“Good companies have well-honed processes for just about everything they do.”

Matheson and Matheson (1998), page 154

SUMMARY

Title
Information Security at ACT Systems – An Evaluation of ISO/IEC 27000

Department
Lund Institute of Technology – Industrial Management and Logistics

Period
September 2006 – January 2007

Author
Stefan Tinnert

Tutors
Juan de Dios Hermosín Ramos, CEO, ACT Systems
Carl-Johan Asplund, Lecturer, Lund Institute of Technology

Key words
ISO 27000, ISO 27001, ISO 17799, benchmarking, best practice, technology strategy, certification

Problem
ACT Systems wants to know if the processes and controls recommended by ISO/IEC 27000 can help them to improve their ICT security, and if these processes and controls are in line with best practice and with the company's technology strategy.

Purpose
The purpose of this master thesis is to evaluate if ACT Systems should become certified with ISO/IEC 27001:2005, presupposed that there is a demand from customers.

Method
The evaluation of ISO/IEC 27000 is based on three pillars. The first pillar is a comparison with best practice on an organizational level, represented by the theory of the Smart Organization presented by Matheson and Matheson (1998). The second pillar is a comparison with best practice on an ICT

security specific level. This best practice is represented by the results from a benchmarking study of principally the Swedish market. The third pillar is a comparison with ACT Systems' technology strategy, with the purpose to evaluate if this is supported by ISO/IEC 27000.

Conclusion

ISO/IEC 27000 represents best practice both on an organizational and ICT security specific level. It also supports ACT Systems' technology strategy. This means that ACT Systems' internal processes are supported. On the other hand, ISO/IEC 27000 is sparsely mentioned in the debate and is unlikely to give any sustainable competitive advantage.

PREFACE

The realization of this master thesis has been like a bridge that has enabled me to depart from my student life and arrive in my professional life. Along this bridge, I have assembled and utilized different parts of my university studies and I feel that this has been an excellent preparation for my future professional life.

For this challenging and instructive journey, I would like to thank Carl-Johan Asplund at The Lund Institute of Technology and Juan de Dios Hermosín Ramos at ACT Systems. I would also like to thank everyone working for ACT Systems in Seville for all the laughs I have had along the way.

I hope that this master thesis provides interesting reading, and that the conclusions will be useful for ACT Systems and for all organizations interested in ICT security.

Lund, 26th of January 2007

Stefan Tinnert

ABSTRACT

Information and communications technology (ICT) is at the forefront of the current wave of technological development. This development of ICT has resulted in new information security related threats. It has therefore become a crucial need for organizations to protect their information and to manage their ICT security. To address this need for ICT security, a family of international standards called ISO/IEC 27000 is under development. The standards published to this date are ISO/IEC 27001:2005, a process approach for information security management, and ISO/IEC 17799:2005, a collection of practices for information security management. ISO/IEC 27001:2005 is the standard used for certifications.

The thesis is conducted for the Spanish company ACT Systems, which has core competencies in information management and ICT solutions. ACT Systems has received some indications that there is a growing demand amongst customers for improved ICT security, and the company believes that they may gain competitive advantage by having their ICT security certified. ISO/IEC 27000 is a relatively new standard addressing the issue of ICT security, and ACT Systems considers it as an interesting alternative. They want to know if the processes and controls recommended by the standard can help them to improve their ICT security. If they do, a certification will be considered. If not, other measures have to be considered to improve the company's ICT security. For an implementation to generate benefits, it is also fundamental that the standard is in line with ACT Systems' technology strategy.

The purpose of this master thesis is to evaluate if ACT Systems is eligible to become certified with ISO/IEC 27001:2005, presupposed that there is a customer demand.

The thesis focuses on three principle investigations. The first pillar is a comparison with best practice on an organizational level, represented by the theory of the Smart Organization presented by Matheson and Matheson (1998). Best practice on an organizational level is the processes that should be in use in the organization. The second pillar is a comparison with best practice on an ICT security specific level. The best practice is represented by the results from a benchmarking study made principally on the Swedish market. The third pillar is a comparison with ACT Systems' technology strategy, with the purpose to evaluate if this is supported by ISO/IEC 27000. The analysis of the technology strategy is based on theories presented by Dodgson (2000). The thesis also contains comprehensive summaries of the standards ISO/IEC 27001:2005 and ISO/IEC 17799:2005, as well as a shorter presentation of ACT Systems.

The conclusions are that ISO/IEC 27000 represents best practice both at an organizational and ICT security specific level. It also supports ACT Systems' technology strategy. This means that ACT Systems' internal processes will be supported in the best possible way. On the other hand, ISO/IEC 27000 is sparsely mentioned in the current debate and is unlikely to give any sustainable competitive advantage.

The most important recommendation for further studies is to conduct a customer analysis. This is the most important recommendation because everything ACT Systems does, it does for its customers. The main purpose with this study would be to determine the probability of ISO/IEC 27000 becoming a threshold capability.

RESUMEN

La tecnología de la información y las comunicaciones (TIC) es la base en la ola actualmente reinante de desarrollo tecnológico. Aparte de nuevas oportunidades, el desarrollo de las TICs ha originado nuevas amenazas relacionadas con la seguridad de la información. Por eso, es una necesidad empresarial decisiva proteger la información y gestionar la seguridad de las TICs. En contestación a esta necesidad de la seguridad de las TICs, un conjunto de normas internacionales llamada ISO/IEC 27000 esta desarollandose. Las normas publicadas hasta la fecha en esta materia son ISO/IEC 27001:2005, que es un enfoque de proceso para la gestión de la seguridad de la información, y la ISO/IEC 17799:2005, que es una colección de prácticas para la gestión de la seguridad de la información. La ISO/IEC 27001:2005 es la norma utilizada para certificarse.

Este proyecto fin de carrera esta realizado por la empresa española ACT Sistemas, que tiene sus principales competencias en la gestión de la información y en soluciones de las TICs. ACT Sistemas tiene conocimiento de que existe una petición en favor de una mejor seguridad por las TICs creciendo entre los clientes, y la empresa cree que puede ganar ventajas competitivas si tiene una seguridad certificada de las TICs. La ISO/IEC 27000 es una norma relativamente nueva que trata este tema, y ACT Sistemas la considera un alternativo interesante. La empresa quiere saber si los procesos y las medidas recomendadas en la norma pueden ayudar a mejorar su seguridad de las TICs, y si estos procesos y medidas son alineadas con la mejor práctica. Si lo estan, una certificación será considerada. Si no, otras medidas tienen que ser consideradas para mejorar la seguridad de las TICs de la empresa. Para una implementación de generar beneficios, es también fundamental que la norma esté alineada con la estrategia de la tecnología de ACT Sistemas.

El propósito de este proyecto fin de carrera es de evaluar si ACT Sistemas sería certificado según la ISO/IEC 27001:2005, presuponiendo que hay una petición de los clientes.

Para esta evaluación, el proyecto fin de carrera es fundado sobre tres pilares. El primer pilar es una comparación con la mejor práctica al nivel organizativo, representado por la teoría del Smart Organization presentada de Matheson y Matheson (1998). El segundo pilar es una comparación con la mejor práctica al nivel específico de la seguridad de las TICs. Esta mejor práctica es representada

por los resultados del benchmark hecho principalmente en el mercado sueco. El tercer pilar es una comparación con la estrategia de la tecnología de ACT Sistemas, con el propósito de evaluar si ésta es apoyada por la ISO/IEC 27000. El análisis de la estrategia de la tecnología está basado en teorías presentadas de Dodgson (2000). Esta presentación del proyecto fin de carrera contiene también resúmenes detallados de las normas ISO/IEC 27001:2005 e ISO/IEC 17799:2005, así como una presentación corta de ACT Sistemas.

Las conclusiones son que la ISO/IEC 27000 representa la mejor práctica, tanto al nivel organizativo como al nivel específico de la seguridad de las TICs. La estrategia de la tecnología de ACT Sistemas está apoyada también. Este significa que los procesos internos de ACT Sistemas serán apoyados en la mejor forma. Por el otro lado, la ISO/IEC 27000 es escasamente mencionada en el debate actual y es poco probable que ACT Sistemas pueda obtener ventajas competitivas sostenibles.

La recomendación más importante para estudios futuros es realizar un análisis de los clientes. Esta es la recomendación más importante porque todo lo que ACT Sistemas hace, lo hace para los clientes. El propósito principal con este estudio será determinar la probabilidad de que la certificación a ACT Sistemas en la ISO/IEC 27000 sea la meta a alcanzar.

TABLE OF CONTENTS

1 INTRODUCTION TO THE MASTER THESIS

1.1 Introduction

The chapter starts with a description of the background of this master thesis, which leads up to the problem formulation and to the definition of the overarching purpose. After that, delimitations and target groups are presented. The chapter ends with a presentation of ACT Systems, the company for whom the master thesis has been conducted, and a thesis outline.

1.2 Background

In Nationalencyklopedin (www.ne.se), a Swedish encyclopaedia, it can be read that IT, Information Technology, is a generic term for the technical possibilities that have been created through advances in computer science and telecommunications. The notation ICT, Information and Communications Technology, is used when it is desired to emphasize the role of telecommunication. Dodgson (2000) asserts that ICT is at the forefront of the current wave of technological development. Juan de Dios Hermosín Ramos, CEO at ACT Systems, says that enterprises that do not invest in appropriate ICT solutions will perish because ICT today, and even more in the future, is a threshold capability or even a core competence in many sectors.

