Master Thesis in Information Systems

Faculty of Economics and Social Sciences
Agder University College - Spring 2007

Managing Information Security in Organizations

A Case Study

Are Nakrem

Managing information security in organizations
A CASE study

Master thesis in information systems
Spring 2007

Institute of information science, department of economy and social studies
HIA

By
Are Nakrem (are@nakrem.com)

1

Figure list

Abstract

During a participation in a security project in an enterprise in Norway, I have been able to get knowledge about the field of information security. The project leader told me that the method he was using has not been documented. The ideas of the way of handling information security has been used with another company in Norway, in a earlier project that he had also been project leader of. The main theme of the method was organizing the IT department into processes and roles, with tasks and responsibilities.

In my literature research I have found several ways of handling information security. There is no grounded theory in the field of information security, but there are several guidelines, frameworks and standards, and there is a lot of research about these. Most of these frameworks and standards are based on commercial use and not free of charge. I have also done research about the human factor, to verify that the topic is valid.

I have done a CASE study of the enterprise; to get detailed information of how they handled information security. I found that the method that has been used and has parallels to frameworks and standards I found in the literature research.

By my findings in the literature research and the CASE study, I have been able to develop a simple framework for handling information security in organizations. The framework is suited especially to medium organizations, with less ability to implement several frameworks and standards. Large companies can use frameworks like Cobit, ITIL and ISO standards.
The key elements of the framework is a three dimensional cube containing the elements of business requirements, IT resources and information security requirements. I have not found any framework in literature that has linked this combination together.

1 Introduction

Some years ago I read a book by the top selling writer Coelho, and would like to use the same expression as he used in his book. A reporter asked him if he could describe the aim of his book in one sentence. He answered that if he could do that, there was no need for him to write a whole book. The findings of this research can not be told in a sentence without telling the whole story.

In the last years information security has become a more important issue for most large companies around the world. These companies have also understood that better security cannot be achieved by just installing another security hardware device like a firewall or an intrusion detection system. Even the most secure system would not give you any security if the people operating it have the wrong attitudes and don't behave, as they should. It is a common understanding that information security heavily depends on the behaviour of the employees. Some say information security consists of 20% technical concepts and 80% human behaviour; some say the ratio is 10/90. In an AT&T Network Security survey from March/April 2003(AT&T, 2003) Meta Group estimates that "30% of IT security relates to technology, and 70% relates to people and practices".

In the research I have done is how to handle information security in a human perspective. To manage people, there has to be an organization in a business perspective. This combination of organization and information security is the main theme of this research work that has been done.

During participation in an information security project in an enterprise, I got good insight how this company has a model of how to handle information security. During this participation, the project leader told me that the model has not been documented. This gave me a great opportunity to do research about the model. I have done literature research about the theme to find any frameworks or models that are similar, that had been used in CASE enterprise.

1.1 Report outline

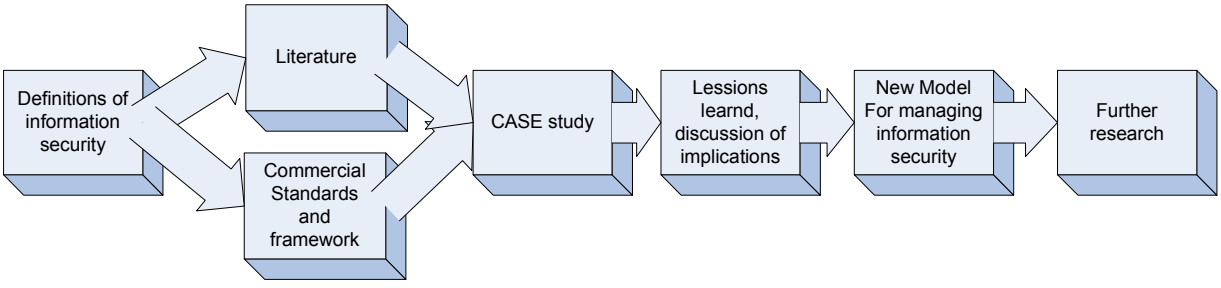


Figure 1 - Report outline

This is a visual view of how the report is conducted.

1.2 Research problem

Many organizations find it difficult and costly to handle the information security in a proper way. The question is whether organizations are able to handle these challenges. The research problem is how to solve information security in organizations.

I visual view of how the master thesis was done is shown below

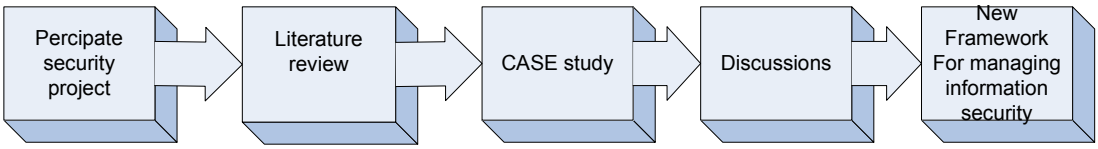


Figure 2 - Timeline of master thesis

In the next chapter I have discusses some definitions of information security and what definition I have used in this report.

1.3 Definition of information security

In order to do the research it is important to define what information security is about? Most definitions of information security tend to focus, sometimes exclusively, on specific usages and, or, particular media; e.g., "protect electronic data from unauthorized use". In fact it is a common misconception, or misunderstanding, that information security is synonymous with computer security.

The U.S. National Information Systems Security Glossary defines **Information systems security** as:

> *the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.*

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities (ISO-IEC 17799:2005).

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes (ISO-IEC 17799:2005).

Three widely accepted elements of information security are:

- confidentiality
- integrity
- availability

I have used this definition of information security in the master thesis. In the thesis I have also used two other definitions, that is important to this research.

1.3.1 Definition of IT Risks

In recent discussions in the profession, many authors say that the next level of information security is how to handle risks.

As a part of human nature we take risks. We take the risk for business opportunities, for recreation or just for fun of it. The world is one where we take and we need to take business risks to make venture. Logically, we would expect the higher risks to be up on the radar, and lower risks to be in the background, but that is often not the case (Jordan and Silcock, 2005)

Risk is the possibility of suffering loss (Scafer, 2004)

Risk is the potential impact (positive or negative) to an asset or some characteristic of value that may arise from some present process or from some future event. In everyday usage, "risk" is often used synonymously with "probability" and restricted to negative risk or threat. In professional risk assessments, risk combines the probability of an event occurring with the impact that event would cause. Financial risk is often defined as the unexpected variability or violability of returns, and thus includes both potential worse than expected as well as better than expected returns (ISO:IEC Guide 73).

A subset of management includes the processes concerning with identifying, analyzing, and responding to risks. It consists of risk identification, risk quantification, risk response development and risk response.

Risk management is about understanding the internal and external influences that can cause failure. Once a plan for action is built, a risk analysis should be performed. The result of the initial risk analysis is a risk plan that should be reviewed regularly and adjusted accordingly. The main purpose of risk management is to identify and handle the uncommon causes of variation plan. This is captured in a formal process in which risk factors are systematically identified, assessed, and provided for.

1.3.2 Definition of Security awareness

ISF (Information Security Forum) defines IT security awareness in this way:

> IT Security Awareness is the degree or extent to which every member of staff understands:
>
> - the importance of IT security
> - the levels of IT security appropriate to the organization
> - their individual security responsibilities
>
> … and acts accordingly.

This definition is important for this research, since the research is focused on organizations.

2

2.1 Literature review

In my research for a master thesis topic, I got knowledge from participation in an information security project. The project leader of the project told me that the idea of handling information security he is using has not been documented. I chose to have the content of this idea as the topic. The main essence of this way of handling information security was making an IT organization divided into roles, with tasks and responsibilities.

During this work I did a literature review of what have been published on the topic. There are written many books about the theme, some of them have a relevance to my topic. Most of these books are written to explain and propose a method of implement information security in a technical manner linked with security rules and policies.

Lot of literature has been published on the topic by accredited scholars and researchers. There seems to be many researchers done work by technical issues, and researches have been done about commercial standards. There are also a large number of surveys done. In the following chapters I have summarized the most important papers and researches to my subject. I have done search in literature by the expressions "information security"," management" and "organization". MIS Quarterly, Information Systems Management and Information Security Today have been resources to articles. I have also been searching in the IEEE, ISO, IT Governance Institute, Department of Trade Industry, Information Systems Audit and Control Association & Foundation (ISACAF) and Office of Governance Commerce organizations.

A search done in May 2007, gave me the result that there where 26 books, containing the phrase "information security management". A search performed at the electronically library at Agder University College, for "information security management" and articles released in year 2000 to February 2007, had the following results.

	Number of matches
Scirus (with Science Direct)	18134
Business Source Premier (EBSCO)	294
Academic Search Premier (EBSCO)	138
WorldCat (OCLC)	128
Library, Information Science & Technology Abstracts (EBSCO)	12
ISI Web of Science	8
Nora	6
SocIndex (EBSCO)	2
Econlit (EBSCO)	1
Eric (EBSCO)	1
Total:	18724

With this large number of books and articles, it was not possible to read all of them, so I had to dig manually into the list of articles to find them relative to my subject. I have narrowed the search to the year 2005 and newer to get the most up to date information, since there is much updated information. I have also narrowed my search so that I have found articles that have

brought something new to the subject. I have started with the most recent ones and then moved my backwards to get the history.

Since there are a lot of investments in the area of information security, there are many consultant companies that have done some work methodology or frameworks for implementation of information security in commercial companies worldwide. Most of these work methodologies are patented and protected. Most of these methods and frameworks are based on best practices and not based on research or the research is not shown to the public.

In magazines and conferences there has been more attention to IT Risks in the subject of information security. There are resent books about handling IT risks, which is interesting for my topic, like Beating IT Risks by Jordan and Luke (2006). There are many standards based on best practises, like IEC:ISO and Cobit. The most resent standard was in first edition 5. October 2005 (IEC:ISO 27001).

I have also attended two 2 conferences to receive up to date information about the subject. These conferences are Infosecurity Europe London 2006 and Norwegian ISF conference in Tønsberg 2006.

The main theme for this research is information security handling. I have found that the human factor is a interesting. In business and public sector there are organizations. I have searched for how to organize by looking for standards, models and framework, and how to get the organization aware of risks to information security.

To provide a further research, I have divided the literature about information security into a concept-centric approach (Webster and Watson, 2002). By reading literature about information security I have been able to divide the subject into the following concepts.

1. **Information Security Management** – characterizes the process of and/or the personnel leading and directing all or part of an organization through the deployment and manipulation of resources (human, capital, natural, intellectual or intangible).
2. **Information Security Organization** – how human resources are related and communicating to each other.
3. **IT Risks management** – understanding the internal and external influences that can cause failure, and how to handle these failures.
4. **Information Security Training/Awareness –** education and campaigns to the whole organization.
5. **Commercial and international standards** – information security / Governance

I have also looked at trends in the field of information security handling to verify that the topic is valid.

Thru the research process I have made the following literature framework to get an integrated view what I have found to be relevant to my subject.

Author	Manage-ment	Organization	IT Risks	Object security	Incident handling	Business continuity management	Compliance	Training / Awarenes ss	Behavio r
Information Security Architecture and Information Security Governance	X	X	X	X	X	X	X	X	X
COSO (SOX)	X	X	X		X		X		
ISO 27001/17799	X	X	X	X	X	X	X		
ITIL	X	X		X		X	X		
Cobit (SOX) Management and organization	X	X	X		X	X	X	X	
Li. et al.(2003)	X	X							
Siponen (2003)	X	X							
Solms (2005)	X	X							
Tejay (2005)	X	X							
Pattinson (2003)	X	X							
Pearson and Ma (2005)	X	X							
Behavior									
Rhee and Ryu (2005)	X								X
Stanton et.al.(2004)	X								X
Kolkowska (2005)	X	X							X
Mathisen (2005)	X							X	X
Albrechtsen (2006)	X	X						X	X
Human Firewall / Withman et.al (2005)		X						X	X
IT Risks by Jahner and Krcmar (2005)	X	X	X						

In the following module I will present a summary of the most relevant literature.

2.1.1 IT security management and IT security organization

There are plenty of standards, models and framework for information security management. On of the first standard was BS7799 that was released in 1999. A paper has been written by Li. et al. (2003) to present the BS7799 standard. They have presented this standard as a suitable model for information security. The BS7799 is based on a standard archived by best practices in the information security management area. Organizations have been using own developed frameworks earlier. They have concluded that this standard together with organization specific requirements is the most effective way of providing information security.

In the paper information security management standard: problems and solutions written by Siponen (2003) there has been a critically analyses of the three widely information security standards used in 2003 and earlier. The conclusion of this paper that these normative standards are claimed to be generally valid and not based on what is done in other organizations like in research approaches.

A survey done by Stamland (2004) about is BS7799 worth the effort. He has concluded that that organizations certified according to BS 7799-2 have a higher maturity in the organization versus organizations that have chosen to only use the standard in an informal way. Those organizations that use the standard informally have higher maturity than those organizations that do not implement any ISMS. He believes that the findings support the statement. BS 7799 will be worth the effort for organizations which needs to protect their assets.

Solms (2005) has written a paper to investigate the co-existence of and complementary use of COBIT and ISO 17799 as reference frameworks for Information Security governance. The investigation is based on a mapping between COBIT and ISO 17799 and provides a level of ‘synchronization’ between these two frameworks. He has present COBIT to positions itself as ‘the tool for information technology governance’. COBIT is therefore not exclusive to information security. It addresses Information Technology governance, and refers amongst many other issues, to information security. The downside of using COBIT for Information Security governance is that it is not always very detailed in terms of ‘how’ to do certain things. ISO 17799 is exclusive to information security, and only addresses that issue. The upside of using ISO 17799 for Information Security governance is that it is more detailed than COBIT, and provides much more guidance on precisely ‘how’ things must be done. The downside of using ISO for information security is that it is very much like “stand alone” guidance, not integrated into a wider framework for Information Technology governance. His suggestion is to use a mapping of the standards so it takes the best from both standards by make the very useful content provided by COBIT and the very useful content provided by ISO 17799, much more useful in implementing comprehensive and standardized Information Security governance environments.

