2013. http://www.finlex.fi/en/laki/kaannokset/1999/19990523

Finland. 1999. The Constitution of Finland 11.6.1999/731. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf

Finland. 1999. Act on the Openness of Government Activities 21.5.1999/621. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/kaannokset/1999/en19990621.pdf

Finland. 2003. Act on Electronic Services and Communication in the Public Sector 24.1.2003/13. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/ajantasa/2003/20030013

Finland. 2004. Act on international information security obligations 24.6.2004/588. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Finland 2004. Act on the protection on privacy in working life 13.8.2004/759. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Finland. 2010. Government Decree on information security in central government 1.7.2010/681. Accessed 16 December 2013. http://www.finlex.fi/fi/laki/kaannokset/2010/en20100681.pdf

Finland. 2011. Act on public defence and security procurement 29.12.2011/1531. Accessed 16 December 2013. https://www.finlex.fi/fi/laki/ajantasa/2011/20111531

Hong, K. 2003. An integrated system theory of information security management. Bradford: Emerald Group Publishing, Limited.

ISACA. 2012. COBIT 5 for Information Security. Rolling Meadows: ISACA.

ISO. 2013. ISO/IEC 27001 – Information security management. Accessed 11 April 2014. http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

ISO 27000 Directory. 2007. Background Information. Accessed 11 April 2014. http://www.27000.org/background.htm

ISO/IEC 27001. 2013. Information technology — Security techniques — Information security management systems — Requirements. Switzerland: ISO copyright office.

ISO/IEC 27002. 2013. Information technology — Security techniques — Information security management systems — Requirements. Switzerland: ISO copyright office.

ISO/IEC 27003. 2010. Information technology — Security techniques — Information security management systems — Requirements. Switzerland: ISO copyright office.

ISO/IEC 27004. 2009. Information technology — Security techniques — Information security management systems — Requirements. Switzerland: ISO copyright office.

ISO/IEC 27005. 2011. Information technology — Security techniques — Information security management systems — Requirements. Switzerland: ISO copyright office.

Kadam, A. 2007. Information Security Policy Development and Implementation. New York: Taylor & Francis Ltd.

Kosutic, D. 2013. Statement of Applicability. Accessed 11 April 2014. http://www.iso27001standard.com/en/documentation/Statement-of-Applicability

Laaksonen, M. et al. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Ministry of Defence. 2011. National Security Auditing Criteria. Accessed 11 April 2014. http://www.defmin.fi/files/1871/KATAKRI_eng_version.pdf

Ministry of Finance. VAHTIn rakenteisen verkkosivuston ensimmäinen versio. Accessed 20 February 2014. https://www.vahtiohje.fi/

Ministry of Finance. 2011. VAHTIn toimintakertomus vuodelta 2011. Accessed 16 Dec 2013. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20120606VAHTIn/VAHTI_1_Toimintakertomus_2011.pdf

Ministry of Finance. 2010. Instructions on Implementing the Decree on Information Security in Central Government. Tampere: Tempereen Yliopistopaino Oy.

OECD. 2012. The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy. OECD Digital Economy Papers, No. 209. OECD Publishing. Accessed 16 December 2013. http://dx.doi.org/10.1787/5k8zq930xr5j-en

Parker, D. 1998. Fighting computer crime – a new framework for protecting information. New York: Wiley Computer Publishing.

Routio, P. 2007. Empiirisen tutkimuksen suunnittelu. Accessed 16 December 2013. http://www2.uiah.fi/projects/metodi/044.htm

Smith, M. 1989. Computer security - threats, vulnerabilities and countermeasures, Information Age, Vol. 11 No. 4, pp. 205-10.

State Treasury. 2013. Central government agencies and public bodies. Accessed 16 December 2013. http://www.suomi.fi/suomifi/english/state_and_municipalities/state_administration_and_central_government/central_government_agencies_and_public_bodies/index.html

Stephens, D. 2013. Understanding the OODA Loop. Accessed 4 February 2014. http://www.policemag.com/channel/careers-training/articles/2013/09/understanding-the-ooda-loop.aspx

Tipton, H. & Krause, M. Information Security Management Handbook. 2009. Broken Sound Parkway: Auerbach Publications.

The Security Committee. 2014. The implementation programme of the Cyber Security Strategy. Accessed 4 February 2014. http://www.turvallisuuskomitea.fi/index.php/en/kyberturvallisuusstrategia/toimeenpano-ohjelma

Tudor, J et al. 2001. Information Security Architecture. Boca Raton: CRC Press.

Veiga, A. & Eloff, J. 2007. An Information Security Governance Framework. Bristol: Taylor & Francis, Inc.

von Solms, B. 2000. Information security – the third wave? Computer & Security, issue 7. Elsevier Advanced Technology.

Work Life Management. The PDCA Method or Deming Wheel for Your Improvement. Accessed 4 May 2014. http://www.iwolm.com/en/the-pdca-method-or-deming-wheel-for-your-improvement/

Figures