Besides new opportunities, the development of ICT has also resulted in new security related threats because applications such as electronic databases, wireless communications etc also mean new risks, both for the own company and for its partners. Nationalencyklopedin defines IT security as a generic term for everything dealing with security in IT systems, including communication as well as storage and processing of data. As communications activities are included in this definition of IT security, it equals what in this master thesis is referred to as ICT security. ICT security is a less established, but more correct, term. Besides, the encyclopaedia defines information security as the term focusing on the information itself. Thus, ICT security should be regarded as the area within information security that specifically deals with information that is communicated, stored, or processed in an ICT system. Walter Fumy, vice president of Security and Technology at the division of Communications at

Siemens, writes in UNE (2006) that there is a crucial need for organizations to protect their information and to manage their ICT security. He writes further that the legislation in many countries demands the enterprises to take adequate measures to diminish the risks related to commercial activities and the use of ICT. According to the International Electrotechnical Commission (www.iec.ch), information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

The objectives with ICT security are, according to Nationalencyklopedin, to secure access to information for authorized persons, to prevent access to information for unauthorized persons, and to prevent that incorrect information is accepted by the system. The risks can never be completely eliminated, but the objective must be to reduce them to an appropriate level. What this means is individual for each company and each process, and has to be decided by a risk assessment and an acceptance policy. The challenges of ICT security can be of different nature and with different origins, and some examples are listed here to give the reader a first insight:

Software	*Environmental*
Illegal encroachment	Power failure
Virus	Damage caused by carelessness
Spam	Sabotage
Spy ware	Fire
Trojan horses	Weather

To deal with information security, a new family of international standards called ISO/IEC 27000 is under development by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The ISO/IEC 27000 family will, according to a press release from the Swedish Standards Institute (2006), consist of the following standards:

- ISO/IEC 27001 Information Security Management System – Requirements
- ISO/IEC 27002 Code of Practice for Information Security Management
- ISO/IEC 27003 Information Security Management System Implementation Guidance
- ISO/IEC 27004 Information Security Management Measurement
- ISO/IEC 27005 Information Security Risk Management

The only standard published to this date is ISO/IEC 27001:2005. ISO/IEC 27002 exists under the name ISO/IEC 17799:2005. ISO/IEC 27001:2005 is the standard used for certifications, while the practices presented in ISO/IEC 17799:2005 are eligible and used to support the processes in ISO/IEC 27001:2005.

The master thesis is conducted for the Spanish company ACT Systems, with head office in Seville. ACT Systems is developing IT solutions with integrated communication applications, and has its core competences in information management and ICT solutions. In order to cover all the activities of ACT Systems and its clients, a broad definition of ICT has been considered. This includes both software, hardware, and infrastructure like networks and servers, but also security devices and data centres. ACT Systems hopes that an improved ICT security will give them competitive advantage, both by means of communication with external parties, and by internal benefits. They also see the possibility to integrate ICT security in products and services delivered to customers in a way that increases customer value.

1.3 Problem Formulation and Purpose

1.3.1 Problem Formulation

ACT Systems has received some indications that there is a growing demand amongst customers for improved ICT security, and the company believes that they may gain competitive advantage by having their ICT security certified. ISO/IEC 27000 is a relatively new standard treating the issue of ICT security, and ACT Systems considers it as an interesting alternative. They want to know if the processes and controls recommended by the standard can help them to improve their ICT security, and if these processes and controls are in line with best practice. If they are, a certification will be considered. If not, other measures have to be considered to improve the company's ICT security. For an implementation to generate benefits, it is also fundamental that the standard is in line with ACT Systems' technology strategy.

1.3.2 Purpose of the Study

The purpose of this master thesis is to evaluate if ACT Systems is eligible to become certified with ISO/IEC 27001:2005, presupposed that there is a customer demand.

1.4 Delimitations

The study focuses on ACT Systems, and it has a European perspective. The evaluation of ISO/IEC 27000 is confined to a comparison with best practice and with ACT Systems' technology strategy.

1.5 Target Groups

This master thesis is aimed to provide support and guidance for ACT Systems and for all other organizations that are interested in improving its information and ICT security. It is also aimed for last year engineering students, especially in management and computer science, who are interested in information and ICT security on an organizational and strategic level.

1.6 ACT Systems

This thesis work has been realized together with ACT Systems (www.actsistemas.es), a company that designs and develops information and communication systems principally applied in engineering solutions. The business of ACT Systems consists of three principal areas, all three with information management as the focal point:

- *Systems Engineering:* Control systems for different installations, including for example remote control and surveillance. These control systems are also applied in integrated control systems for buildings, like climate systems, fire control systems, access control systems etc. Other businesses within this area are Geographical Information Systems (GIS) and Fleet Control, the latter using GPS and GIS for vehicle localization and fleet management.
- *Management Systems:* Development of customized applications and customization of standard software within the following areas:
    - Support Systems and Resource Management: Development of control tools for the ISO 9000 standard. Also development of applications for PDAs (Personal Digital Assistants), principally for field collection of data.
    - Information Systems on the Internet: Development and implementation of high-tech solutions on the Internet.
    - Business Development: Internet solutions for information management within companies and for relations between companies.

    - ERP (Enterprise Resource Planning) and SAP Systems: Development of interfaces between technical applications and ERP/SAP, as well as implementation of these interfaces for the clients.
- *Industrial Installations:* Specialists in data centres, i.e. facilities used to house mission critical computer systems. ACT Systems develops installations with a security level for the IT equipment proportionally to current and future necessities for the client.

ACT Systems is today certified for ISO 9000 and ISO 14000.

ACT Systems is conducting big parts of their work in cooperation with partners, clients, or subcontractors. The principal part of ACT Systems' production is realized for the public sector, and some of the principal clients are the following:

- the Spanish Department of Environment
- the Spanish National Rail Administration
- the Spanish Autonomous Organization for National Parks
- EMASESA (the municipal water administration company in Seville, Spain)
- TUSSAM (the municipal traffic company in Seville, Spain)

The customers also include private companies, principally with business in Spain. Examples are Sevillana Endesa and IBM.

ACT Systems is a part of the Ayesa Group, that in 2003 had a turnover of more than 30,000 millions Euros. Apart from ACT Systems, the group consists of the following companies:

- Ayesa: Investigation and realization of projects in the construction sector.
- Aynova: Construction consultancy in the same sector as Ayesa.
- Ayesanet: Development of smart Internet solutions.

All information presented above has been found on the company web sites of ACT Systems and the Ayesa Group.

The technology strategy of ACT Systems is, according to the CEO Juan de Dios Hermosín Ramos, to be equipped with high security infrastructure (data centres). This has two purposes: (1) to have state-of-the-art installations with maximum security, and (2) to have the opportunity to offer services like outsourcing, housing, and hosting to third parties. The technology strategy also includes information systems. ACT Systems aims to have an ERP (Enterprise Resource Planning) platform that agglutinates all businesses of ACT Systems and the Ayesa Group and also some collaborative systems of maximum robustness that allows the employees to work out of office in a secure and stable way.

ACT Systems hopes that ISO/IEC 27000 will support the creation of an internal methodology that guarantees and facilitates the fulfilment and maintenance of the above mentioned objectives. ACT Systems does not exclude the possibility that an ISO/IEC 27000 certificate may give competitive advantages in the market for suppliers of technological services.

1.7 Thesis Outline

Chapter 1 is an introductory chapter including the background and purpose of the study, as well as a presentation of ACT Systems.

In *Chapter 2* the theoretical frame which will be used throughout this thesis work is presented, i.e. the theoretical models are introduced and they are related to each other and to the purpose of the study.

Chapter 3 is a presentation of the methodology of the work and gives an overview of the thesis' structure.

Chapter 4 presents the data collected in the empirical studies. This data will in chapter 5 be used for the comparisons between ISO/IEC 27000 and best practice.

In *Chapter 5* ISO/IEC 27000 is compared with best practice, both on an organizational level and on an ICT security specific level. This is done with the purpose to see if ISO/IEC 27000 corresponds to best practice.

Chapter 6 is an analysis of the conformity between ISO/IEC 27000 and best practice, based on the comparison in chapter 5. It is also an analysis of the conformity between ISO/IEC 27000 and ACT Systems' technology strategy.

Chapter 7 presents the conclusions whether ISO/IEC 27000 corresponds to best practice and whether it suits the technology strategy of ACT Systems.

In *Chapter 8* further recommendations are given.

Chapter 9 is a critical self evaluation of methodology and conclusions.

2 THEORETICAL FRAME

2.1 Introduction

In this chapter the theoretical models and concepts that are used to evaluate if ACT Systems should become certified with ISO/IEC 27001:2005, presupposed that there is a certain demand from customers, are introduced. When all models and concepts have been presented, they are related to each other and to the final purpose of the master thesis.

2.2 The Smart Organization

2.2.1 Introduction

From decades of consulting in Europe, Japan, and the United States, among others with the world's largest R&D intensive companies, as well as extensive work on strategic decisions of all kinds, the authors, David Matheson and Jim Matheson, have developed theories for how an organization can improve its decision quality and create more value by being "smart". These theories are presented in the book "The Smart Organization: Creating Value trough Strategic R&D" (1998).