Making sense of information systems security standards has been presented by Tejay (2005) in a paper. This paper concludes that there are a plethora of standards and it is not effective and economical to adopt these to organizations. A set of security standards working coherently as an integrated model and aligned with its business objectives is suggested. The set would integrate a minimum set of standards to cover maximum IS security needs of an organization.

An approach for IS Managers and internal auditors to establish the extent to which their organization complies with the international standard AS/NZS 17799 (IEC:ISO 17799) is proposed by Pattinson (2003). This approach incorporate a set of baseline IS controls, extracted from the standard, with a GAS-based (Goal Attainment Scaling) evaluation methodology.

Some researches have recognized that relationship between security objectives and practices are complicated, but important for practitioners to understand. Pearson and Ma (2005) have done a survey about objectives and practices in information security management by a canonical analysis based on data from 354 security professionals. In the survey they have found that "Confidentiality" is the highest correlation with information security practices. They concluded with that it is important that practitioners must take an appropriate management intervention to improve the effectiveness of information security management.

2.1.2 IT Security management and IT Security behaviour.

In a survey done by Rhee and Ryu (2005) they have found that there is a tendency of people to believe that negative events are less likely to happen to them than to others and that positive events are more likely to happens them than others. By the survey they have stated that this is also addressed in information security. They have concluded that it is necessary to address this issue when doing low level of user and managerial awareness as a key factor to achieve good information security in sense of reducing security breaches and their serious consequences.

Another survey done by Stanton et.al.(2004) concluded that positive and negative emotional workplace events and the subsequent behavioural outcomes emphasizes the influence of unique personal experiences at work than those factors that are shared across a variety of an organizations like norms, standards, rules etc. The results suggest that some practical opportunities for improving security may lie in changing the culture of the organization.

Value sensitive approach to information security is presented in a paper done by Kolkowska (2005). This paper is a contribution to the ongoing research efforts to view security problems from a more holistic, socio-organizational perspective. The approach is to help to identify organizational and individual values, since the objectives suitable for each organization can be identified by eliciting these values.

In a research done by Cline and Jensen (2004), they have examined changing information security requirements and the strategies organizations are developing to meet the related challenges. Many firms exchange information across internet, which have been a new challenge to handling information security. They have developed a theoretical framework with a set of questions by interviews, validated it and concluded with a suggested methodology. They have suggested using a practical lens approach. A practical lens (Orlikowski, 2000) is defined as that people are purposive, knowledgeable, adaptive, and inventive agents who engage with technology in multiplicity of ways. This perspective is advocated because it provides the much-needed flexibility required to investigate the problem of information security management.

2.1.3 IT Risk Management

In a paper written by Jahner and Krcmar (2005) they have present a theoretical motivated framework for analyzing the construct risk culture, to mitigate IT risks. They have written that standards, handbooks and guidelines in handling information security have approaches to provide broad guidelines rather than detailed set of recommendations. They have provided a statement that information security and IT security management are components of overall IT risk management.

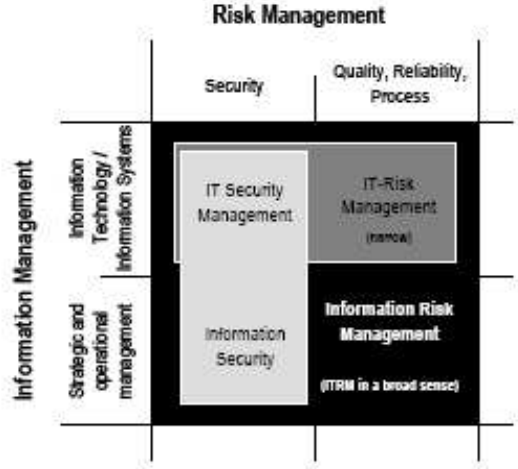


Figure 3 - Risk Management

From their empirical findings they have derived important factors for establishing risk culture such as communication campaigns or top-management involvement.

2.1.4 IT security Management and IT security training/awareness

Behaviour is an important factor in information security. To struggle bad behaviour there are written many articles about training and awareness. In the closing session, hackers panel, at Infosecurity Europe Conference 2006, all panel attendees agreed that technical barriers are lees important than the human factor. It is a common understanding that we are the greatest risk to our organizations.

Mathisen (2005) has written a master thesis about measuring Information security awareness. He has done a survey about the theme. The attitudes and awareness of the employees are very important for information security in a company of today. It is a common view that the people and their behaviour mean more to information security than all technical solutions. The survey has shown that the contacted companies and organizations do a lot of work trying to raise the awareness and improve the attitudes towards information security.

A quantitative study of users view on information security has been done by Albrechtsen (2006). This study discovered that users play an important role in the information security performance of organizations by their security awareness and cautious behaviour. Interviews of users in an IT-company and a bank were qualitatively analyzed in order to explore users' experience of information security and their personal role in the information security work. The main patterns of the study were: (1) users state to be motivated for information security work, but do not

perform many individual security actions; (2) high information security workload creates a conflict of interest between functionality and information security; and (3) documented requirements of expected information security behaviour and general awareness campaigns have little effect alone on user behaviour and awareness. The users consider a user-involving approach as much more effective for influencing user awareness and behaviour.

2.1.5 Human firewall

In 2000, a consortium of industry, government and academic representatives formed the Human Firewall Council, established on the premise that information security is a people problem, and a managerial problem that does have some technical solutions. In 2004 the Human Firewall organization changed hands, from the original commercial sponsoring organization to the ISSA. With this change came a need to revise and update the organization's Web site, an online survey that allowed respondents to benchmark their organizations with their peers, based on the ISO 17799 standard. This updated survey shows that information security continues to be a people problem (Withman et.al, 2005).

2.1.6 Information Security Architecture and Information Security Governance

In recent literature, there have been presented new information security management philosophies. I will present two of them in this chapter.

The concept of information security architecture was introduced by Killmeyer in 2000. She has written a book about the concept, and it was updated in a second edition in 2006. This security architecture includes the process of developing risk awareness, the assessment of current controls, and finally the alignment of current and new controls to meet the organization's information security requirements. Killmeyer clearly states that the security architecture is a process, and "… an Information Security Architecture is not something one can purchase" (Killmeyer Tudor, 2000). She has presented the following framework.

Figure 4 - Information Security Architecture

The architecture is based on the balanced and holistic mix of five different aspects, namely security organization and infrastructure; security policies, standards and procedures; security baselines and risk assessments; security awareness and training program, and lastly, compliance. Grobler and Lourwrens (2005) have also presented a model for information security architecture. The content of the framework is the same as the framework of Killmeyer (2000) but it has a different view of the framework.

A framework, "New information security architecture", PROTECT, has been presented by Eloff (2006). The model of Killmeyer (2006) has been extended with new dimensions. Organizations need to establish new security business structures based on an Integrated Architectural approach. An Integrated Architectural approach to Information and Computer Security should operate in a distributed, heterogeneous and multi disciplinary business environment. It is necessary for such an Architectural approach to include the issues Policy, Risk, Objectives, Technology, Execution, Compliance and Team.

- **P**olicy should include Responsibilities and disciplinary action especially for developers. Procedures, standards to support source code changes.
- **R**isk of disgruntled employees and Trojan Horses.
- **O**bjectives should address Availability and Integrity.
- Technology should be robust and reliable with regard to Change control software and RAS.
- **E**xecute – establish, maintain and manage a proper ISMS environment.
- Compliance – evaluate efficiency of software maintenance against code of good practice. Internal certification.
- **T**eam - responsible for interaction of security Team with programmers / developers. Security awareness of programmers. Ethical and social issues need to be addressed.

The framework of the PROTECT has not been released (January 2007), so I am not able to present it in this report. The information about PROTECT is found in lecture notes.

The framework "Information security governance" is another concept. This has been presented by Solms (2006) as Fourth Wave of information security management. The First Wave was characterized by Information Security being a technical issue, best left to the technical experts. The Second Wave was driven by the realization that Information Security has a strong management dimension, and that aspects like policies and management involvement are very important. The Third Wave consisted of the need to have some form of standardization of Information Security in a company, and aspects like best practices, certification, an Information Security culture and the measurement and monitoring of Information Security became important. The Fourth wave is about using development cycle and the role of information security Governance. Information Security Governance is an integral part of Corporate Governance.

2.1.7 Trends in information security breaches

DTI (Department of Trade Industry) had a research in 2006 about information security. The same survey was also done in 2004. The survey is done in United Kingdom.

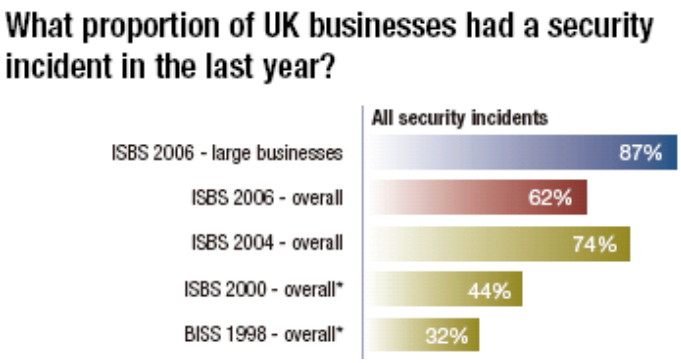


Figure 5 - Security Incidents

This shows a tendency of increasing incidents. The survey done by FBI, (2006) shows the changes in types of attacks.

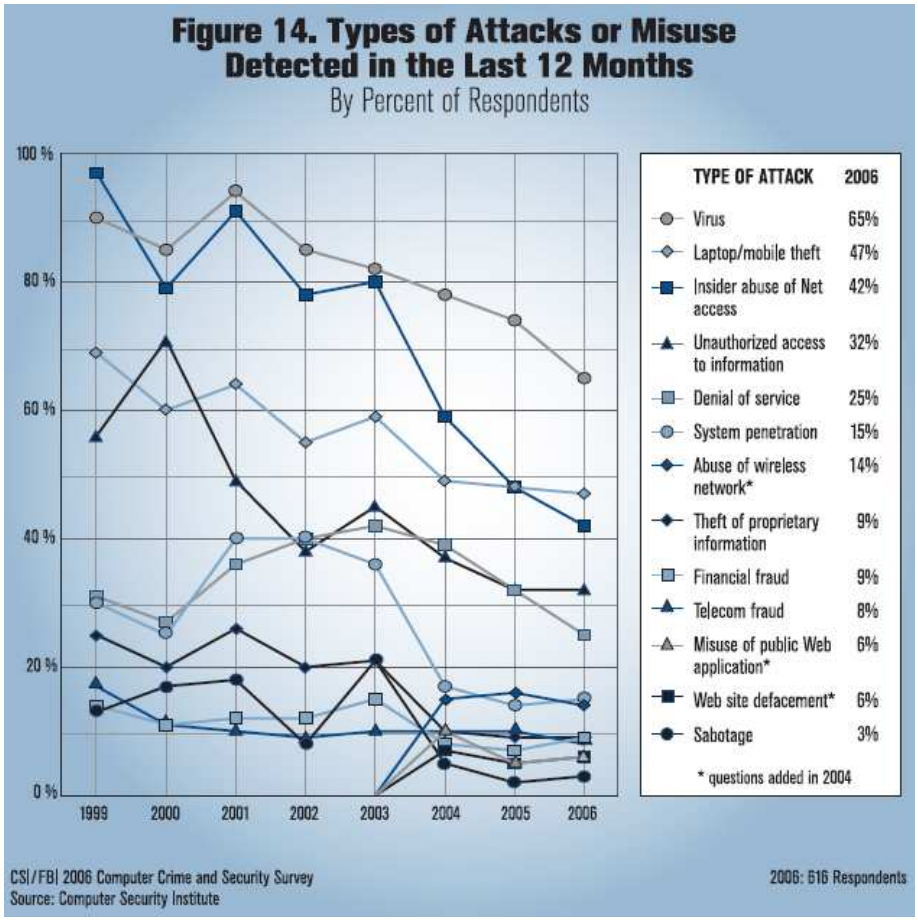


Figure 6 - Security Attacks

This survey shows that no. of incidents is not increasing, but incidents are still in place so they should be still dealt with.

A study of these surveys is not covered in this report, since they are not included as a part of this theme. I will use the conclusion that the security incidents and complexity are growing and that information security is still valid for

2.2 Commercial standards

It is perhaps inevitable that the increasing and frequently critical dependence on IT, together with the computer crime related aspects, has been accompanied by a whole range of legal and regulatory activities especially in the financial sector. Relatively recent examples of such legislation includes Sarbanes–Oxley Act(‘‘SOX’’) and Basel II which aims are to protect investors and shareholders from corporate fraud, bad investment decisions and poorly controlled systems. Other examples include Data Protection and Computer Misuse legislation. A lot of these legal and regulatory requirements need to be translated into IT terms and there are a number of standards that can assist in at area. Some of these standards are BSI, COBIT, GASSP, GMITS, ISF, NIST, IEC:ISO 27001 and IEC:ISO 17799:2005. In the next sections I have described some of the most widely used standards and the Sarbanes-Oxley Act.

2.2.1 ITIL - IT Infrastructure Library

An early framework developed was the ITIL (Information Technology Infrastructure Library**).** This framework was developed in the early 1980’s but was not adopted until in the 1990’s. This framework was developed by the UK office of commerce. The main components of the standard (version 3) are: IT Service Design, IT Service Introduction, IT Service Operations, IT Service Improvement and IT Service Strategies consolidating. This framework has a highly service orientated approach and is also adopted into the ISO 20000 standard.