David Matheson is a principal of the international management consulting firm "Strategic Decision Group", and has conducted extensive research into decision making. In addition to strategy consultancy, he conducts seminars for executives.

Jim Matheson, a founding director of "Strategic Decision Group", is a recognized leader in the development and application of decision analysis.

2.2.2 Decision Quality Chain

Matheson and Matheson (1998) have asked hundreds of R&D decision makers and executives what questions they would like to have answered before making an important decision. From the answers, they have compiled six categories. They call the model *the Decision Quality Chain*, describing the process for making good decisions. An important note is that a chain never is stronger than its weakest link.

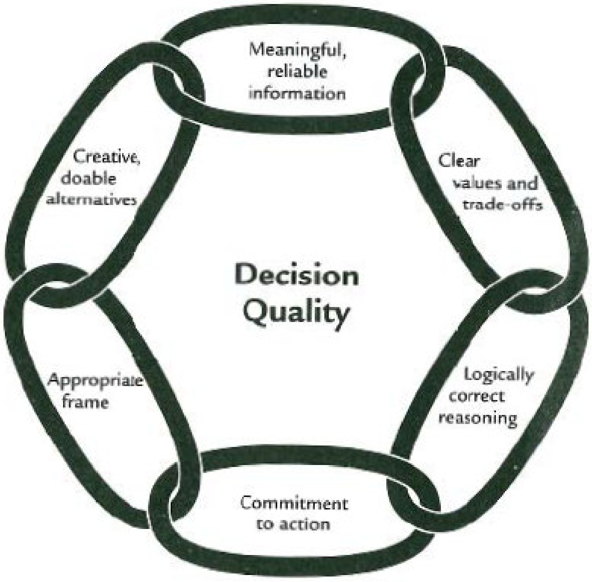

Meaningful, reliable information
Clear values and trade-offs
Logically correct reasoning
Commitment to action
Appropriate frame
Creative, doable alternatives
Decision Quality

Figure 1. The Decision Quality Chain with its six links.

Appropriate Frame

The frame is a window through which a particular problem is viewed, and thus it forms the background, setting, and context for the decision. To create and examine different frames, the decision situation should be exposed to people with different points of view, and a problem should never be accepted as first presented. To choose the appropriate frame, one should ask oneself what the problem really is and what kind of result is wanted. A correct frame helps the company to solve the right problem.

Creative, Doable Alternatives

The very definition of a decision is choosing between different alternatives, which can be a basis for comparison and discussion. A good decision-making process should therefore create multiple alternatives for management's consideration. The alternatives should be broadly constructed and not simply minor variations of a single concept, reasonable candidates for selection, and sufficiently numerous for presenting a true choice. Each alternative must also represent a comprehensive and feasible strategy and a viable way forward.

Meaningful, Reliable Information

As there are no sure facts about the future, the decision maker needs information providing the best possible insight. It is equally important to know what is unknown, and all uncertainties should be quantified as probability distributions. The first thing to know is what information is required for a good decision.

Clear Values and Trade-offs

To be able to compare different alternatives, the organisation needs to develop a metric that can be a basis for comparison and that represents the desired end objective of the enterprise. The use of multiple metrics often confuses decision makers. For most corporations, though other alternatives can be useful, net present value of cash flow is the most appropriate measure of value generation over time. Trade-offs among other forms of value are best made by assessing the corporation's willingness to pay for these things out of cash flow. However, the decision maker always has to deal with trade-offs like short term and long term, and because greater returns usually are accompanied by greater uncertainty, also with risk and return.

Logically Correct Reasoning

Reaching a conclusion based on evidence about which alternatives that will create most value, by considering alternatives, information, risks, and values in the context of the decision frame. "At the end of the evaluation, the result must be a clear, understandable recommendation – a concise story that's right. The "clear competitive advantage" is apparent and the decision "feels right"" (Matheson and Matheson (1998), page 26). Of fundamental importance is to manage the focus of attention, i.e. determine which factors are the most important for the decision.

Commitment to Action

It is here the decisions become activities, and for a successful implementation the full commitment from all involved people is needed. The best way to get this commitment is to involve the people who make or can veto the decision, as well as key implementers, into the process. Commitment also means that the people charged with implementing the decision will be given the resources and authority to get the job done without micromanagement from above.

2.2.3 The Nine Principles of a Smart Organization

Introduction

Matheson's and Matheson's research on decision quality has led to a specific set of principles that characterize an excellent organization, and that applies to all organizations that have its future tied up in the future of innovation, research, technology, or corporate renewal. According to Matheson and Matheson (1998, page 96), "these principles provide the organizational readiness that every company must have if it wants to be a top performer in R&D decision making or in anything else". Hence, these principles can be seen as best organizational practice. The more an organization is imbued with the principles, the fewer barriers stand between it and the implementation of best practice.

The principles can be organized around three important organizational functions: achieve purpose, understand the environment, and mobilize resources.

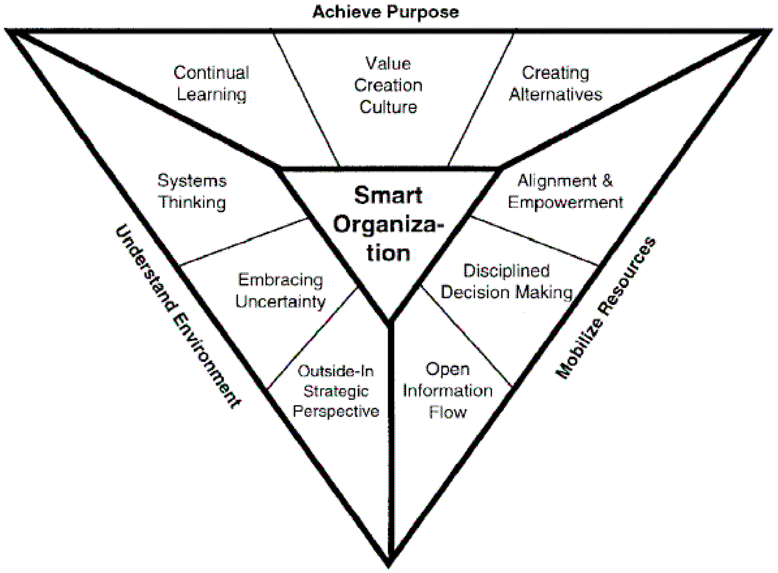


Figure 2. The Nine Principles of a Smart Organization.

Value Creation Culture

Having a value creating culture is having an orientation towards the ultimate value created by the organization and using value creation as a compelling argument for change. In the Smart Organization, creating value is an integral part of the organization's purpose, and this purpose is understood by everyone.

This understanding is used as a final test of whether strategies and actions are creating value. For a business model to be successful, it is important that value is created for all important stakeholders. Very few metrics should be used for calculating value. Most financial theory points at net present value of cash flow as the best primary economic measure. Having too many metrics is almost as bad as having none, because project champions will select a set of metrics making their own project looking good, biasing the decision. Furthermore, different metrics are often close to impossible to compare with each other.

Creating Alternatives

Strategic action should never be taken before multiple alternatives have been created and evaluated. The evaluation is normally based on net present value of cash flow. The alternative creating the greatest value for all important stakeholders should always be chosen. In fact, the best one is many times an alternative that was not even considered from the beginning. It may be a combination between several alternatives, or an entirely new one that has come up during the decision process. Without alternatives, there can be no true choice.

Continual Learning

The pace of change is constantly increasing. Being smart means continually learning how to create more value in the face of change. The Smart Organization identifies opportunities and paradigm shifts, and finds continuously new and better ways to create value. Bad news are welcomed, and used to initiate improvements. Personnel and resources are available for learning and experimentation. Absence of this principle creates barriers to the implementation of best practice. This absence is evidenced in the lack of proper skills. Continual learning also lifts the focus from the organization to the outer world, and thus overcome the common problem of internal focus.

Embracing Uncertainty

People in the Smart Organization understand how to deal with uncertainty. They measure what is not known and manage the associated risks. Uncertainty is never denied, but understood and managed. The key to embracing uncertainty is to communicate it, and to give forecasts the form of ranges or probability distributions. It is also important to know what is possible to influence and what is beyond control, and never promise something that is out of control. Smart Organizations identify the key sources of uncertainty, assess them as well as possible, and then create strategies with an appropriate balance of risk and return.

Outside-In Strategic Perspective

In the Smart Organization, important strategic decisions begin with an understanding of the broad territory in which the organization operates, and the dynamics of its industry and customers. Then it works inwards towards the implications for itself. The core of all activities must be a knowledge about what customers want and need, i.e. knowledge about the critical success factors. The Smart Organization starts to look at the end-customers, and then works back trough the value chain to understand the basis for competition at each stage. An outside-in approach gathers external information to form a broad conception of who customers are, how their needs are changing, how technology develops, and how the industry and its basis of competition may be altered. This gives a perspective that can be used to position the organization advantageously and possibly influence competition in favour of the own firm. Lacking an outside-in perspective, a company will always be a follower, and will never be prepared for future events.

Systems Thinking

A strategic situation is complex, and it is important to uncover complex cause-and-effect relationships from the perspective of the whole business. Systems thinking recognizes that everything is fundamentally connected to everything else, and that different actions have far-reaching and often counterintuitive consequences. Smart Organizations use systems thinking to understand the long-term implications of its decisions.

Open Information Flow

It is often impossible to tell in advance which information that is important, and the Smart Organization therefore creates open and virtually unrestricted information flows, even across functional boundaries. In a value-creating culture, everyone needs open access to information to do his or her job. People within the Smart Organization feel safe in sharing their information and obliged to contribute to the information sharing systems. To ensure open information flow, formal and informal communication channels like e-mail, groupware, workshops etc are abundant. No one keeps their information for themselves in order to exercise personal power. Research has shown that companies taking advantage of knowledge generated from many locations in the organization are significantly more productive than their rivals. The free flow of information across organizational boundaries is fundamental to build this knowledge. However, many organizations operate on the principle of restricting information to those “who need it”, with the purpose to protect almost all information from their competitors. The risk is that this attitude destroys more value in terms of poor decision making than it creates by the benefits of secrecy. It is important to distinguish the information that really should be protected, in order to ensure both secrecy and the benefits from open information flow.

Alignment and Empowerment

Everyone in the Smart Organization is aligned around common goals, and people are empowered to pursue value creation in order to meet these goals. Traditional hierarchical, command-and-control structures are too slow with fast-moving global competition. Employee empowerment is therefore needed, but for the empowerment to be effective there must be alignment. Empowerment without alignment is very probable to result in chaos. The Smart Organization uses participation in the decision-making process to achieve alignment in order to make the empowerment effective. When alignment is in place, higher-level decisions inform lower level decisions.

Disciplined Decision Making

Smart Organizations have processes for just about everything they do, including processes to recognize the need for strategic decisions before they are overtaken by events. They then apply systematic, disciplined decision processes, which involve the right people in order to secure their commitment to the final decision. This process is always used, for all kinds of projects. In a disciplined decision process, top executives participate already from the beginning at a new project, and continue to participate at important stages of the process. In this way, quality is built-in into the project from the start instead of having a top executive to judge a finished proposal and sending it back for rework.

2.3 Technology Strategy

Mark Dodgson is Professor of Management at the Australian National University, and is Executive Director of the Australia Asia Management Centre. He has researched and taught the management of technological innovation in over thirty countries, and many of his findings are published in the book "The Management of Technological Innovation" (2000).

Dodgson (2000) makes the definition that for technology-based organizations "technology strategy comprises the definition, development, and use of those technological competencies that constitute their competitive advantage" (page

134), and he says that technological innovation is a strategic issue for among others the following reasons:

- The use of technology is a key source for competitive advantage.
- The complex, uncertain, and expensive processes of R&D, new product development, and production and operations innovation will result in piecemeal, short-term, and potentially disruptive outcomes unless they are guided by a strategy that builds synergies and grows expertise cumulatively.
- The globalization of technology and markets requires companies to take a strategic approach to their technological investments.

Technology strategy involves identifying the key technologies that underpin the organization's present and future value-creating activities, and ensuring that they are improved, supplemented, and effectively introduced and used. Successful firms that rely on technological innovation look, according to Dodgson (2000), beyond their individual product lines and build a strategy around core knowledge and competencies.

Strategic matters include choosing and developing the competencies that shape organizations' opportunities for innovation and continuing competitiveness. The technological competencies of an organization consist of two elements: the resources available to the organization, and the innovative capabilities it possesses to define and change those resources. Some of the elements defined by Dodgson (2000) as resources are company routines and the technology base. The technological competencies have strategic potential if they are:

- valuable – exploit opportunities and/or neutralize threats in a firm's environment,
- rare – the number of firms that possess them is less than that needed to generate perfect competition in an industry,
- imperfectly imitable – because of their complexity, or the uniqueness of the conditions under which they are acquired, and
- have no strategically equivalent substitutes – no alternative ways of achieving the same results.

2.4 Benchmarking as a Management Technique

Since the capability of an organization concerns the ability to meet and beat the performance of competitors, it has to be assessed in relative terms. An independent, Internet based management portal presented by the Dutch strategy consultant Jaap de Jonge, Valuebasedmanagement.net, describes benchmarking as a systematic comparison of organizational performance and processes. The purpose is to create new standards or to improve processes by comparing the own organization with best practice. Different models are used to determine how well a business unit, division, organization or corporation is performing compared with other similar organizations. A benchmark is a point of reference for a measurement.

Johnson, Scholes and Whittington (2005) present three types of benchmarking methods:

- *Historical benchmarking:* Benchmark for evaluating the performance relative previous years. Can also be used for benchmarking for example between different business units. The danger is that it can lead to complacency since it is the rate of improvement compared with competitors that is important.
- *Industry benchmarking:* Benchmark performance or processes with competitors, and other similar processes, within the industry. The danger is that the whole industry may be performing badly compared with other industries that satisfy customer needs in different ways. Another important note about this kind of benchmarking is that the boundaries of industries are blurring through competitive activity and industry convergence.
- *Best-in-class benchmarking:* Benchmark best practice wherever it may be found. The power of this method is that today, organizations face threats from other organizations that achieve dramatic improvements in performance on particular value activities or through how activities are linked together. A critical issue is that improved performance in one sector shifts the general level of expectations among customers. This is especially the case according to speed and reliability. Best-in-class benchmarking can be used to spot opportunities to outperform incumbent providers.

According to Valuebasedmanagement.net, benchmarking generally involves the following steps:

1. Define the scope of the benchmarking
2. Choose benchmark partner(s)
3. Determine measurement methods, units, indicators, and data collection method
4. Collect data
5. Analyse similarities and discrepancies
6. Present the results and discuss implications, improvement areas, and goals
7. Make improvements and new procedures
8. Monitor the progresses and plan ongoing benchmark

Another independent, web based management portal also presented by Jaap de Jonge, 12manage.com, says that comparing performances and processes with the "best in class" is important and should be done on a continuous basis as the competition must be expected to continuously improve its processes as well. However, one should be clear with that benchmarking is a tough, time-consuming, and expensive process. The process itself can take over and cloud the purpose of the exercise. Too often benchmarking projects end with the "they are different from us" syndrome or competitive sensitivity prevents the free flow of information that is necessary. If the benchmark is done as a profound study of the processes of one or a few companies, a lot of commitment is needed in order to succeed. Moreover, one should ask oneself if the success of the target company really is attributable to the best practice that is benchmarked, and if there are any downsides by implementing the new practice. The benchmark can result in behavioural changes that are unintended and even dysfunctional.

2.5 Interconnections within the Theoretical Frame

The purpose of this master thesis is to evaluate if ACT Systems should become certified with ISO/IEC 27001:2005, presupposed that there is a certain demand from customers. The method used to reach this purpose is to compare the standard with best practice, both on an organizational level and on an ICT security specific level. To find best practice on an ICT security specific level, a benchmarking study of more developed markets has been conducted. Matheson's and Matheson's theory for the Smart Organization (1998) has been considered best practice on an organizational level.

In this master thesis, two models from the theory of a smart organization have been applied: the Decision Quality Chain and Nine Principles of a Smart Organization. Matheson's and Matheson's original research was on decision making in organizations. When they had developed their Decision Quality Chain, next question was why certain organizations always seem to make good decisions. To answer this question, Matheson and Matheson found a big number of best practices that distinguish these organizations from others. Further research found out how an organization should be to be able to implement these best practices: it should have the Nine Principles of a Smart Organization. To develop these models, Matheson and Matheson conducted extensive benchmarking studies.

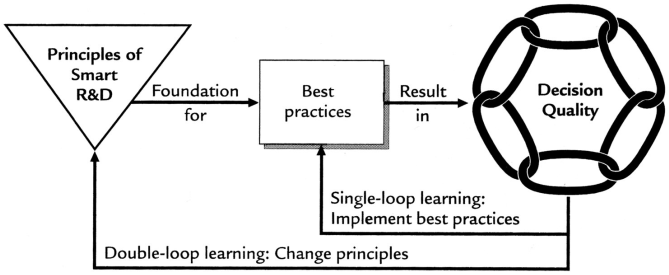


Figure 3. To make good decisions, or to excel at anything else, an organization must have some principles in place. Without these principles, it is very hard to develop the organization and to implement best practice.

To evaluate if ACT Systems should become certified with ISO/IEC 27001:2005, the standard has also been put in the context of ACT Systems' technology strategy.

3 METHODOLOGY

3.1 Introduction

This chapter presents how the work with this master thesis has been conducted, and how the theoretical frame has been selected and elaborated. All parts of the process are related to the purpose, i.e. to evaluate if ACT Systems should become certified with ISO/IEC 27001:2005. All choices that have been carried out throughout the work are motivated. The chapter ends with a discussion about validity and reliability.

3.2 Research Approach

Figure 4 gives a schematic view over the project. The figure underlines that the empirical studies and the theoretical frame have been elaborated in parallel. It also illustrates how each part of the work contributes to take the project forward from the initial purpose to the final conclusions.