This standard also includes information security management. They define information security management as The Process that ensures the Confidentiality, Integrity and Availability of an Organizations Assets, information, data and IT Services. Information Security Management usually has a wider scope than the Service Provider. It normally includes handling of paper, building access, phone calls etc., for the entire organization.

2.2.2 IEC:ISO standards

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

IEC:ISO17799 has been founded in 1987 as British Standard 7799 part 1 by the Department of Trade Industry (DTI). There were a growing interest to adopt the standard in many other countries worldwide, are the standard was adopted the IEC and ISO organizations.

The International Standard has been prepared to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The adoption of ISMS should be a strategic decision for an organization. The design and implementation of an organization's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organization. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organization, e.g. a simple situation requires a simple ISMS solution.

The 2005 version of the standard contains the following twelve main sections:

- Risk assessment and treatment
- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

ISO/IEC 27001 is an information security standard published in 2005 by the International Organization for Standardization and the International Electrotechnical Commission. Its complete name is *Information technology -- Security techniques -- Information security management systems -- Requirements*. The current standard is a revision of BS 7799-2:2002, which has now been withdrawn.

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS). It specifies requirements for the management of the implementation of security controls. It is intended to be used with ISO 17799:2005, a security Code of Practice, which offers specific security controls to select from.

An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and being managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process. The application of a system of processes within an organization, together with the identification and interactions of these processes and their management, can be referred to as a "process approach". The process approach for information security management presented in the standard encourages its users to emphasize the importance of:

- understanding an organization's information security requirements and the need to establish policy and objectives for information security;

- implementing and operating controls to manage an organization's information security risks in the context of the organization's overall business risks;
- monitoring and reviewing the performance and effectiveness of the information security system;
- Continual improvement based on objective measurement;

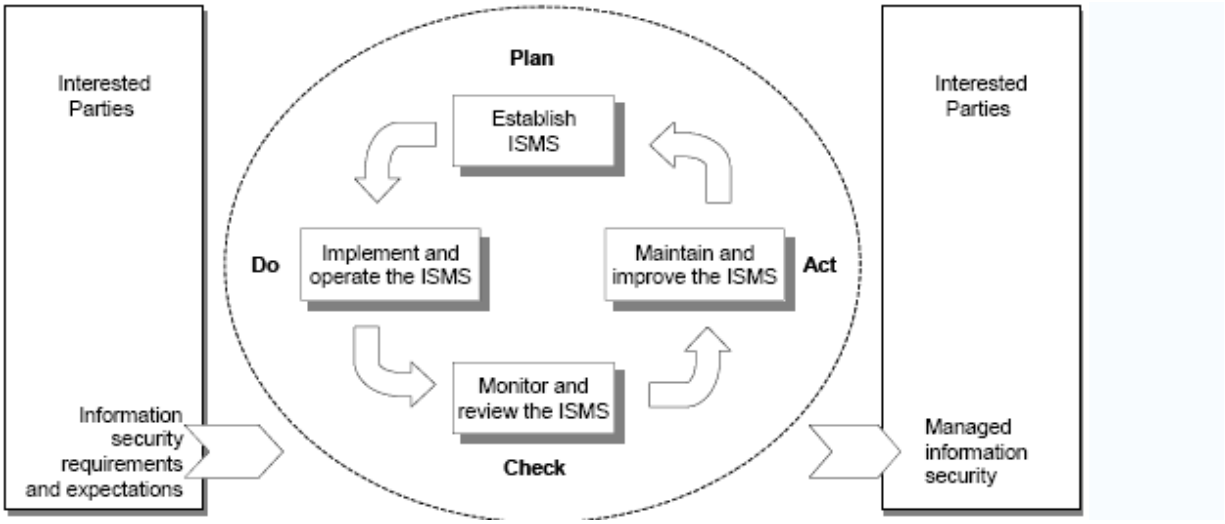


Figure 7 - ISO PDCA

This is also the first standard in a proposed series of standards which will be assigned numbers within the ISO 27000 series, and are specially assigned to security matters.

The complete range of the IEC:ISO 27000 series is to be :

ISO 27001 - This is the specification for an information security management system (ISMS) and replaces the old BS7799-2.

ISO 27002 - This is the potential new standard number of the existing ISO 17799 standard.

ISO 27003 - provide help and guidance in implementing the Information Security Management System requirements. It will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages on the PDCA process to establish, implement and operate, monitor and review, and improve the ISMS.

ISO 27004 - provides guidance to the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. It is intended to be applicable to a wide range of organizations with a correspondingly wide range of information security management systems. It provides guidance for measurement procedures and techniques to determine the effectiveness of information security controls and information security processes applied in ISMS. The purpose of the Information security management measurements development and implementation process, defined in this Standard is to create a base for each organization to collect, analyze, and communicate data related to ISMS processes.

This data is ultimately to be used to base ISMS-related decisions and to improve implementation of ISMS.

ISO 27005 - provides techniques for information security risk management that includes information and communications technology security risk management. The techniques are based on the general concepts, models, and management and planning guidelines laid out in Part 1 of this International Standard. These guidelines are designed to assist the implementation of information security. Familiarity with the concepts and models, and the material concerning the management and planning of information security in ISO/IEC 13335-1, is important for a complete understanding of Part 2. This document gives guidelines for information security risk management, which ISO/IEC 13335-1 of this International Standard specifies as one of activities that information security management requires to be carried out. ISO/IEC 27005 is applicable to any organization which intends to manage risk that could compromise the organization's information security.

ISO 27006 - to specify general requirements a third-party body operating ISMS (in accordance with ISO/IEC 27001:2005) certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration.

2.2.3 The Standard of Good Practice for Information Security

The Standard of Good Practice for Information Security is designed to help any organization, irrespective of market sector, size or structure, keep the business risks associated with its information systems within acceptable limits. It is a major tool in improving the quality and efficiency of security controls applied by an organization.

The Standard is based on over 16 years and US $75 million of investment in practical research and draws on the knowledge and experiences of the Information Security Forum's global members as well as building on other standards such as ISO 17799 and COBIT.

The Standard has been produced by the Information Security Forum (ISF), an international association of over 270 of the world's leading organizations which fund and co-operate in the development of a practical research programme in information security and best practices in IT security and information risk management. The ISF is referring their work to be probably represents one of the most comprehensive and integrated set of reports anywhere in the world regarding the process of managing information risk. (http://www.securityforum.org).

The Standard addresses information security from a business perspective. It provides a practical, business-focused and proven statement of good practice for information security, presenting organizations with a challenging, but achievable target against which they can measure their performance. The standard is provided by reports by the organization. The standard is not documented with research or any measures, so it is not to be known what the credible of the standard is.

Sarbanes-Oxley Act (SOX)

Sarbanes-Oxley is a US law passed in 2002 to strengthen corporate governance and restore investor confidence. SOX were sponsored by US Senator Paul Sarbanes and US Representative Michael Oxley. Sarbanes-Oxley law passed in response to a number of major corporate and accounting scandals involving prominent companies in the United States. These scandals resulted in a loss of public trust in accounting and reporting practices.

When the Sarbanes-Oxley Act was originally passed in 2002, many companies were less than enthusiastic about it. Concerns about the additional accountability and the internal changes that would need to take place weighed heavily on the minds of many company executives. These concerns turned out to be well founded. Some companies struggled to make the deadlines, and others missed them completely. Reasons included the high cost and enormous effort involved. In some cases, department directives were even changed to focus on meeting compliance.

An information security survey released by Ernst & Young in November (2006) found that over the 12 months prior, the main driving force for information security, in 61 percent of firms surveyed was compliance rather than worms and viruses.

SOX compliance has made corporate ethics training more common within the corporate environment. According to a 2005 survey by the Ethics Resource Centre, 69 percent of employees reported that ethics training in their organizations was up, as compared to 14 percent who said so in the same survey conducted in 2003. (http://www.ecommercetimes.com)

The U.S. Sarbanes Oxley Act of 2002 required many companies to adopt control frameworks. The most widely uses frameworks is COSO and Cobit. COSO Internal Control Integrated Framework states that internal control is a process, established by the board of directors, management, and other personnel. This was designed to provide reasonable assurance regarding the achievement of stated objectives and was a result of the Enron scandal. Many companies has used the COSO framework, but the Cobit standard is now more used also to provide competitive advantage (Ernst&Young, ISF conference in Tønsberg, 2006)

2.2.4 Cobit 4.0

The main theme of Cobit is business orientation. Cobit approaches IT control by looking at information, not just financial information, which are needed to support business requirements and the associated IT resources and processes. Cobit is extended to cover quality and security requirements in seven overlapping categories, which include effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

The latest version 4.0 of the standard has been widely accepted, since the framework now have cross references of inputs and outputs to/from the different processes. The framework also provide activities for all processes which shows what the CFO, CEO, IT Service Manager, Development Manager, etc should do or be involved in.

A 2005 IT Governance Institute (ITGI) global survey indicates an alarming number of organizations who do not have any form of IT governance framework within their organization. More than half of the 623 respondents to the survey had no formal framework. Gartner Group, as an in depended advisor, recommends use of this framework. It found COBIT 4.0 a significant improvement on the third release, "making it more relevant, filling some gaps and adding clarity. Most importantly, it better aligns with good and best practices. In the management of IT and so increases the possibility that its use will result in a better-managed IT environment and, specifically, improve risk management," Gartner said

Before I will present the Cobit framework, I would like to introduce the Cobit cube. The cube gives a visual view of how it integrates business requirements, IT processes and IT resources. This cube also describes that information security in hence of confidentiality, integrity and availability is business requirements and not an IT department task.

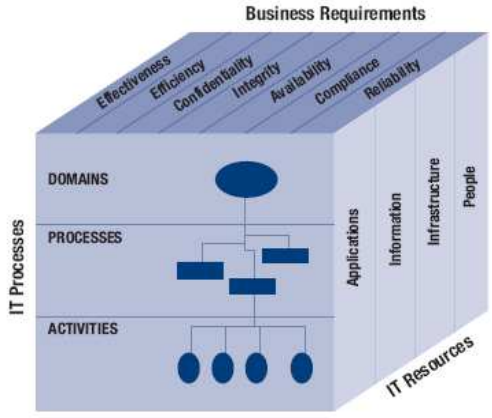


Figure 8 - Cobit Cube

2.2.5 The main topic of the Standard

Control Objectives
The key to maintaining profitability in a technologically changing environment is how well you maintain control. Cobit control objectives provide the critical insight needed to decline a clear policy and IT controls. There are included statements of desired results or purposes to be achieved by implementing the 215 specific, detailed control objectives throughout the 34 IT processes.

Audit Guidelines
Analyze, assess, interpret, react, implement. To achieve your desired goals and objectives you must constantly and consistently audit your procedures. Audit Guidelines outlines and suggests actual activities to be performed corresponding to each of the 34 high-level IT control objectives, while substantiating the risk of control objectives not being met. Audit Guidelines is an invaluable tool for information systems auditors in providing management assurance and/or advice for improvement.

Implementation Tool Set
An Implementation Tool Set, which contains Management Awareness and IT Control Diagnostics, and Implementation Guide, FAQ, case studies from organizations currently using Cobit, and slide presentations that can be used to introduce Cobit into organizations.

Management Guidelines
To ensure a successful enterprise, you must effectively manage the effective partnership between business processes and information systems. The new Management Guidelines is composed of Maturity Models, to help determine the stages and expectation levels of control and compare them against industry norms: Critical Success Factors, to identify the most important actions for achieving control over the IT processes; Key Goal Indicators, to define target levels of performance; and Key Performance Indicators, to measure whether an IT control process is meeting its objective. These Management Guidelines will help answer the questions of immediate concern to all those who have a stake in enterprise success.

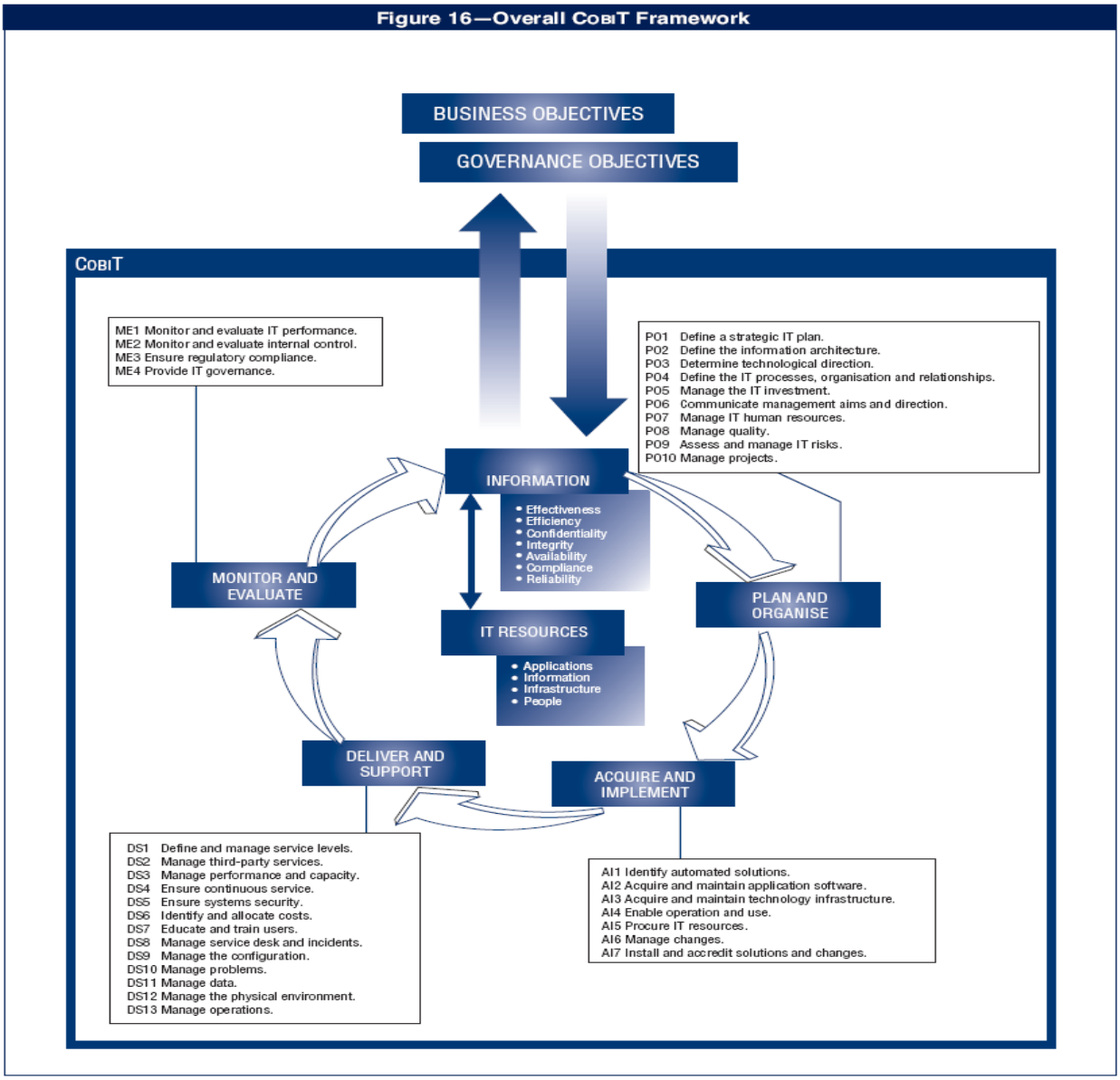


Figure 9 - Cobit framework

2.2.6 Cobit structure

The framework of Cobit has 34 IT processes, which are organized into 4 domains.

Plan and Organize

The Planning and Organization domain covers the use of technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.

Acquire and Implement

Identifying what is IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a

maintenance plan that a company should adopt in order to extend the life of an IT system and its components.

Delivery and Support

The Delivery and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as, the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training.

Monitor and Evaluate

The Monitoring and Evaluation domain deals with a company's strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors.

The IT Governance Institute has presented the following figure to illustrate what the Cobit framework is covering.

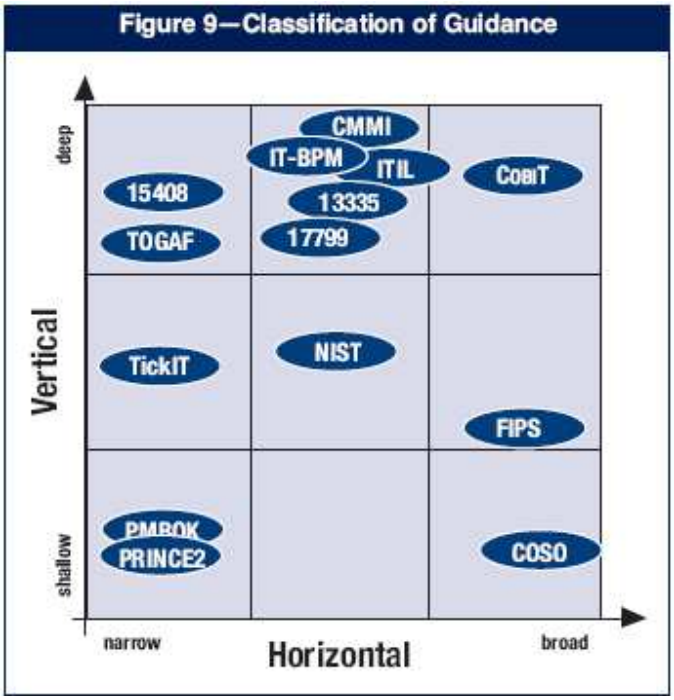


Figure 10 - Framework overview

3 Research methodology for the CASE study

In this chapter I will describe how the research has been done.

Research is often described as an active, diligent, and systematic process of inquiry aimed at discovering, interpreting and revising facts.

Methodology can be defined as: a body of methods, rules, and postulates employed by a discipline, a particular procedure or set of procedures, or the analysis of the principles or procedures of inquiry in a particular field (Merriam–Webster 1909). The common idea here is the collection, the comparative study, and the critique of the individual methods that are used in a given discipline or field of inquiry.

Research methodology is the attempt to validate the rationality behind the selected research design and provide justification of why it is appropriate in solving the selected research problem. It is the process of the research that produces knowledge.

The case study method is used of learning about a complex instance through extensive description and contextual analysis. The method has been described early as 1934, in a CASE history in medicine. The result of a case study articulates why the instance occurred as it did, and what one might usefully explore in similar situations.

Case studies can generate a great deal of data compared to a straightforward analysis. CASE studies for research purposes remain one of the most challenging of all social science endeavours (Yin, 2003). The goal for this CASE study is to get a closure by writing a compelling report.

3.1 Model for scientific empirical research methodology

The investigation process performed in this thesis is based on method for CASE study done in the master thesis made by Reierstad and Salvesen (2004), which is based on Janesick (2000) three stages divided into Jacobsen's (2000) different phases. The table below gives an overview of the methodology stages been used.

Stage (Janesick)	**Phase** (Jacobsen)	**Done in this research**
Research design	Phase 1 - Develop a research criteria	• Literature review process • Identified research issue
	Phase 2 - Choose a design	• Identified and developed a suitable research strategy • Single CASE study found suitable
	Phase 3 - Choose a method	• Identified suitable research method. • Developed research protocol. • Observation status agreed • Interview agenda and document research method identified suitable.
Data collection	Phase 4 - How to collect data	• Conduct multiple interviews with different stakeholders. • Observations thru participant • Collect and organize documents • Use of physical artefact
	Phase 5 - Select samples (units)	• Identified suitable company to conduct CASE study
Data analyze	Phase 6 - Analyze data	• Analyze and discuss information from the CASE study can be interpreted using existing theory.
	Phase 7 - Validity and reliability issues	• Triangulation • Discussed and clarifies boundaries of the research.
	Phase 8 - Interpret results and conclusion	• Empirical conclusions and interpretations.

3.2 Research design

Research design can be defined as the logical plan to interrelate research question to gathered data, and the interpreting and conclusions to be drawn (Yin, 2003). The research design is the first part of the empirical research methodology.

3.2.1 Phase 1 - Development of research topic

Development of research topic is a process of reviewing literature to identify research issues (Jacobsen, 2000). Literature reviews presented in the preceding chapters indicate that there are political, managerial, technical, social, and cultural issues related to information security. “Too many cooks in the kitchen” is a good description of the multitude of standards, methodologies and tools in the field of information security management. Many consultation offerings in the field only add to the confusion and make is more difficult to make decisions (Fumy and Sauerbrey, 2005).The topic here is to find an easy way of handling information security.

3.2.2 Phase 2 - Choose a design

Choosing a design refer to deciding the most appropriate way in which data should be collected and analyzed, with regards to the developed research topic (Jacobsen, 2000). To be able to gain valuable knowledge about the research questions it is necessary to take on a holistic approach.

Yin (1989) has defined a case study as:

An empirical enquiry that investigates a contemporary phenomenon within its real life context, when the boundaries between phenomenon and the context are not clearly evident, and in which multiple sources of evidence are used

The case study method seeks to facilitate an understanding of complex real life situations, by studying the situation in context.

Yin (1994) suggests that a case study is an intensive examination of a phenomenon in its natural setting, employing multiple methods of data to gather information from one or more entities (e.g. people, groups).

The case study allows an investigation to retain the holistic and meaningful characteristics of real-life events – such as individual life cycles, organizational and managerial processes, neighbourhood change, international relations, and the maturation of industries (Yin, 1994)

Yin (2003) also suggests that a case is a good strategy for investigating how something is conducted to achieve something. For this CASE study I have selected single case study because it is a unique case. The disorder in the case is so rare that that it is interesting to document and analyzing.

3.2.3 Phase 3 - Choose method

The method is the way in which we chose to conduct the case study. Research that examines complexities and processes in-depth, which cannot be carried out experimentally for practical or ethical reasons, suitable for qualitative methods.

3.2.4 Development and use of research protocol

A case study protocol is described by Yin (1994), as a tool for which to operational the research, acting as an action plan, and setting rules and regulations by which data would be gathered. The protocol acts as a data collection tool, where data are derived from case studies. Such protocol is considered necessary to increase the consistency and focus of the data gathering process. The timeline for the security project is long, as a result of organization changes, so it is important to gather information from the project and not the surroundings.

The case study protocol is used to keep track of activities, upcoming tasks, interviews, detail the objectives and procedures of the analysis in spirit of what Yin (2003) recommends. The fieldwork research procedures have been:

- Specify who needs to be interviewed
- Identify appropriate data gathering research methods and established the line of inquiry
- Develop a data collection agenda that takes into account contingencies in case of a respondent fail to keep the appointment
- Develop an interview timetable consisting of scheduled date and time
- A strategy to gain confidentiality among respondent and interviewer
- Develop a strategy for analyzing the collected data

3.3 Data collection

Data collection includes how information is collected and from whom, and is the second part of the empirical research methodology. First I have to identify ways and sources from which I collect data including interviews, documentation, archival records, physical artefacts and observation.

3.3.1 Phase 4 How to collect data

Multiple data collection methods are typically employed in case studies. Yin (1994) identifies several sources of evidence that can be used in case studies. These sources include interviews, documentation, archival records, physical artefacts and observation. The table below summarizes the strengths and the weaknesses of the main sources of evidence as identified by Yin (2003).

Source of evidence	Strengths	Weakness	In this research
			No of documents in ()
Direct Observations	• Reality – covers event in real time • Contextual – covers context of events	• Time-consuming • Selectivity – unless broad coverage • Reflexivity – event may proceed differently because it is being observed	• First faze of case study is done by learning what have be done, by document review and unstructured interview of the project leader and the IT director
Participant - observation	• Same as above for direct observations • Insightful into interpersonal behaviour and motives	• Same as above for direct observations • Bias due to investigator's manipulation of events	• Second faze of case study is done by participant in the security project and one structured interview about method. • I was hired as IT Security officer in the enterprise, and continued the work that has been done in the information security project
Documentation	• Stable – can be reviewed repeatedly • Unobtrusive – not created as a result of the case study • Exact – contains exact names, references, and detail of an event • Broad coverage – long span of time, many events and many settings	• Retrieve ability – can be low • Biased selectivity – if collection is incomplete • Reporting bias – effects (unknown) bias of author • Access – may be deliberately blocked	• Steering committee report(1) and documents(48) • Reports from external parties – risk report(1) and audit reports(3) • Organization charts(3) • Project reports(2) • Project plans(1) • Presentations from consultants (2)
Archival Records	• Same as above for documentation • Precise and quantitative	• Same as above for documentation • Accessibility due to privacy reasons	• Risk report(1) • Audit report(3) • Organization change report(2)
Interviews	• Targeted – focuses directly on the case study topic • Insightful – provides perceived causal inferences	• Bias due to poorly constructed questions • Response bias • Inaccuracies due to poor recall	• Unstructured interviews (many, more than 30) • Structured interview of project leader(1) • Reports from meetings in information security team(8) • E-mails(several, more than 20)

		• Reflexivity – respondent gives what interviewer	
Physical artefacts	• Insightful into cultural features • Insightful into technical operations	• Selectivity • Availability	• Software and solutions made in the project o Role DB o Employee DB • Motivation for the work done in the project – external project leader, management drives etc.

3.3.2 Phase 5 – Select samples (units)

3.4 Data analysis

Data analysis is the third part of the empirical research methodology. A difficulty in the use of qualitative data is that the methods of analysis are often not well formulated (Yin, 2003).

3.4.1 Phase 6 – Analyze data

Research strategies are important to secure a valid result of conclusions based on the analysis of the collected data. Yin (2003) describes three general analytic strategies:

- Relying on theoretical propositions – imply to follow the theoretical propositions that led to the case study.
- Thinking about rival explanations – imply to define and test rival explanations. The strategy can be related to the above, but is also relevant in the absence of theoretical propositions.
- Developing a case description – imply to develop a descriptive framework for organizing the case study.

The objective of the case is how to solve information security threats. The case is based on theoretical propositions and can be based on rival explanations. There is not one single grounded theory in the field of information security. There are many different approaches, by guidelines, models and frameworks. Developing a case description seems to be adequate for this case. A framework for issues to study will be developed.

3.4.2 Phase 7 - Validity and reliability issues

In logic, the form of an argument is valid precisely if it cannot lead from true premises to a false conclusion. An argument is said to be valid if, in every model in which all premises are true, the conclusion is true.

Construct validity, or credibility, refers to establishing match between the constructed realities of respondents and realities as represented by us, attributed to various stakeholders (Yin, 1994)

This is an important issue as much of the criticism against using case studies is dealing with effects and dependencies that really are not related to the phenomenon being studied. Methods to ensure the construct validity of the case include establishing and maintaining a chain of evidence, drafting a case study to discuss with key informants, and using triangulation (Yin, 1994).

In the social sciences, triangulation refers to the use of multiple cross-checked sources and methodology. The table below shows what type of triangulation and sources that have been used.

In the CASE enterprise I am employed as IT Security Manager, so I would be able to repeat the collected data, because I got insight in stored documents in the enterprise.

Type of triangulation used in the CASE study	Sources (nr of documents)
Data	Intranet sources Interviews • Project leader • IT director • Employee representative Observations • Security team meetings Participate • Security project • Researcher is IT Security Manager in the enterprise. Reports • Advisor reports (3) • Project report(1) • Organization change report(2) Plans • Security project plan Organization charts • Org. charts(3) Documents • Security policy • Security rules • Role descriptions

	Role database (Lotus Notes) Quality system
Investigator	Interpreting the data
Theory	Books and best practice standards • Security handbooks(many) • Security management book(1) • Guidelines • Frameworks(4) • ISO standards(5)
Methodological	Archive records Documents Interview Observation Participate

In statistics, reliability is the consistency of a set of measurements or measuring instrument. Reliability does not imply validity. That is, a reliable measure is measuring something consistently, but not necessarily what it is supposed to be measuring. For example, while there are many reliable tests, not all of them would validly predict job performance.