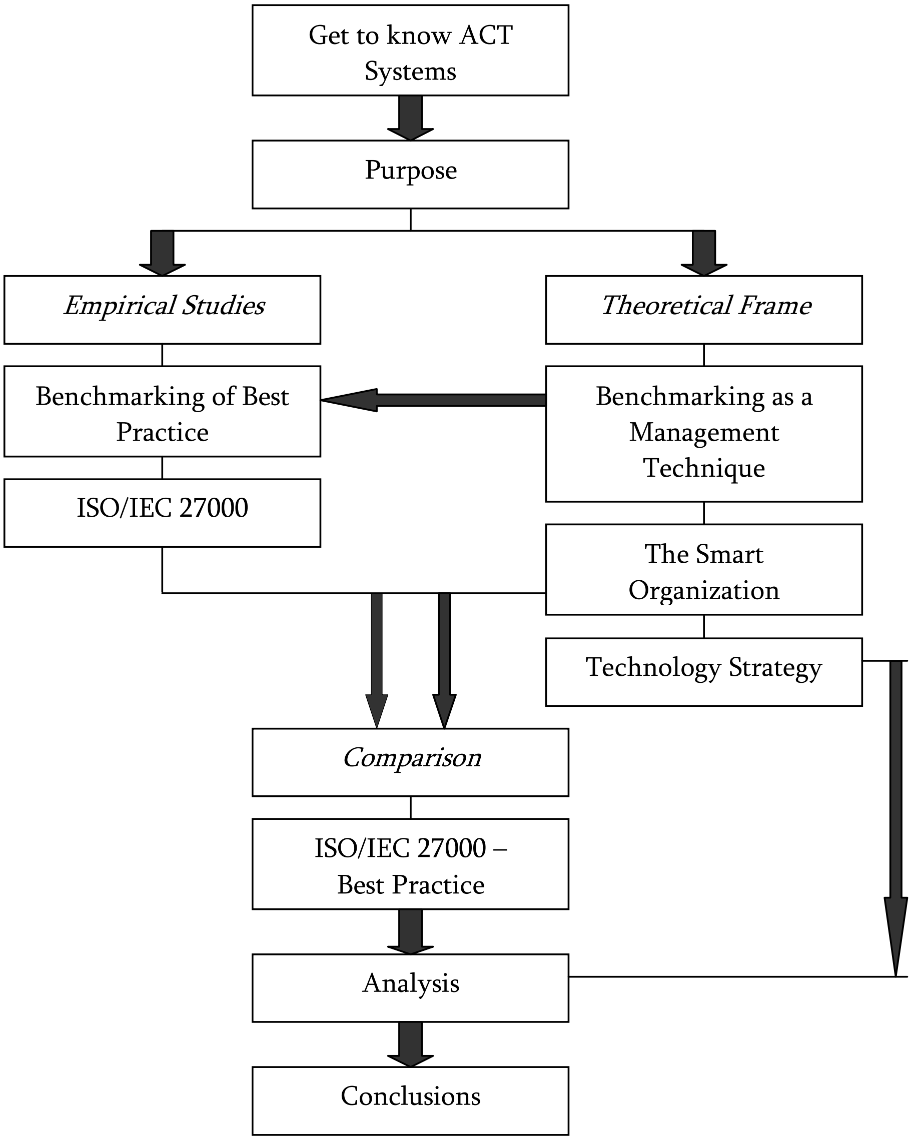


Figure 4. Graphical presentation of the structure of the master thesis. As shown, the development of the theoretical frame and the empirical studies have been conducted in parallel, and finally the information has been brought together. The master thesis is finished with conclusions where the purpose is targeted. The figure shows how the theoretical frame has been used throughout the master thesis.

Both ISO/IEC 27001:2005 and ISO/IEC 17799:2005, the parts of the ISO/IEC 27000 family that had been published when realizing this master thesis, have been studied. For each standard, a summary is presented because the basis in the evaluation whether or not ACT Systems should become certified is knowledge about the standards.

A benchmarking study has been realized with the purpose to map best practice in northern Europe. The European perspective is a desire from ACT Systems. This benchmarking has been divided into three parts. The first part aims to study best practice on a device specific level, i.e. in which concrete ICT security devices do northern European companies invest? For this part of the benchmarking study, Sweden has been chosen to represent northern Europe. The purpose with the second part is to map the use of ISO/IEC 27000 worldwide, to see to what extent companies choose to become certified. These two first parts of the benchmarking have been conducted by a study of statistics on the Internet. The third part aims to investigate the trends and the current debate in relation to ISO/IEC 27000. The reason why this has been considered interesting is that the subjects that experts and trade press are treating often is a current best practice. Moreover, the subjects found in the current debate are often of immediate importance. This part of the benchmarking has been conducted by studying articles in the trade press and on the Internet.

Hence, the benchmarking of northern Europe is based entirely on secondary data. It would be interesting to conduct profound interviews with a few northern European companies as a part of the benchmarking. However, selecting these companies would require an extensive selection process to ensure that the companies chosen actually represent best practice.

The purpose of this master thesis is to evaluate if ACT Systems should become certified with ISO/IEC 27001:2005, presupposed that there is a certain demand from customers. This has been done through comparing ISO/IEC 27001:2005 and ISO/IEC 17799:2005 with best practice. The idea with this method is to see if the recommendations presented in ISO/IEC 27000 are in line with best practice. The most important, maybe the only, reason to become certified is if the customers demand it. ACT Systems has already seen a certain interest from customers, but it is a new standard and it is still to early to say if it will have a breakthrough. Through the benchmarking, it is possible to see if the processes and controls presented in the standard can develop the company in the same direction as best practice. If so, an implementation should be considered and ACT Systems will have the opportunity to get competitive advantage by becoming a fist mover. If ISO/IEC 27000 does not seem to develop ACT Systems in the same direction as best practice, other measures for improving the company's ICT security should be considered. The best practices with which ISO/IEC 27000 is compared are the following:

- The theory of the Smart Organization, presented by Matheson and Matheson (1998), treats how an organization should be and act. This is a best practice generally valid for all organizations. This best practice will in the following be referred to as Best Organizational Practice. This has been compared with the processes presented in ISO/IEC 27000. When comparing the theory of the Smart Organization with ISO/IEC 27001:2005, all processes presented by the standard were went trough carefully. At the same time, the theory of the Smart Organization was considered for comparison. Matheson's and Matheson's theory of the Smart Organization has been chosen because it is thoroughly elaborated through many years of studies and consulting of hundreds of companies. Matheson and Matheson primarily focus on the Smart Organization in terms of strategic R&D, but they use the term R&D in its broadest sense to mean any technologically related activity that has the potential to renew or extend present business or to generate new ones. They also state that the Smart Organization can be generalized to all functions and major business areas. This theory is very interesting for ICT security specifically, because state-of-the-art technology is no guarantee for good security, but an excellent security must come from a well implemented strategy and be augmented by inputs from the employees. Technology ensures the success of a winning strategy, but it does not automatically solve ICT security problems.

- Best practice on an ICT security specific level has been benchmarked in accordance with the description above. This best practice will in the following be referred to as Best ICT Security Specific Practice. This best practice has been compared with the controls suggested in ISO/IEC 17799:2005, but also with the processes presented in ISO/IEC 27001:2005. For the comparison, the results from the benchmarking study has been compiled into a number of controls and processes, i.e. best practices. These controls and processes have after that been compared with the controls and processes recommended by ISO/IEC 27000. Does ISO/IEC 27000 suggest the measures that are used by companies on more developed markets and that are accentuated in the current debate? Where do they differ? And what does the current debate say about ISO/IEC 27000?

Comparing the standard with both Best Organizational Practice and Best ICT Security Specific Practice gives a wider picture of how the standard eventually can develop ACT Systems. It is also considered how ISO/IEC 27000 fits into the technology strategy of ACT Systems.

3.3 Motivation for the Choice of Benchmarking Object

The choice of benchmarking object has been made with the assumption that northern Europe is more developed than southern Europe in its use of ICT. This assumption is based on experience shared by the author of this master thesis, and Juan de Dios Hermosín, CEO at ACT Systems. Countries like the United States and Japan have not been considered because the study aims to give a European perspective. This is a wish from ACT Systems. In the first part, where the use of different ICT security devices is studied, Sweden has been chosen to represent northern Europe. The choice of Sweden is motivated by the fact that Sweden through modern history often has been a precursor in its use of ICT and as the author is from Sweden, he has a specific knowledge about the Swedish market and potential Swedish information sources. A benchmark of several northern European countries would have given a more general point of view, but because of the time limit of the project one specific country has had to be chosen.

The following statistics show the advance of Sweden versus Spain in broadband access, both for enterprises and private persons, in percentage of employees working out of office accessing the enterprise’s IT system from there, and in the percentage of companies that have taken ICT precautions. It can also be seen that Sweden has an advantage over all years included in the study, and can therefore be seen as a precursor. The difference was even bigger some years ago. This statistics supports the assumption that Sweden is more and earlier developed than Spain in its use of ICT, and that Spanish companies historically have gone the same path but some years later. Therefore, it is interesting to see the trends in Sweden, as the same trends probably will arise in Spain. This supports the choice of Sweden as subject for a benchmarking of best practice.

Percentage of enterprises with broadband access (Eurostat, 30 October).

	All companies			10-249 employees			250+ employees		
	2003	2004	2005	2003	2004	2005	2003	2004	2005
EU (25 countries)	..	52	63	..	50	62	..	86	92
Spain	51	72	76	50	71	76	84	94	93
Sweden	62	..	83	61	..	82	97	..	98

Percentage of enterprises with employees working part of their time away from enterprise premises and accessing enterprise's IT systems from there (Eurostat, 30 October).

	All companies			10-249 employees			250+ employees		
	2003	2004	2005	2003	2004	2005	2003	2004	2005
EU (25 countries)	..	16	19	..	15	18	..	54	62
Spain	7	9	8	6	8	8	42	43	45
Sweden	36	39	40	35	38	39	82	84	85

Percentage of enterprises having taken ICT precautions (Eurostat, 30 October)

	All companies			10-249 employees			250+ employees		
	2003	2004	2005	2003	2004	2005	2003	2004	2005
EU (25 countries)	..	87	89	..	86	89	..	99	99
Spain	35	87	89	34	87	88	76	99	98
Sweden	92	94	95	92	Confidential	95	99	Confidential	99

Figure 5. Statistics showing the percentage of enterprises with broadband access, the percentage of companies with employees working part of their time away from enterprise premises and accessing enterprise's IT systems from there, and the percentage of enterprises having taken ICT precautions. The financial sector is not included. "All companies" include companies with more than 10 employees.

OECD (www.oecd.org) develops statistics over the broadband penetration rates, and concludes that northern European countries continue their advance with all five Nordic countries among the eight with best broadband penetration worldwide in June 2006. The ranking is as follows, with the number representing the percentage of subscribers in each country:

1.	Denmark	29,3 %
2.	Netherlands	28,8 %
3.	Iceland	27,3 %
4.	Korea	26,4 %
5.	Switzerland	26,2 %
6.	Finland	25,0 %
7.	Norway	24,6 %
8.	Sweden	22,7 %
:		
19.	Spain	13,6 %

3.4 Validity and Reliability

Northern Europe is chosen as benchmarking object, a selection based on an assumption. However, this assumption is considered being so well-founded that it should not affect the validity negatively. On the other hand, the assumption that Sweden can be considered representing northern Europe is less well-founded, and can possibly have a negative influence on the validity. The assumption that Sweden can be considered as best practice relative to Spain has anyway a good validity. This is seen in the statistics represented above. Even if the statistics show isolated examples and not the overall picture, these examples are considered to complement each other and that they therefore give a relatively good validity. The benchmarking has a good reliability because it is conducted by studying comprehensive statistics and expert opinions, and not by choosing single benchmarking objects.

4 ICT SECURITY IN THEORY AND PRACTICE

4.1 Introduction

The chapter presents data collected from the empirical studies. This includes summaries of ISO/IEC 27001:2005 and ISO/IEC 17799:2005, and the results from the benchmarking of Best ICT Security Specific Practice.

4.2 Summary of ISO/IEC 27001:2005

4.2.1 Introduction

This text is a summary of ISO/IEC 27001:2005, aiming to give the reader an overview of the most important parts of the standard. The standard presented here will in later chapters be compared with Best Organizational Practice, to see if it supports the principles of the Smart Organization, and to Best ICT Security Specific Practice, to see if the processes recommended by the standard correspond to the findings from the benchmarking study. These comparisons have been done in order to evaluate if ACT Systems should become certified.

ISO/IEC 27001:2005 presents a process approach for the implementation of an Information Security Management System (ISMS). These processes are structured with the "Plan-Do-Check-Act" (PDCA) model. A process approach is the application of a system of processes within the organization, including establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented ISMS within the context of the organization's overall business activities and the risks it faces. The design and implementation of an ISMS are influenced by the company's individual needs and objectives, security requirements, the processes employed, and the size and structure of the organization. This design and implementation have to be continually improved. ISO/IEC 27001:2005 is the part of the ISO/IEC 27000 family that is used for accreditations. The other standards in the family are different kinds of support for the processes presented here. For example, ISO/IEC 17799:2005 provides implementation guidance when designing controls.

ISO/IEC 27001:2005 is aligned with ISO 9001:2000 and ISO 14001:2004 in order to support a consistent and integrated implementation and operation in relation to these management standards. One single, suitably designed management system can thus satisfy the requirements of all these standards. This means that if the organization already has an operative business process management system, e.g. ISO 9001:2000 or ISO 14001:2004, it is in most cases preferable to satisfy the requirements of ISO/IEC 27001:2005 within this existing management system.

4.2.2 The "Plan-Do-Check-Act" Model

The "Plan-Do-Check-Act" (PDCA) model that structures the processes takes inputs from interested parties, and after processing these inputs it delivers information security outcomes that meet requirements and expectations from stakeholders, see *Figure 6*.

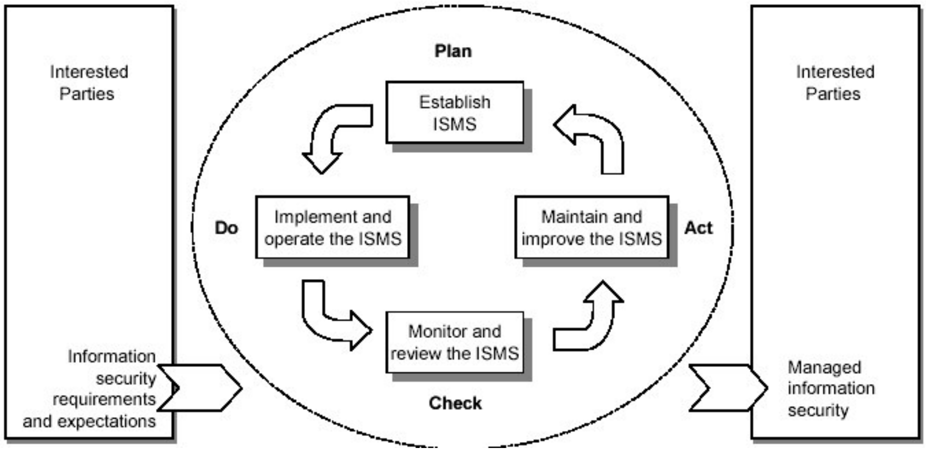

Interested Parties
Information security requirements and expectations
Plan
Establish ISMS
Do
Implement and operate the ISMS
Act
Maintain and improve the ISMS
Monitor and review the ISMS
Check
Interested Parties
Managed information security

Figure 6. The "Plan-Do-Check-Act" (PDCA) model. The picture illustrates how the different processes in the ISMS are structured and related.

Plan is about understanding the organization's information security requirements and the need to establish policies, objectives, and processes relevant for risk management and information security. *Do* treats the implementation and operation of these policies, controls, and processes in order to manage the organization's overall business risk. *Check* includes monitoring, measuring, and reviewing the performance and effectiveness of the ISMS. *Act* is about continual improvements based on objective measurements.

4.2.3 The Information Security Management System (ISMS)

In the following, the different processes included in the ISMS are presented.

Establish the ISMS

The ISMS should be established in terms of the organization's business, structure, location, assets, and technology. Scope and boundaries should be defined first, and after that an ISMS policy. The policy should include a framework for setting objectives and establishing an overall sense of direction as well as principles of action with regard to information security. The policy should also establish criteria against which risk will be evaluated. When these definitions are made, a risk assessment methodology suited to the ISMS should be identified. The methodology must ensure that the risk assessments produce comparable and reproducible results. Criteria for accepting risks must be developed.

Next step in the establishment of the ISMS is to identify the risks. This is done in four steps: (1) identify the assets within the scope of the ISMS, (2) identify the threats to those assets, (3) identify the vulnerabilities that might be exploited by the threats, and (4) identify the impacts that losses of confidentiality, integrity and availability may have on the assets.

When the risks are identified, the risk levels should be estimated. This should be done by assessing the impacts that might result from security failures, and the realistic likelihood of each failure. Determine if the risks are acceptable or not using the criteria for accepting risks developed earlier. Next step is to identify and evaluate options for risk treatment. These options might include the application of appropriate controls to reduce the risks, acceptance of risk, avoidance of risk by not allowing actions that would cause the risks to occur, and transference of risk to other parties, e.g. insurance companies or suppliers. Finally, control objectives and controls can be selected and implemented. When all this is done, management approval of the proposed residual risks, and management authorization to implement and operate the ISMS, must be obtained

Implement and Operate the ISMS

The metrics selected above have to be implemented, together with a risk treatment plan that identifies appropriate management actions, resources, responsibilities and priorities for managing information security risks. It also has to be defined how to measure the effectiveness of the selected controls.

Training and awareness programs, and procedures capable of enabling prompt detection of security events, have to be implemented.

Monitor and Review the ISMS

The organization has to execute monitoring and reviewing procedures regularly, in order to promptly detect errors and identify attempted and successful security breaches and incidents. These procedures shall also enable management to determine whether the security activities delegated to people or implemented by information technology are performing as expected, as well as determine whether the actions taken to resolve a breach of security have been effective.

Maintain and Improve the ISMS

The organization shall regularly implement identified improvements, communicate actions and improvements to all interested parties, and ensure that the improvements achieve their intended objectives. It shall also apply the lessons learnt from security experiences of other organizations as well as those of the organization itself.

4.2.4 Management Responsibility

This part of the standard regularizes management commitment and resource management. Management commitment includes, besides initiating and managing the ISMS, the need of communicating the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under law, and the need of continual improvement. Resource management includes providing sufficient resources and securing appropriate training, awareness and competence. An important part of this is ensuring that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

4.2.5 Audits and Reviews

The organization shall conduct a planned ISMS audit programme, with the realization of audits at planned intervals, to determine whether the control objectives, controls, and processes of its ISMS conform to the standard, legislation, and identified information security requirements, that they are effectively implemented and maintained, and that they perform as expected.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Auditors must be objective and impartial to the audit process.