In the case study organizations charts and business process charts have been documented, since format is essential of the research. Enterprises will have different chart, but the concept can be reused.

3.4.3 Phase 8 - Interpret results and conclusion

It is important that the example for the case study is documented by its most relevant evidence. By doing this the reader can conclude, independent of the investigator. In this report the results and conclusion is presented in the end, after considering how other investigation could interpret.

4 A CASE study

For security reason the company name will be held confidential, so potential risks of the company will not be public.

In the literature research I have done some findings to investigate in the enterprise I have chosen. The literature framework has the topics to investigate. I have added one line to show what have been found in the CASE enterprise.

Author	Manage-ment	Organization	IT Risks	Object security	Incident handling	Business continuity management	Compliance	Training / Awareness	Behavior
Information Security Architecture and Information Security Governance	X	X	X	X	X	X	X	X	X
COSO (SOX)	X	X	X		X		X		
ISO 27001/17799	X	X	X	X	X	X	X		
ITIL	X	X		X		X	X		
Cobit (SOX) Management and organization	X	X	X		X	X	X	X	
Li. et al.(2003)	X	X							
Siponen (2003)	X	X							
Solms (2005)	X	X							
Tejay (2005)	X	X							
Pattinson (2003)	X	X							
Pearson and Ma (2005)	X	X							
Behavior									
Rhee and Ryu (2005)	X								X
Stanton et.al.(2004)	X								X
Kolkowska (2005)	X	X							X
Mathisen (2005)	X							X	X
Albrechtsen (2006)	X	X						X	X
Human Firewall / Withman et.al (2005)		X						X	X
IT Risks by Jahner and Krcmar (2005)	X	X	X						
CASE study	X	X	X	X	X	X	X	X	

4.1 Background for the CASE

The IT organization of the enterprise has been changed in the last 5 years. I have looked at these changes to investigate what they have changed to be in today's status. In specific, have been investigating the IT security environment.

The enterprise changed the audit firm in finance and accounting in 2002 and this firm is still the current audit firm. As a part of the first audit in 2002 they had a special focus of the IT security environment in the enterprise. The enterprise management was aware of that there were several problems in IT operations. Some of these problems were a result of loss of IT security handling in the enterprise. The enterprise management had an opportunity to a neutral investigation of the IT function. The audit company produced a report that had some remarks and concluded that there was a loss of IT security in the enterprise. Summarized the following issues were found:

- Missing issues in the security policy and lack of implementation of the policy.
- Loss and missing control of management in controlling user rights.
- Vulnerable in security configuration in operation systems and network.
- Divergence in national law requirements in the personal requirement law.

As a result, the IT function changed their organization and build up an IT security function. This IT security function has been investigated in the master thesis.

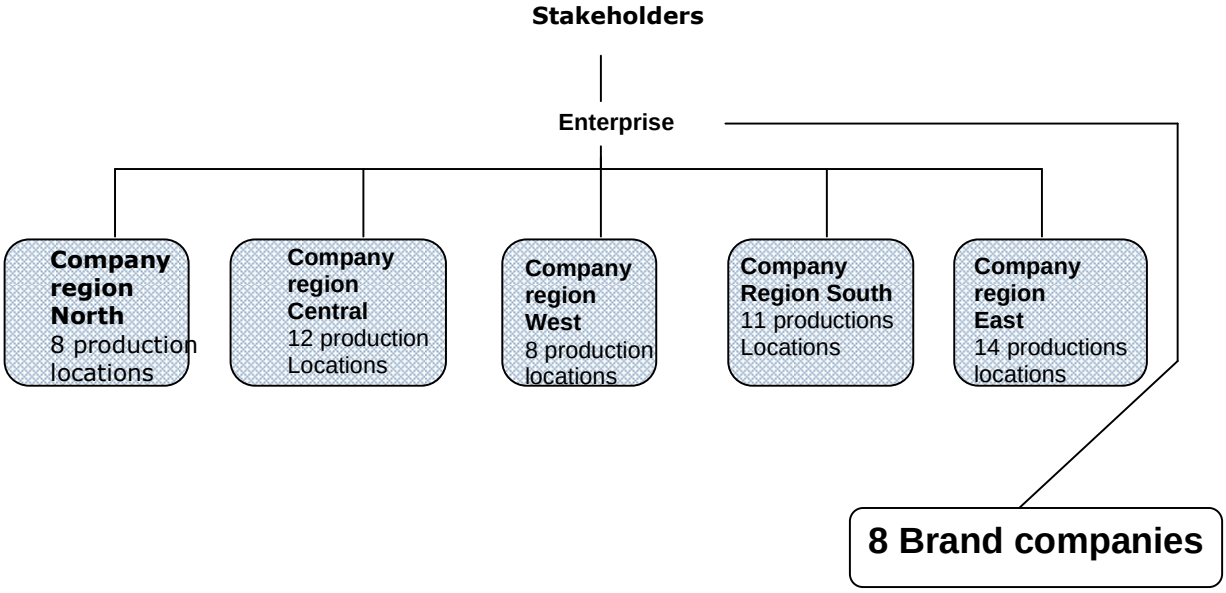
In the CASE study I have been studying the following elements of the IT function, according to the literature framework:

1. IT Management
2. IT Organization
3. Behaviour of IT security
4. Object IT security
5. Incident handling of IT security breaks
6. Business continuity management
7. Compliance of IT security towards laws and regulation
8. Training and Awareness of IT security handling

4.2 Presentation of the CASE Enterprise

The enterprise is one of the leading in the food industry in Norway. The enterprise has a sales and marketing organization and is responsible for product development, quality assurance, production and distribution planning, marketing and export of food products. The enterprise has 5500 employees. The vision of the enterprise is. "We shall be Norway's most important contributor to value creation."

The enterprise was merged into an enterprise in 2002. Earlier there where several companies in the same branch which had their own stockholders. These companies were not competitors, but where working together with a common owned company, who regulated the market. The market was regulated as a co-operative. Today the enterprise has the following enterprise structure, as the result of the merge in 2002.



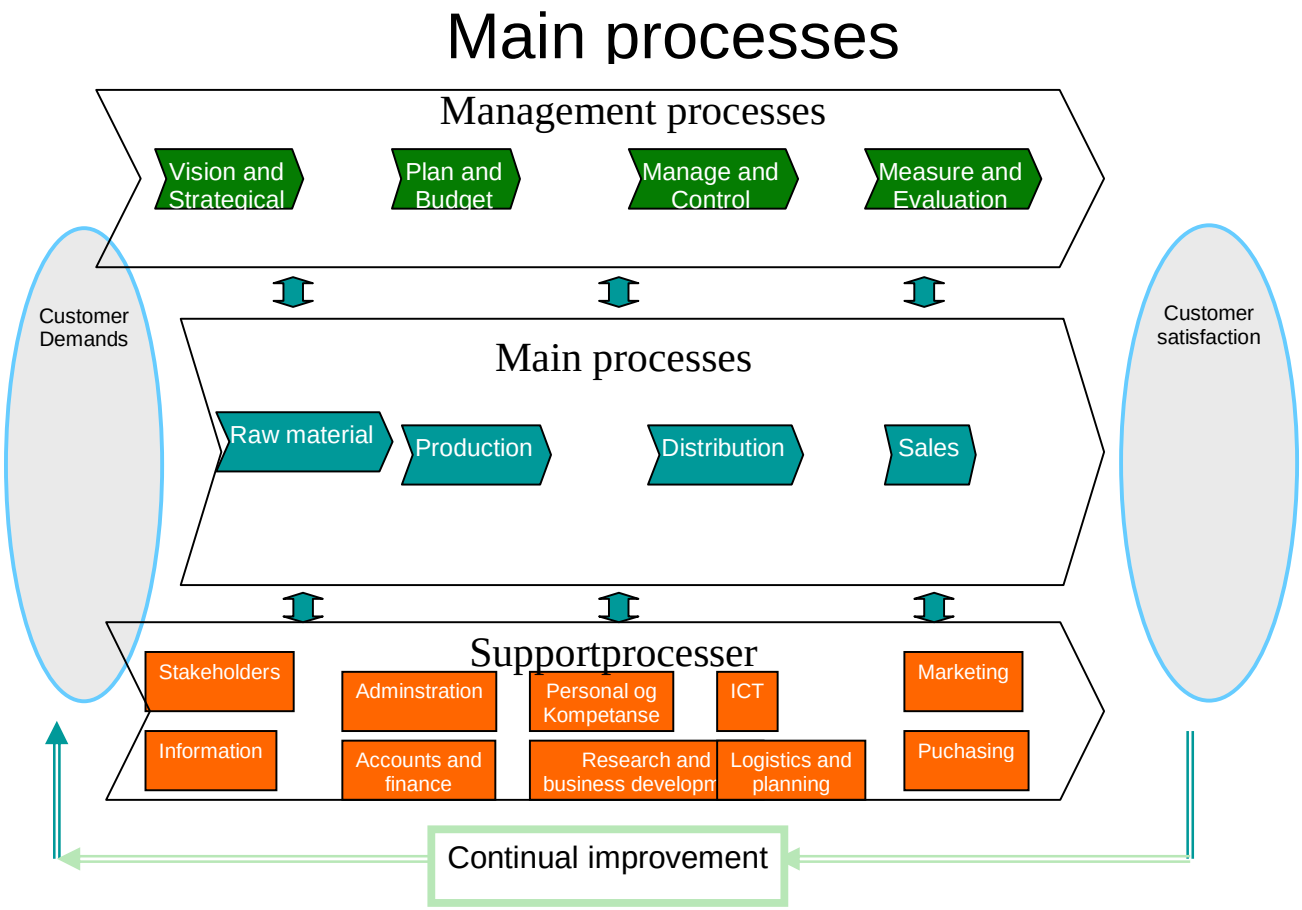
The enterprise has an administration, enterprise staff and 13 departments serving the whole enterprise including regional companies and some of the brand companies. One of these departments is the IT department.

The merge resulted in many organization changes in all levels of the organization.

The enterprise is certified according to the international IEC:ISO 9001:2000 standard. The enterprise believes that this standard is a tool to ensure that they are following laws and regulations within internal audit and quality measures (health, environment and safety).

4.2.1 Business processes in the Enterprise

The co-operate enterprise has a business process approach. This is according to that they are ISO 9001 certified. The business process is:



The process chart has one main process to archive the goal of customer satisfaction. To manage the main process the enterprise has a manage process. The enterprise also has a support process. The overall business process also has an iterative link to the start of the process to do continual improvements.

4.3 IT management

The current IT function consists of 55 employees. The IT function supports the enterprise and most of the daughter companies. They are supporting about 4000 users. The IT function provides both complete IT architecture as well as applications like ERP systems as an application provider. The IT function also widely outsources parts of the functions like WAN and hosting of servers. The operational budget for the year 2006 is NOK 167 mill. The IT department is using an ITIL "light" model. They call it "light" because of they are not using all the parts of the framework. They are not planning for an ITIL certificate, because this is costly and is not required by the customers of the IT department. The IT department is divided into roles with responsible tasks instead of job position in departments.

The CIO (IT Director) of the IT function is reporting to a Vice President in the enterprise management. In the enterprise management organization chart, the chart is showing that the Vice President that has responsible of several functions: IT, finance and personal.

For maintaining the system portfolio, planning and prioritizing of projects, there is a board containing the CIO, vice president of finance, IT and HR, Vice President of purchase, COO, Vice President one of the daughter companies, employee representative and a secretary from the IT department. Project leaders are reporting to this board and a project method is developed for running IT projects. During the budget process this board prioritize projects in three categorizes; 1. must be done, 2. will be considered and 3. can wait.

4.3.1 An information security project

To archive the current level of information security in the enterprise, there was set up a project to handle all tasks to be done. The project started in December 2003. The project leader of this project was an external consultant. This consultant has done a similar job for a Norwegian branch office of an audit company. During interviews of this consultant, I got information that the idea for the new organization of the IT department was developed in that company. This idea was based on the thinking in roles, but not only for security purposes.

The project was organised with the project leader as the only member. As a project leader he called in the chief for operations, system and help desk as needed. The owner of the project is the IT Director. The project leader reported to the steering committee of IT, which conduct of some of the enterprise management, representative of staff and administration of IT department.

4.3.1.1 Plan for the security project

IT-Security project – main plan revised

Make concept for IT security handling	Consultant
Present concept for IT-Steering committee	IT director
Develop risk map (information, operations, infrastructure, project, development, government etc.)	Deloitte&Touch
Handle risk report in the IT steering committee	IT steering committee
Handle risk report in enterprise management	Enterprise management
Make new information security policy	Consultant
Map IT-department functions and its working tasks and make these into roles	Consultant

Make Enterprise information security rules	Consultant
Make necessary routines and procedures for the working tasks	Consultant
Make adjustments to continual plan as a result of risk report	Consultant
Develop SLA for customers like regional companies and other branch companies	
Consuative in task with developing security and quality in the enterprise	Consultant
Educate all users in the enterprise	Consultant
Implement new organization structure, incl necessary training for the IT department	Consultant
Make final report	Consultant

Project plan presented as Gant diagram.