Also the management shall review the organization's ISMS at planned intervals to ensure continued suitability, adequacy, and effectiveness, including the information security policies and objectives. The input to this management review shall include results of audits, feedback from stakeholders, techniques, products and procedures which could be used in the organization to improve its ISMS performance and effectiveness, status of preventive and corrective actions, experiences and results from effectiveness measurements, and environmental changes. The output shall include modifications and improvements, an updated risk assessment, and allocated resources.

Audits and management reviews, as well as the usage of policies and objectives, shall be used to continually improve the effectiveness of the organization's ISMS. The improvement shall also include corrective actions to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence, and preventive actions to eliminate the cause of potential nonconformities. The organization shall identify changes in risk and preventive action requirements.

4.2.6 Control Objectives and Controls

ISO 27001:2005 contains a list of control objectives and controls, from which adequate parts shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. The list is not exhaustive and additional control objectives and controls may also be selected. ISO/IEC 17799:2005 provides implementation guidance on best practice in support of these controls.

4.3 Summary of ISO/IEC 17799:2005

4.3.1 Introduction

The information security that can be achieved through solely technical means is limited. Excellent information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and responsibilities, in conjunction with software and hardware functions. This requires participation from the entire organization, and may also require participation from shareholders, suppliers, customers, external specialists, and other external parties.

This chapter is a summary of ISO/IEC 17799:2005, and the information presented will in later chapters be used to investigate if the standard takes ACT Systems in the same direction as best practice. ISO/IEC 17799:2005 is a code of practice and presents a set of controls that apply to most organizations and in most environments, and that can be considered as a good starting point for initiating, implementing, maintaining, and improving information security management in an organization. These controls are either based on essential legislative requirements or considered to be common practice for information security. There may be controls presented in this standard that is not applicable for all organizations, and there may also be a need for implementing controls not presented here.

ISO/IEC 17799:2005 contains an introductory clause introducing risk management and treatment, and eleven information security control clauses, each one presented in the following chapters. Each security control clause contains a number of main security categories, each one containing a control objective stating what is to be achieved, and one or more controls that can be applied to achieve this control objective. All these controls are presented in Appendix A in ISO/IEC 27001:2005. The contribution of ISO/IEC 17799:2005 is foremost implementation guidance to all these controls.

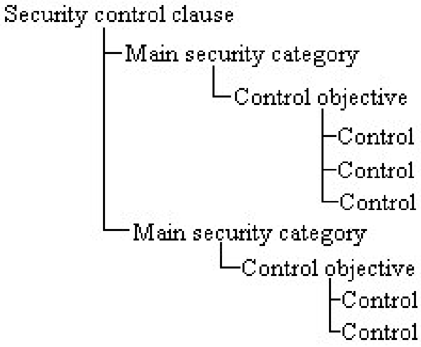


Figure 7. A schematic figure of the structure of ISO/IEC 17799:2005.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into the ISO/IEC 27000 family under the name ISO/IEC 27002.

4.3.2 Risk Assessment and Treatment

Risk assessment should identify potential risks, estimate the magnitude of these risks (risk analysis) and compare the estimated risks with decided risk criteria to determine their significance (risk evaluation). These risk criteria should determine whether or not risks can be accepted. A risk can be accepted if it is assessed that the risk is low or that the cost of treatment is not cost-effective. For those risks where the risk treatment decision has been to apply appropriate controls, these controls should ensure that risks are reduced to acceptable levels taking into account implementation costs versus the risk being reduced and the harm likely to result. To ensure continuous improvement, risk assessments should be performed periodically.

4.3.3 Security Policy

In order to provide direction and support for information security in accordance with business requirements and objectives, as well as with relevant laws and regulations, an information security policy should be established, receive management approval, and be published and communicated to all employees and relevant external parties.

4.3.4 Organization of Information Security

A management framework should be established to ensure that information security goals are identified, and to initiate and control the implementation of information security within the organization. Management should provide clear direction and visible management support for security activities, allocate and clearly define information security responsibilities, and coordinate and review the implementation of security across the organization, encouraging a multi-disciplinary approach to information security. These management responsibilities could be handled by a dedicated management forum or an existing management body, such as the board of directors. Besides management reviews, the information security should be reviewed independently at planned intervals. Needed resources should be provided and internal expertise as well as external contacts should be established. The external contacts should ensure expertise as well as legal or other kinds of support and can consist of authorities as well as special interest groups.

Extra controls should be in place when implementing products or services from external parties, and when giving external parties access to the organization's information or information processing facilities. In these situations, it is important to make an agreement clearly stating all rights, responsibilities, and liabilities before access is given.

4.3.5 Asset Management

The term asset includes information, software, physical assets, services, people, and intangible assets like image and reputation. In order to achieve and maintain appropriate protection of all assets, they should be clearly identified and an asset inventory should be created. Responsibility should be identified for each asset.

Information has varying degrees of sensitivity, criticality, value, and legal requirements, and different information should therefore receive different levels of security. To ensure this, all information should be classified to indicate the needs, priorities, and expected degree of protection when handling it. All information should be given appropriate security, but over-classification may result in additional expenses. In accordance with the classification scheme, an appropriate set of procedures for information labelling and handling should be developed and implemented, i.e. information classified as being sensitive or critical should carry an appropriate label and be handled with special procedures.

4.3.6 Human Resources Security

Prior to employment, security responsibilities should be addressed in terms and conditions in accordance with the organization's information security policy, and all candidates, contractors and third party users should be adequately screened and, if adequate, sign an agreement on their security roles and responsibilities. All this to ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce risk of theft, fraud or misuse of facilities.

During employment, all employees, contractors and third party users should be provided an adequate level of awareness, education, and training in security procedures and requirements, and in the correct use of information processing facilities. Management has an important assignment in spurring the employees to conform to the organization's information security policy. A formal disciplinary process for handling security breaches should be established, to ensure correct and fair treatment of employees who are suspected of committing breaches of security.

If exiting the organization or changing employment, responsibilities should be in place to ensure that an employee's, contractor's or third party user's exit or transfer is managed, and that the return of all equipment and documentation, and the removal of all access rights, are completed. There is a risk that the person leaving wants to collect information for future use.

4.3.7 Physical and Environmental Security

Secure Areas

Critical or sensitive information and information processing facilities should be housed in secure areas, protected by appropriate security barriers and controls. This chapter presents the barriers and controls having this purpose that are recommended by ISO/IEC 17799:2005 .

The perimeters of a building should be physically sound, including external walls of solid construction, external doors equipped with control mechanisms such as alarms and locks, and external protection considered for windows. Multiple physical barriers can be used if considered appropriate. This physical protection should protect against access of unauthorized persons, but also from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.

Hazardous or combustible materials should be stored at a safe distance from a secure area, and appropriate fire fighting equipment should be provided and suitably placed. Also fallback equipment and back-up media should be sited at a safe distance from the main site. This to avoid damage from a disaster affecting this.

Physical access to secure areas should be protected by appropriate entry controls and be restricted to authorized personnel only. This should be ensured by for example access control card plus PIN or manned reception desks. Unsupervised working in a secure area should be avoided both for safety reasons and to prevent opportunities for malicious activities. Access rights to secure areas should be restricted, and regularly reviewed and updated.

Access points where unauthorized persons may enter the premises, such as delivery and loading areas, should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. All incoming material should be inspected before it is moved from the delivery or loading area to the point of use.

Everyone entering a secure area, employees as well as visitors, should be required to wear some form of visible identification.

All fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable standards.

Suitable intruder detection systems should be installed to cover all external doors and accessible windows, and unoccupied areas should always be alarmed. Cover should also be provided for areas such as computer rooms.

Information processing facilities managed by the organization should be physically separated from those managed by third parties.

Where applicable, buildings should be unobtrusive and give minimum indication of their purpose and with no obvious signs identifying the presence of information processing activities. Personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis.

Photographic, video, audio or other recording equipment should be forbidden, unless authorized.

Equipment Security

Equipment should be protected from physical and environmental threats, in order to prevent loss, damage, theft, unauthorized access or compromise of assets and interruption to the organization's objectives. To attain this, ISO/IEC 17799:2995 presents the following controls.

Equipment should be sited to minimize unnecessary access into work areas. Information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons.

Items requiring special protection should be isolated to reduce the general level of protection required.

Controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water, dust, vibration, chemical effects, lightning, electrical supply interference, communications interference, electromagnetic radiation, and vandalism. Environmental conditions, such as temperature and humidity, should be regulated.

Equipment should be protected from failures in supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air condition. An alarm system to detect malfunctions in the supporting utilities should be evaluated and installed if required.

In case of emergency, power off switches should be located near emergency exits in equipment rooms, and emergency lightning should be provided.

Power and telecommunications cabling should be protected from interception or damage. Where possible, they should be laid underground and conduits should be used. To prevent interference, power cables and telecommunications cables should be separated. For sensitive and critical systems, further controls should be considered, including the installation of armoured conduit, locked rooms or boxes at inspection and termination points, use of alternative routings and/or transmission media providing appropriate security, use of fibre optic cabling, use of electromagnetic shielding to protect the cables, and controlled access to patch panels and cable rooms.