ID	Task Name	% arbe	Slutt	Foregå aktivite
1	*ICT-Security project - mainplan revised*	0%	Fre 12.12.03	
2	Make consept for ICT security handling	100%	Man 05.01.04	
3	Present consept for ICT-Steering commity	100%	Ons 07.01.04	2
4	Develope risk map (information, operations, infrastructure, project, devlopment, goverment etc.)	100%	Fre 30.01.04	3
5	Handle risk report in the ICT steering commity	100%	Fre 07.05.04	4
6	Handle risk report in enterprice management	100%	Tir 15.06.04	
7	**Make new infomation security policy**	**100%**	**Man 11.10.04**	
11	**Map ICT-department functions and its working tasks and make these into roles**	**60%**	**Tir 31.05.05**	**3**
26	**Make Company information security rules**	**6%**	**Fre 08.07.05**	
30	**Make nesesary rutines and procedures for the woring tasks**	**0%**	**Fre 30.09.05**	**29**
41	Make adjustments to continual plan as a result of risk report	0%	Fre 28.10.05	38
42	Develop SLA for cutomers like reginal companies and other branch companies	0%	Fre 16.12.05	41
43	Consuative in task with developing security and quality in the company	30%	Fre 23.12.05	
44	Educate all users in the company	0%	Fre 23.12.05	28
45	Implement new organisation structure, incl nessesary traning for the IT department	0%	Fre 23.06.06	24
46	Make final report	0%	Fre 30.06.06	45

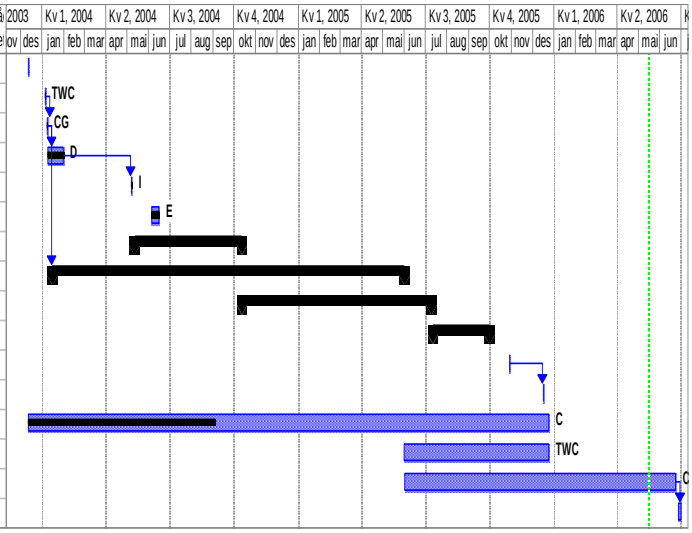


Figure 11 - Project Plan

The project plan describes how the project has been done. Due the merge of companies to an enterprise, there were started a separate project to make the organizations more effective. One result of this project was that a merge of regional IT departments into the enterprise IT department. This caused that the security project was delayed. This resulted in that the project is going to end 30.june 2006 instead of middle of 2005. The project leader and the IT director have stated that organization changes are very time consuming, and the IT department has the ongoing business that has to be operative. This is undertaken in literature about organization management.

4.3.1.2 How was the project done

The project started with looking into the organization structure and what the core business in IT is. For this process they started to look into the department what tasks is done. By previous experience from other projects in other companies they also make some new tasks to be done. In an interview by the IT director, he stated that they are going to build a new IT organization. The goal for this to is “do the same things with fewer people”. The people that are left are going to do the new tasks. The term “work smarter”, was widely used in that period.

All tasks done by the enterprise and regional IT departments where written down. By using the main structure of the business chart for the enterprise, they build a new business chart for the IT department. Building the new business process for the IT department was a working process, so they developed several charts. The final result is show in appendix C.

By this time each process where mapped up with how long time each task take in time. Time could be number of hour each day or each month.

After this was done, that had to place tasks into people at the department. To do this that had to make a map of all qualifications and interest of new working field in the department. This was done by a sub project, because 50 people where going to be interviewed. People that were interviewed was present the new structure of business processes in the IT department. Each one was asked what where interesting working area and what was the second area. The project manager for this sub project gathered together all data and where making this into a system. He arranged a meeting with the management of the IT department, for doing a process of placing people into tasks. They started with on process and picked on person which have the interest of doing the tasks in this process. They used one full day with 5 managers to do this work. The managers did not know who had the interest. The reason for doing the anonymous process was that no one should be excluded as a result of social factors. After this process was done, each employee in the IT department got an offer of new tasks in the new IT organization and the new. The entire employee accepted the offer.

After this process was done, the manager of the information security project used recommendations used in the IEC:ISO 17799:2002 to place security tasks in the IT organization. By this time he had to use the term role and tasks in working descriptions to get enough details. The ISO standard recommenders that, for example, destructive computer code should be handled by antivirus programs. The task of handling antivirus program is done by the person who got the role as antivirus responsible. This role was then supplied with was tasks to do and what information security demand the enterprise has. This implies that routines and procedures are necessary in addition to the framework. The project has not completed all routines. The completion of these routines and procedures is to be handled of newly build security organization. By this the database administrator, has the demands and knowledge to secure a database. If the role responsible does not have the skills, he/she will be educated.

There was a lot of information about people, roles, tasks and business processes. The project manager talked with system department in IT. Lotus Notes is a strategic tool used in the enterprise so they developed a Lotus Notes database with all this information.

4.4 IT Security management

IT security in the enterprise is managed at the top management of the enterprise. The managing director (CEO) has approved the information security policy, and is valid for all parts of the enterprise, e.g. all companies they have shares with 51% or more. The policy states that the IT director has the responsible of the day to day IT security management. The IT director has an IT security manager to do task of IT security.

The IT security manager has an IT security team. This team has several members, divided into role responsible. This is physical IT security, access control, malicious code, network and emergency planning.

4.4.1 Documents implemented in the enterprise

During interviews I have found four important documents that had been developed. They were developed during a information security project. These documents are Enterprise information security policy, Enterprise information security rules for employees, Enterprise information security rules for IT and enterprise information security rules for locations.

4.4.2 Enterprise information security policy

This document describes rules of information security in the enterprise. The document describes what level of information security the top management want in the enterprise. This document has been signed by the director of the enterprise. This has showed me that the information security is important for the enterprise. The main issues in the document is strategic goals for the enterprise, variables for what is the meaning of information security is, parameters for continuation of operation of information systems, organization of IT security handling, information classification and consequences of breaking the rules. The policy is based on information from the risk analyses that has been done by the audit company. The document states that all information in the enterprise should be marked with four different categories. These are: open to public, internal, confidential and strictly confidential. Another parameter in the policy is response time. Sales and distribution system show have maximum of 1 hour downtime, groupware systems 1 day and account system 1 week.

4.4.3 Enterprise information security rules for employees

As the information security policy does not have specific rules for the employees, it has been developed a document that has specific rules for user behaviour and act of information systems in the enterprise. The first part of the document describes what information security is and what the management demand is. The next part of the document describes how to handle documents, PC, PDA and other IT equipment, use of internet, use of e-mail. The last part is how to report information security breakages, dismisses of the enterprise and consequences of breaking these rules. This document had been developed together with the employees of the enterprise. Staff representative and enterprise management has agreed that this document together with a

presentation is to be presented into meetings the daily hierarchy organization of the enterprise. The leader of each department uses the presentation to present information security rules in the enterprise. In this matter the employees get education before they get the document. The document is to be signed by the employee.

During the case study the document was in progress of being signed by the employees. In a interview of the director of personnel, this process will take minimum 6 months. By the end of the case study it had taken 3 months, and about 20% of the employees have signed. The statement of that it will take about 6 moth is based on earlier experience within the enterprise. A similar process has been done about ethics rules.

4.4.4 Enterprise information security rules for IT

The project leader of the information security project had some knowledge about the ISO 17799:2002 standard. This standard about information security is a guideline for implementing information security. By this standard the project leader developed a framework document for the IT department of the enterprise. This framework is having rules and demands of services the IT department uses.

The document follows the numbering of the ISO standard. Key points in this document is security organization, 3.part access, training, physical security, network security, access control, systems development and continuity planning. The document has been updated to with the changes in the ISO 17799:2005 standard, but has missed the part with risk assessment and treatment, in the document. The risk assessment is handled in the IT department by the IT Security Manager, and is performed in change management process in the IT department.
Enterprise information security rules for locations
The enterprise has developed rules for locations. Most of the locations have a manager with is responsible for employees and buildings at the location. To provide rules for handling equipment holds information in the location, e.g. equipment is servers, routers and switches. The main rules in the document are access management, employee and consultant's checks.

4.5 IT Organization

The IT department is officially presented by the business process chart (Appendix C. To supply this they also have a hierarchical organization chart. The organization chart of the current IS department can be seen in appendix B. The organization has a central organization form, but employees are not placed in same office localization. There are employees placed in 12 localizations. Most of these employees are have office location in headquarter. They have a long term plan, to make 2 centers placed outside headquarters. There has been an organization change in the hierarchy chart in year 2002 as a result of a merge process by establishing of the enterprise. The organization chart at the year 2002 is presented in appendix A.

4.5.1 Processes

The work process of the IT function is organized as a sub support process of main corporate business process. The process for IT is corresponding with the corporate one; with a main process, manage process and a support process. It is possible to drill down into further levels in all processes.

4.5.2 Role based organization

The whole IT organization is build up of roles, with responsible tasks. There are about 200 roles divided into 55 employees. A system is developed to manage them and mapping between roles and employees. This system shows roles responsible for the processes in the IT department.

As shown in appendix C, there are several sub processes in the responsibilities of the IT department. Each sub process has a manager, and if the sub process has tasks that require more man power than one person, there are sub roles. An example is that there is one manager for the operation process. This manager has five sub processes to manage where one of these sub processes is managing PCs. Since there are 3000 PCs in the main enterprise to support there is one manager and three operators. They are using LANDESK systems management software for managing tasks, like patch management, inventory, software distribution and remote support.

4.6 Behaviour of IT security

In the literature research I discovered that the human factor is very important to manage information security. In this case study it was not possible to get any measurements about what effects information security management has made to the enterprise. The information security policy is placed into the quality system, which is electronically. The quality system is not used in daily basis in headquarter, and questions to some middle managers show that this policy is not known. The distribution of the document enterprise information rules for employees is in progress and will be measured during the process. Feedback from the employees in the enterprise is positive, so it seems to be useful. As an awareness campaign, key factors in information security have been published in the enterprise news magazine which is mailed to every employee. This was done in August 2006. The publishers are measuring that this magazine is read by the employees, but not on each article. Their survey has concluded that this magazine is read of most of the employees.

Information security rules is not published in the intranet of the reason that they want to do the presentation of the document before they publish the document, according to the agreement between employees and the enterprise management. The document is placed in the human recourses manual and manager manual. These manuals are published electronically in the end of this case study. There are plans to make awareness sessions in the intranet, so that information in the rules document is not forgotten after rollout. There is established a project on handling e-mail in the enterprise. Rules of handling e-mails are developed some years ago, but there have not been any campaigns to publish these rules.

A risk report on information security was done in 2004. This report discovered several risks to the enterprise. The latest audit performed by en external partner, shown that there is great progress in reducing these risks. To archive this result they have had an IT security project in the enterprise. I have described this project earlier in a separate chapter of this report.

4.7 Object IT security

I have not done a detailed research on object IT security, as this is not the main theme in this master thesis. I have focused on how information security is handled in the IT organization. The IT department has an ISO 17799:2005 approach, which requires that they have to meet the

requirements in the standard. To meet these requirements they have written routines. These routines are developed together with the specialist on the object (server, PC, firewall etc.) and the IT security team. They also use the concepts of ITIL framework. With this framework they have control of their business processes. There is a change management process, where all major system changes are handles. The IT security manager is part of this process. The security manager involved the security team, depended on which changes are planned to be done. There are specific roles for components like PC, servers, LAN and WAN. In each role there are specified object to secure and what tasks to perform. Patch testing and updating are a task for all operators. Theses operators are given education to be a specialist in their field. Some of them have product certification, Microsoft Certified Engineer. Developers are given specific training in writing secure code.

Many of the tasks are outsourced to a 3.part. By this way of doing, the 3.part is doing the actual tasks, but internal they have resources and competence to check that the 3.part do their tasks in a secure manner.

4.8 Incident handling of IT security breaks

The IT department has a no formal way of handling IT security breaks, in the meaning of written form to use. In the document security rules for user there are specified how to report breaks. The chapter below describes what is written in the document.

Everyone that works for Enterprise has the responsibility to report any activity, problems or suspicion of irregularities that can affect "data" or information security. These reports must be handed to the IT department Helpdesk or your closest executive. A security occurrence can be defined as:

- *"Data" that is read or copied of people with out authorization to the respective "data"*
- *Modifications that allow unauthorized people to access our systems, or disallow authorized people to do so.*
- *The lost of a enterprise-PC or other devises with saved information*
- *Virus atakk or suspicion.*
- *Receiving big amounts of unwanted Mail (advertise…).*
- *When receiving a Virus alert pop-up (you are not authorized to delete the alert with out contacting the IT Helpdesk.*
- *Burglary or theft of IKT-equipment or unauthorized access to Enterprise working premises.*
- *Observation of general violation or weakness of information security.*

4.9 Compliance of IT security towards laws and regulation

The enterprise is seated in Norway, and only has to deal with Norwegian regulation. Have are not registered at the stock marked, so they do not have same strict laws as other companies at the stock marked. SOX regulations is not acquired too be meet. However, they have to follow many of the same national laws as the other Norwegian companies. There is some regulation about national account according to audit.

The national law, “personopplysning loven” is about handling how to deal with personal information. This law has strong requirements for handling information that can identify a person. Customer and payroll systems are some of these systems that have to be also have to be taken care of. The law has different grading. If the strongest grading is too be meet, the enterprise has to apply. The enterprise has outsourced the payroll system, and the enterprise that owns this application has applied to the federal authority. Customer information is not so specific that they have to apply for this application. The law has also some requirement for information security handling, but it has no specific demands. These general terms about information security is handled by the IS0 17799 standard the enterprise uses.

4.10 Training and Awareness of IT security handling

There are several plans to develop security awareness sessions in the enterprise. There was article in the enterprise’s newspaper, which is sent home to all employees. This article was about information handling and general information security from the national news. Most of the plans was stopped because of that the management of the enterprise, made a decision that education in IT security is going to be at the same time as the distribution of the user IT security rules. There was made a presentation together with the document. The management and the employees representative has agreed that all employees are going to have a small training before the user information security rules are signed. A presentation in form of a PowerPoint document was made. This presentation was to help the leader of their department to do the presentation of IT security in the enterprise. After that this process of d is done, there are plans to put information security drops in the intranet.

5 Discussion of implications and contributing

Main theme of this research work has been investigating how to handle information security in organisations. Thru my literature research, I have found that the elements organising and humans are important factors in handling information security. The CASE study has shown a way of handling. In the literature research I have found the current different standards, guidelines, models and frameworks for handling information security.

The case study has showed me one way to handle information security in an organization. The CASE enterprise has established an information security project, to handle information security. The project had not been evaluated by measures, so it is not possible to make a clear conclusion of the ideas of handling information security is the more the right solution to this enterprise. The advisor report (2007) shows that there are fewer risks in the enterprise than advisors report in 2004. The advisor report made in 2002, show that there are numbers of risks are from the period of 2002 to 2004, because they discovered that there where risks at all. The number of information security breaks is not measured in the enterprise. The collected material from the CASE study has showed me that information security in organizations is about organization structure and responsible to all in the IT organization. The documents developed in the project shows what responsible the organization has and how these are divided into roles and tasks.

The advisor reports at the enterprise have shown that there has been a great progress and there are less information security risks in the enterprise. This is a good measurement for how the enterprise has handles information security. The method of handling the information security in this enterprise has not been documented and has been used in other companies. The key factor in the method was using roles to get a good organization for handling information security. By the roles, it was possible to get responsible for information security addresses to tasks instead of employees. The method has great parallel to the ISO 17799 standard and in combination with the ITIL framework, so it is not unique for this CASE. This is confirmed by that the IT department uses the terms “approach to ISO 17799” and “ITIL light”. They use these term in the way that they can full fill these standards. They have chosen to do that, because of that would not give them a better business results and it could be very timely and costly to get these certificates.

The case study together with the standard has shown one possible we of getting an organization that can handle information security from the top level management to practical IT employee. By research in literature I have found several surveys that show that investing in object security, like firewalls and antivirus is not enough (DTI, information security breaches survey 2006). Organization structure and information security responsible together with security awareness (Mathisen, 2004) seems to be a good solution to the problem.

There has been much development in theory and commercial standards in the field of information security in the last years. There has been focus on development of the ISO 27001 standard. The beginning of the British standard numbered 7799, has been developed further on to the ISO 17799 standard, and now to the ISO 27000. Other commercial standards like Cobit and ITIL also has had great development. The Cobit standard is widely accepted by financial advisors to archive requirements in the SOX Act (ISF Conference Tønsberg 2006). New release of the Cobit

4.1 and ITIL will be inn 2007.Gartner Group says about release 4.0: *"It found COBIT 4.0 a significant improvement on the third release, "making it more relevant, filling some gaps and adding clarity. Most importantly, it better aligns with good and best practices In the management of IT and so Increases the possibility that Its use will result In a better-managed IT environment and, specifically, improve risk management,*" They recommends enterprises use it to challenge their established IT governance procedures and to improve the controls they have in place. There has been some criticism about the earlier version of theses standards (Gartner Group, 2005), and minor changes is supposed to check out some of this criticism. I have not been able so get a preview of these new versions, so I can not confirm it. In literature research I have found some interesting research about these standards. In a discussion in a Norwegian ISF meeting this was confirmed by the panel participants Conclusions to these standards are that the human factor is much more important than object security.

There is some theory in the field of handling information security, and most of these researches have been done in the existing ISO standards and other best practises guidelines. The frameworks of Information Security Architecture and Information Security Governance have great parallels to Cobit and ISO standards. IT Risk management is now a part of the ISO 17799 standard and the Cobit framework, as result of comments and researches.

The CASE study has shown that this organization uses several standards and frameworks. The result is improvement in less information security risks. This was confirmed in the advisors reports. The CASE study validate that use of the IEC:ISO 17799:2002 is affordable for the enterprise in a business manner. This validating has given me values of metrics in this master thesis, by the advisors report.

My research has confirmed that handling information security is a management task and not only a technical IT department task. The CASE has shown that object security is not enough, there has to be and organization to handle these challenges. Research literature shows also the same results. Research literature has shown that there are several models and frameworks that will help organizations in handling information security and risks. Organization is not the only element in information security, behaviour and knowledge about risks is also needed. Education is needed to the whole organization and not just the IT department. Human errors are the greatest risk to information security. There are several surveys confirming this claim. In the CASE study organization there has been some training of the whole organization. The knowledge of information security risks in the organization has not been measured, so I can not confirm that the training has been valuable to the organization or not. There are several researches about training and security awareness. One research states that there is difference about awareness and education in information security. Awareness is getting attention to information security, and can be much more effective than formal training, thus is takes much time and can be very costly. Most organizations do not give information security education to all employees that handle information. Security awareness sessions are very effective in organizations. The CASE study organizations have done some sessions and have plans to more after the initial education is done. A survey in this organization would be very interesting, as a further research, to measure information security handling in that particular organization. There are plans to have metrics in the IT department on each role. These metrics are not focused at information security. Metrics for information security should also be an important metric to measure business goals of the organization.

In the CASE study it was done an information security risk analyse before they made the information security policy. This is quite different from the recommended way of doing according to the Cobit framework. The standards recommend using of risk analyses after the IT organization is established. This seems to some missing in the planning face. If the information security risks are not high for an organization there is no business efforts to make a strict systems and organization. The organization in information security manner has to be in according to the business goals. In the ISO standard this has had a change from ISO 17799:2002 to ISO17799:2005, to archive the process of handling IT risks.

There seems to be some not to agreement about using commercial standards. Financial advisors have education in using the Cobit standard to achieve claims in the SOX Act. This standard is also a part of the CISSP (certified Information Systems Security Professional) certification. ISO standards are widely used business and public organizations to achieve information security standards. Since both of these standards are based on best practices they are not recognized in education purposes because they have not and researches and the validity can not be confirmed. There is no formal research methods used to develop these standards. These standards have to be proven in several organizations to be confirmed, and could take long time to measure.

6 Findings

By the case study and with combining standards and literature it has been possible to make a model that is not too complicated to understand. Many of the existing standards are complicated to understand, and are enormous in number of pages. Many of them are made to cover the whole IT environment of large organizations, like the Cobit standard. Large organizations are able to implement several standards to get secure environments and governance. Simplification of the solution to problem is the key. Small companies and organizations are not able to have an own IT staff that can manage their information security matters. Consultants are expensive to use and many of these selects to live with the risk, rather than get a secure information handling environment. There are few stories in the news about large business impacts because of lack of information security, so that most of the management in small and medium sized organizations, do not know what risks they are taking.

6.1 A framework of information security handling

Thru the CASE study I discovered that the ideas of handling information security has been used was not documented as a methodology. The idea of the method has parallels to the ISO17799:2005 standard and the ITIL framework. It has also parallels to the framework of information security architecture (Killmeyer, 2006). Based on this information I am been able to make a new framework for information security. I use the term framework, because it is based on the concepts of standards and the CASE. The framework consists of parts from the ISO: 27001 and the Cobit framework. Instead of making another framework, I have tried to integrate the ISO standard into the Cobit framework. The Cobit framework is designed for IT Governance and not detailed for information security. The ISO 27001 framework is not integrated into the whole organization, just the IT organization. The uniqueness of my framework for information security is the combination of the tree dimensions business requirement, security requirement and needed IT resources.

I have not described a detailed method of how to use the framework. A simplified framework of the new ISO 27000 series will maybe be suitable for my framework in the next release, if it contains links to the business perspective? (2007).

In the literature framework, I have added what my information security framework is covering.

Author	Manage-ment	Organization	IT Risks	Object security	Incident handling	Business continuity management	Compliance	Training / Awareness	Behavior
Information Security Architecture and Information Security Governance	X	X	X	X	X	X	X	X	X
COSO (SOX)	X	X	X		X		X		
ISO 27001/17799	X	X	X	X	X	X	X		
ITIL	X	X		X		X	X		
Cobit (SOX) Management and organization	X	X	X		X	X	X	X	
Li. et al.(2003)	X	X							
Siponen (2003)	X	X							
Solms (2005)	X	X							
Tejay (2005)	X	X							
Pattinson (2003)	X	X							
Pearson and Ma (2005)	X	X							
Behavior									
Rhee and Ryu (2005)	X								X
Stanton et.al.(2004)	X								X
Kolkowska (2005)	X	X							X
Mathisen (2005)	X							X	X
Albrechtsen (2006)	X	X						X	X
Human Firewall / Withman et.al (2005)		X						X	X
IT Risks by Jahner and Krcmar (2005)	X	X	X						
CASE study	X	X	X	X	X	X	X	X	
Information security framework	X	X	X	X	X	X	X	X	X

The main elements of the framework are:

Business requirements – all organizations have a goal(s) and a vision (Sethi, 2002). To reach these goals the organization need support from the organization, by resources. This can be both technical and human resources. The business requires a set of IT services.

IT resources - The IT organization delivers against these goals by a clearly defined set of processes that use people skills and technology infrastructure to run automated business applications while leveraging business information

Information security requirements - preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability.

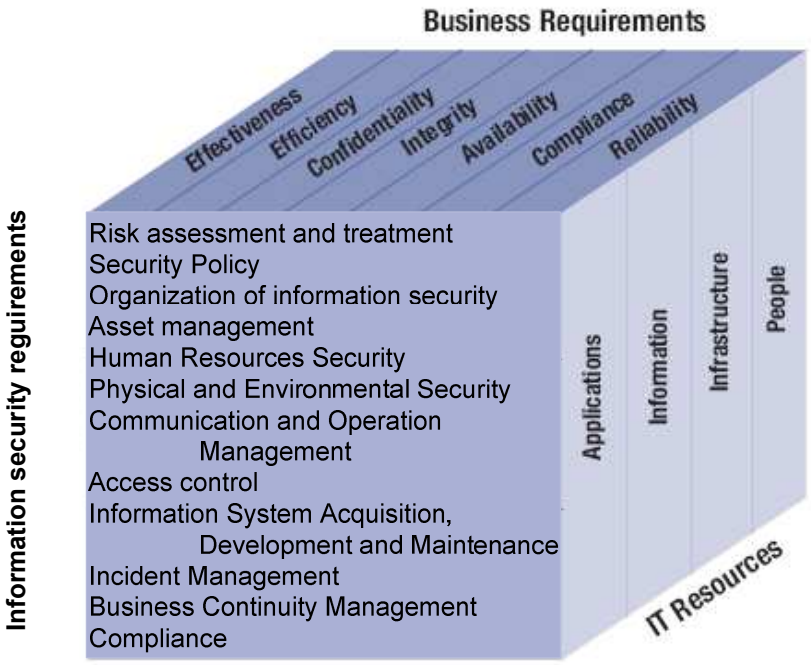


Figure 12 - Information security framework

6.1.1 Business requirements

- **Effectiveness -** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency -** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality -** concerns the protection of sensitive information from unauthorized disclosure.

- **Integrity -** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

- **Availability -** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.

- **Compliance -** deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria, as well as internal policies.

- **Reliability -** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

6.1.2 IT Resources

- **Applications** - are the automated user systems and manual procedures that process the information.
- **Information** - is the data in all their forms input, processed and output by the information systems, in whatever form is used by the business.
- **Infrastructure** - is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports them) that enable the processing of the applications.
- **People** - are the personnel required to plan, organize, acquire, implement, deliver, support, monitor and evaluate the information systems and services. They may be internal, outsourced or contracted as required.

6.1.3 Information security requirements

- **Risk assessment and treatment** - analysis of the organization's information security risks
- **Security policy** - management direction and level of security
- **Organization of information security** - governance of information security
- **Asset management** - inventory and classification of information assets
- **Human resources security** - security aspects for employees joining, moving and leaving an organization

- **Physical and environmental security** - protection of the computer facilities
- **Communications and operations management** - management of technical security controls in systems and networks
- **Access control** - restriction of access rights to networks, systems, applications, functions and data
- **Information systems acquisition, development and maintenance** - building security into applications
- **Information security incident management** - anticipating and responding appropriately to information security breaches
- **Business continuity management** - protecting, maintaining and recovering business-critical processes and systems
- **Compliance** - ensuring conformance with information security policies, standards, laws and regulations

To establish an environment for information security, I suggest using the PDCA model.

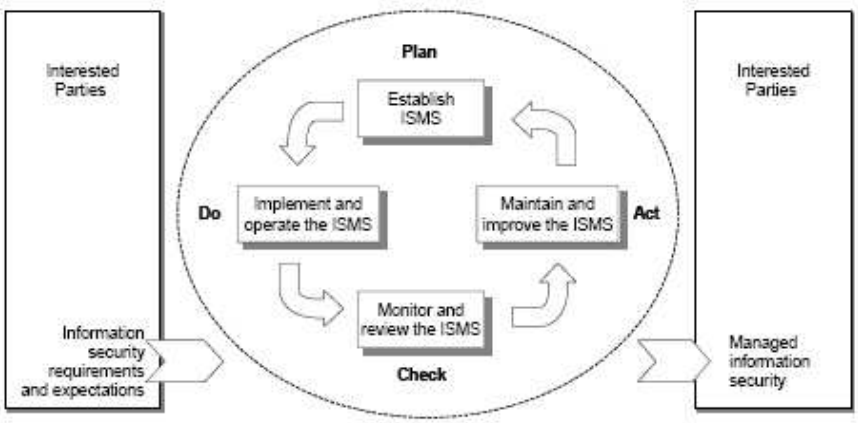


Figure 13 - ISO PDCA model

This PDCA is to be found in the ISO 27001 standard, and consist of:

Plan - Establish information security policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do - Implement and operate the information security policy, controls, processes and procedures.
Check - Assess and, where applicable, measure process performance against information security policy, objectives and practical experience and report the results to management for review.
Act - Take corrective and preventive actions, based on the results of the internal information security audit and management review or other relevant information, to achieve continual improvement of the information security.

6.2 Further research

By the material found in the case study, together with literature and best practise standards, it was possible to make a framework for handling information security. This model can be tested in other organizations and measured by surveys or action research.

In my research and the CASE study I have found that the organizing is one of the most important factors in having control of information security. In the last year there have been several attacks on personal users (Infosec Europe 2007). These users do not have ability to get all utilities to establish an environment for handling information security and risk handling. It is more common to use home PC to do electronically banking. Organized crimes have seen possible in getting control at home PC and do bank postings when the user is logged into their accounts. To do this they need highly skilled hackers (code breakers) to perform these tasks. Organized are not educating own computer personnel, but recruiting them thru their networks around the world and good paid services. Once they have got a person that has the necessary skills, they use pressure go get them ongoing for their organizations. The high skilled computer persons are then trapped into their network of crimes. These hackers are also a treat to organizations, because the organized networks give the hackers all needed resources to do their attacks because pay of could be very high. This raises the question about how to get the right ethics to young computer persons. This has to be treated as all other crimes around the world. There are different laws in each county, are less developed counties does not have laws to stop these crimes. A solution to this could be a strong participant from the UN (United Nations). This could be an interesting further research.

7 Reference

Achieving Network Security - An AT&T survey and white paper in cooperation with the Economist Intelligence Unit. 2003.

Albrechtsen, Eirik, A quantitative study of users' view on information security, Elsevier, Science Direct, 2006

Bosworth, Seymour & Kabay, M.E, Computer security Handbook, fourth edition 2002

Buchanan, D, Bobby, D and McCalman, J. " Getting in, Gettion on, Getting out and Getting back" in Alam Bryman(ed), Readings in Qualitative Research.

Cline, Melinda and Jensen, Bradley K., Americas Conference on Information Systems, 2004

Clue for Windows, Clue Inc, version 3.3, 1994

Cobit 4.0 – Management Guidelines – COBIT Steering Committee and the IT Governance Institute, 2005

Davison, R. M., Martinsons, M. G., and Kock, N. "Principles of Canonical Action Research," Information Systems Journal (14:1), 2004, pp. 65-86.

Department of Trade and Industry, information security breaches survey 2006, technical report

Ecommerce times, http://www.ecommercetimes.com

Elloff, Jan, Information security Architecture, Computer & Fraud November 2006

Fumy, Walter & Sauerbrey, Joerg, Siemens Aktiengesellschaft, 2006

Gartner Group, http://www.gartner.com, 2006

Global Watch Mission Report, Changing nature of information security, 2006

Grobler T, and Prof. Louwrens, B., http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/046_Article.pdf, 2005

Henry Mintzberg, Designing effective organizations, Prentice Hall, 1983

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28, No. 1, 75-105

Hoxey, Cynthia and Shoemaker, Dan, Americas Conference on Information Systems, 2005

IEC/ISO 17799:2005 – International Organization for Standardization and International Electrotechnical Commission, 2005

IEC/ISO 7799:2002 – International Organization for Standardization and International Electrotechnical Commission, 2002

IEC/ISO 27001:2005 – International Organization for Standardization and International Electrotechnical Commission, 2005

Infosec Europe 2006, London, Hackers panel, 2006

Infosec Europe 2007, DTI, 2007

ISF Conference, Tønsberg, http://www.isf.no, 2006

ITIL – IT infrastructure library, Best Practice for Security Management, Introduction to ITIL, 2005

Jacobsen, D.I., Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. Norwegian Academic Press, Kristiansand, Norway, 2000

Jahner, Stefanie and Krcmar, Helmut, Risk Culture as a success factor for IT risk management, Americas Conference on Information Systems, 2005

Janesick, V. The Choreography of Qualitative Research Design, in Handbook of Qualitative Research. (Ed, Lincoln, Y.S.). SAGE Publications, Thousand Oaks, California, USA, pp 379-399, 2000

Jordan, Ernie & Luke Silcock, PA Consulting Group, Beating IT Risks, 2005

Killmeyer, Jan, Information security Architecture, Second Edition, Auerbach Publications, 2006

Kufås, Ivar and Mølmann Roy Are, Informasjonssikkerhet og insiderproblematikk, ISBN 82-7706-204-4, 1993

Li et. al, BS7799: A Suitable Modell for Information Security Management, 2003

Mathisen, Johnny, Measuring Information Security Awareness – A survey showing the Norwegian way to do it, 2004

Myers, M.D. “Investigation information systems with ethnographic research”, Communications of the AIS 2, Article 23, 1999

Noah Webster, A Compendious Dictionary of the English Language, Merriam Company 1909

Pattinson, Malcom R., Americas Conference on Information Systems, 2003

Reierstad, Nina and Salvesen, Hilde, Implementing a Rationalized Data IT Architecture by enterprise application integration, A CASE study, Master thesis, 2004

Sarbarnes-Oxley, US Sarbarnes-Oxley Act, US Law regulations, http://www.pcaobus.org

Sethi,Vikram and King,Willam R., Introduction to business process reengineering, 2002

Shafer, Don, Dynamic Position Conference, 2004

Stamland, Frank-Arne, Is BS7799 worth the effort, 2004

Tejay, Gurvirender, Making Sense of Information Systems Security Standards, Americas conference on Information Systems, 2005

Venkatraman N., IT-Enabled Business Transformation: From Automation to Business Scope Redefinition, 1994

Webster, Jane and Watson Richard T., Analyzing the past to prepare for the future: Writing a literature review, MIS Quarterly Vol 26 No 2, 2002

Wold, Gullik, Key factors in making Information Security policies Effective, 2004

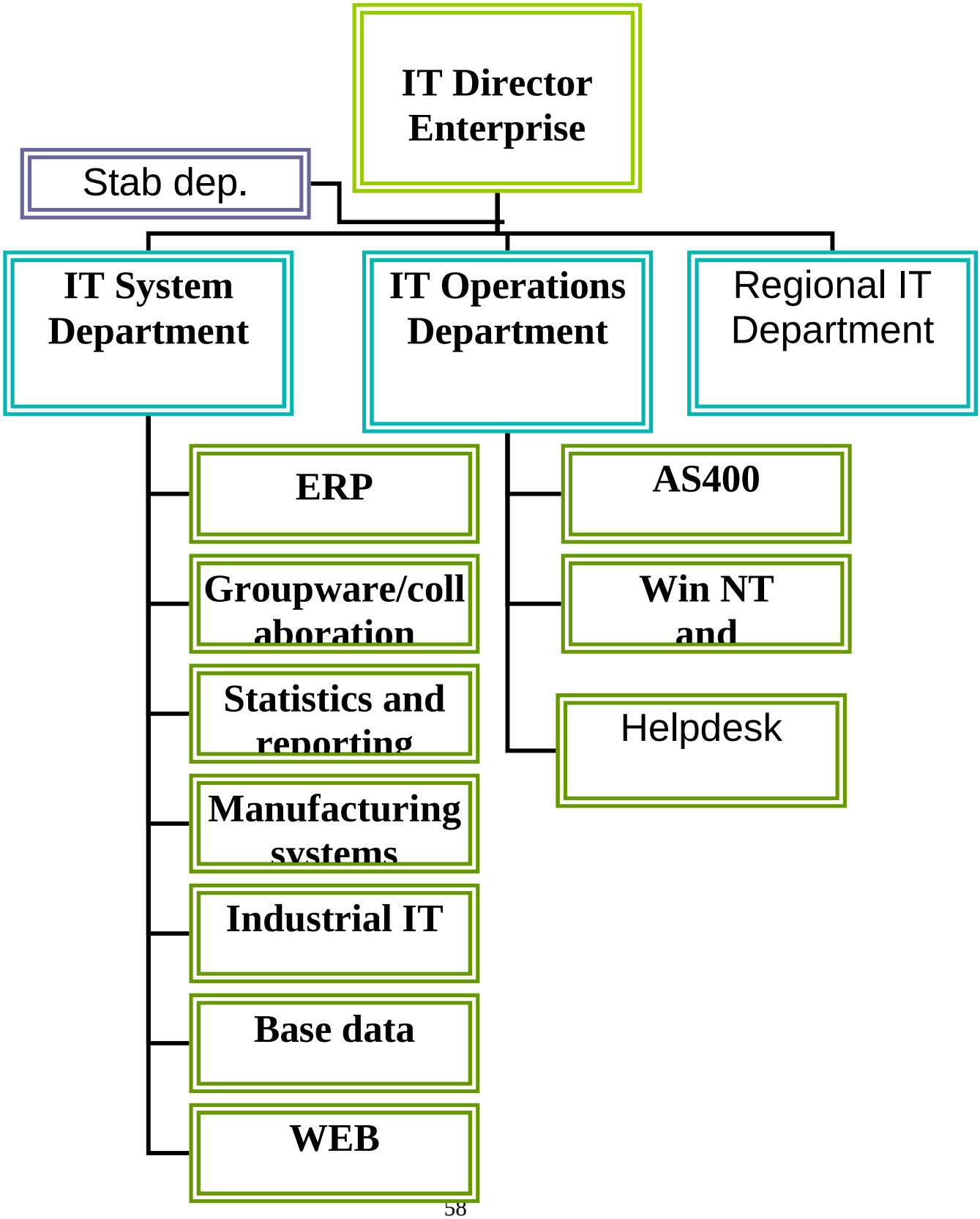
Yin, Robert K., Case Study Research, 1989

Yin, Robert K., Third Edition, Case Study Research, 2003

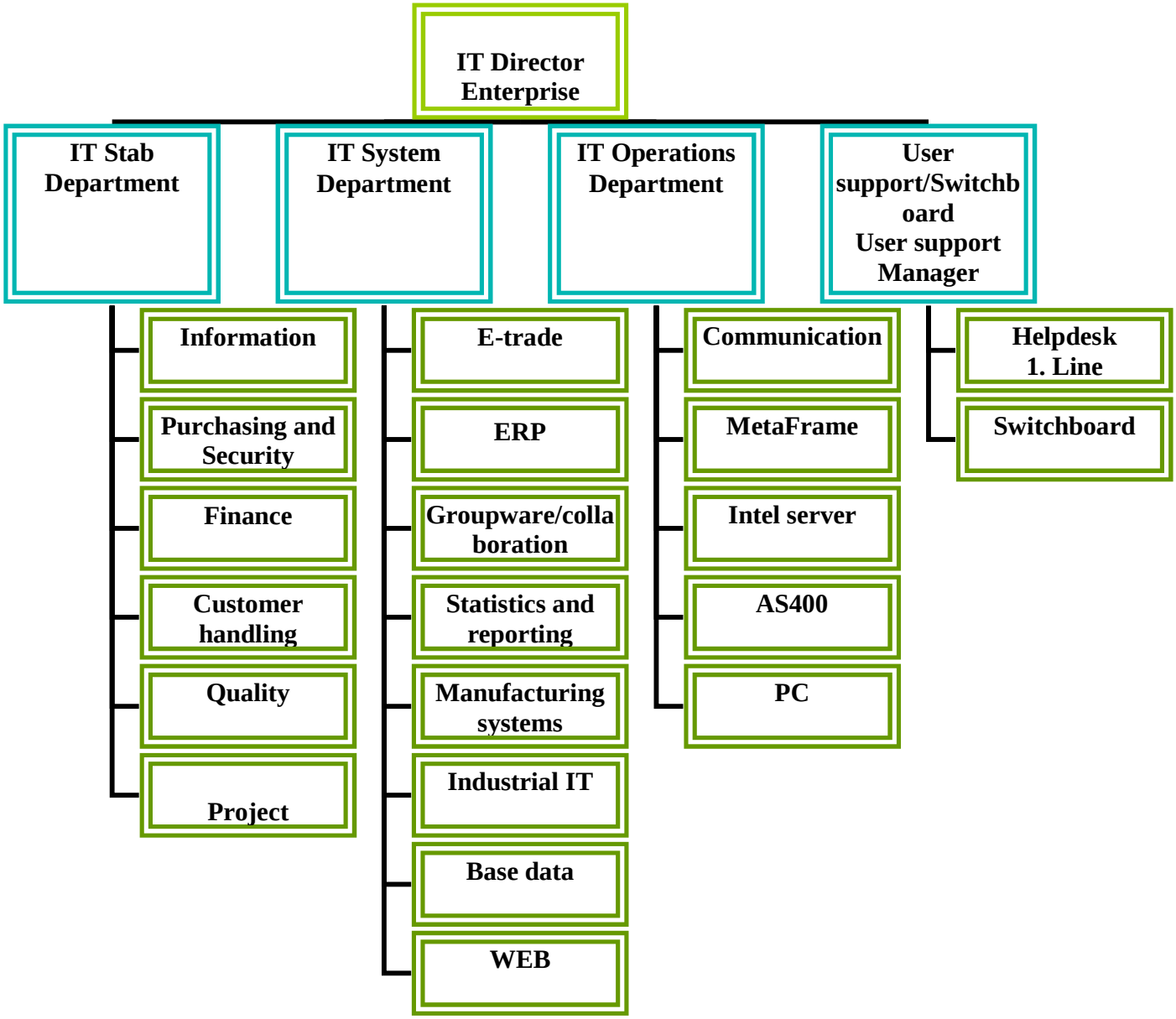
Merriam-Webster and Wikipedia.org (http://wikipedia.org)

Withman, Crayor, Fendler, Baker, White paper, Information Security Curriculum Development Conferences, 2005

8 Appendix A - Organization chart in 2002



9 Appendix B - Current IT organization in the enterprise company



10 Appendix C – IT business processes