Equipment should be correctly maintained. Where necessary, sensitive information should be cleared from the equipment before maintenance. Records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance.

For off-site equipment, security should take into account the different risks of working outside the organization’s premises. Equipment should not be left unattended in public places or checked-in at airports, the equipment manufacturer's protection instructions should always be observed, and adequate insurance cover should be in place.

Prior to disposal, devices containing sensitive information should be physically destroyed or the information should be destroyed or deleted using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Equipment, information or software should not be taken off-site without prior authorization, and persons with authority to permit off-site removal should be clearly identified. Where appropriate, equipment should be recorded as being removed off-site and recorded when returned, and time limits for removal should be set.

4.3.8 Communications and Operations Management

To ensure a correct and secure operation of information processing and communication facilities, a set of procedures should be established. The ones recommended by ISO/IEC 17799:2005 are presented in this chapter.

All changes to these facilities should be controlled and formally approved. To reduce the risks of accidental or deliberate changes, as well as the risk of unauthorized access, development, test, and operation should be separated into different computing environments.

Managerial responsibilities should be established to reduce the risk of accidental or deliberate misuse of the organization's assets. This should include segregation of duties and areas of responsibility, which implies that no single person should be able to access, modify, or use assets without authorization or detection.

It should be ensured that security controls and service definitions included in a third party service delivery agreement, for example in an outsourcing arrangement, are implemented, operated, and maintained by the third party.

To minimize the risk of system failure, and to ensure the availability of adequate capacity and resources to deliver the required system performance, advanced planning, preparation, and projection of future capacity are required.

Prior to the acceptance and use of a new system, operational requirements should be established, documented, and tested.

Protection against malicious code, e.g. viruses, network worms, and Trojan horses, should be based on detection and repair software, security awareness procedures, and appropriate system access and change management controls. Detection and repair software should check all files stored or received over networks, e-mail attachments and downloads, and web pages visited, and they should be updated regularly. Software and data content of systems supporting critical business processes should be reviewed regularly and the presence of any unapproved files or unauthorized amendments should be formally investigated. In order to recover from malicious code attacks, business continuity plans including back-ups and recovery arrangements should be prepared. Extra attention has to be paid during maintenance and emergency procedures, when normal protection controls may be set out of operation.

Mobile code is software code which is transferred from one computer to another and then executes automatically to perform a specific function with little or no user interaction. The use of this kind of code should be controlled and restricted.

In order to ensure that all essential information and software can be recovered following a disaster or media failure, routine procedures should be established for regularly taking and testing back-up copies. The back-ups should be stored in a remote location, separated from the main site. The extent and frequency of back-ups should reflect the organization's business requirements, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization.

In order to protect information in networks and the supporting infrastructure, as well as secure the protection from threats, network security management is needed. To ensure security features and service levels, all network services should be identified and included in any network service agreement. Special importance should be paid to public and wireless networks. To ensure that the network security not is overlooked, operational responsibility for networks should be separated from computer operations where appropriate.

Media, such as documents, hard drives, and DVDs, should be controlled and physically protected from unauthorized disclosure, modification, removal, and destruction.

Exchange of information and software, through all types of communication channels, should be based on formal policies, procedures, and controls, be carried out in line with exchange agreements, and be compliant with any relevant legislation. These procedures and controls should include protection against interception, copying, modification, mis-routing, destruction, and malicious code, as well as guidelines for an acceptable use of electronic communication facilities, user responsibilities, and user awareness about overhearing, eavesdropping etc. During transportation beyond an organization's physical boundaries, media should be protected against unauthorized access, misuse, corruption, and environmental damage.

Electronic commerce and on-line transactions should be commensurate protected to prevent fraud, incomplete transmission, mis-routing, disclosure etc. Many of these considerations can be addressed by the application of cryptographic controls, digital signatures, secured communication protocols, and secured storage of transaction details. Security considerations should include documented agreements concerning terms of trading, integrity, confidentiality, and insurance as well as legal requirements. Access to publishing systems should not allow unintended access to networks to which the system is connected.

All user activities and exceptions, as well as all faults, should be logged, and the log should be kept for an agreed period of time to assist in future investigations and access control monitoring. Fault logs should be reviewed to ensure that the faults have been satisfactory resolved. Also system administrator and system operator activities should be logged, using a system outside of the control of system and network administrators. Monitoring should be conducted with the purpose to detect unauthorized information processing activities and to check the effectiveness of controls adopted. The results of the monitoring activities should be reviewed regularly, and information security events should be recorded. A risk assessment should determine the level of monitoring required for individual facilities, and as both logging and monitoring may contain intrusive and confidential personal data, appropriate privacy protection measures and regards to legal requirements should be taken.

4.3.9 Access Control

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements. An access control policy, clearly stating rules and rights for each user, should be established, documented, and reviewed. Access controls are both logical and physical and these should be considered together. Formal procedures should be in place for access authorization and password allocation.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. The latter should have appropriate protection if left unattended, i.e. active sessions should be terminated when finished and locked when temporarily not in use. A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

To prevent unauthorized access to internal and external networks, operating systems, and information held in application systems, security means based on a risk assessment and reflecting the security risks of the area should be used to classify the information being handled and the applications being used. Access should be controlled by a secure log-on procedure, and systems for managing passwords should be interactive and ensure quality passwords. Where it is considered appropriate, cryptographic means, smart cards, tokens, or biometric means should be considered as an alternative to passwords. When system security policies are breached, an alarm should be issued.

User access to networks and network services should not compromise the security of these services. To prevent this, it should be ensured that appropriate interfaces, e.g. firewalls, are in place between the organization's network and networks owned by other organizations and public networks. Moreover, automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment, physical and logical access to ports for remote diagnostic or configuration should be controlled, large networks should be divided into separate logical network domains protected by defined security parameters such as firewalls, and routing controls based on source and destination address checking mechanisms should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. Network access control is especially important for shared networks, above all those extending the organization's boundaries. For operating systems, restrictions on connection times, both in terms of session duration and restrictions to for example normal office hours, should be considered.

Teleworking uses communication technology to enable personnel to work remotely from a fixed location, e.g. from home. When using teleworking or mobile computing and communication facilities, e.g. laptops, palmtops, and mobile phones, special policies, operational plans and procedures should be in place to ensure that business information is not compromised. This includes requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection and firewalls when using mobile equipment. For teleworking, issues like physical security of the teleworking site, remote access to the organization's internal systems, unauthorized access to information from other persons using the accommodation, and security on the home network should be taken into account.

4.3.10 Information Systems Acquisition, Development and Maintenance

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Statements of business requirements for new information systems, or enhancements to existing ones, should specify the requirements for security controls. These requirements should be integrated in the early implementation stages. If products are purchased, a formal testing and acquisition process should be followed and contracts with suppliers should address the identified security requirements.

Controls including the validation of input data, internal processing, message integrity, and output data should be designed into applications to prevent errors, loss, unauthorized modifications or misuse of information. Note that all these controls should be considered, correct input data and internal processes do not guarantee correct output data.

A policy on the use of cryptographic controls to protect the confidentiality, authenticity or integrity of information should be developed and implemented. To support the use of cryptographic techniques, key management should generate cryptographic keys, distribute them in a secure manner and protect them against modification, loss, and destruction.

Changes can imply security weaknesses, and should therefore be controlled by a formal procedure. There should be procedures in place to control the update and installation of software on operational systems, and operational systems should not hold development code or compliers. Test data, that should be used to avoid testing on sensitive information in the operational databases, should be selected carefully, protected and controlled. Testing of new software should be realized in an environment segregated from both the production and development environments, and both project and support environments should be strictly controlled.

To reduce risks resulting from exploitation of published technical vulnerabilities, timely information including the software vendor, version numbers, current state of deployment, and responsible persons should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

4.3.11 Information Security Incident Management

Formal procedures should be established for reporting information security events and observed or suspected security weaknesses as quickly as possible. All employees, contractors, and third party users should be made aware of their responsibility and obligation to report any event or weakness. In high-risk environments, a duress alarm may be provided whereby a person under duress can indicate security events.

Once information security events and weaknesses have been reported, responsibilities and procedures should be in place to handle them. This includes that procedures and management responsibilities should be established to ensure a quick, effective, and orderly response to information security incidents. For this, there is an increasing need to coordinate responses and share information about these incidents with external organizations as appropriate. It also includes that mechanisms to enable the types, volumes, and costs of information security incidents to be quantified and monitored should be in place. The information gained from this evaluation should be used in a process of learning and continual improvement. For cases where a follow-up action against a person or organization after an information security incident involves legal action, internal procedures should be developed and followed to collect, retain, and present evidence, conforming to the rules for evidence laid down in the relevant jurisdiction(s).

4.3.12 Business Continuity Management

An organizational wide business continuity management process should be developed and maintained. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport, and facilities. The process should identify all assets involved in critical business processes as well as all events that can cause interruptions to these processes (e.g. equipment failure, human errors, theft, fire, and natural disasters), assess the risks in terms of likelihood and impact for these business processes, establish business objectives of information processing facilities, consider eventual purchases of insurances and implementations of additional preventive and mitigating controls, assign sufficient resources, and guarantee the safety for personnel, facilities, and properties. Finally, a business continuity plan should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. To ensure that all plans are consistent, and to identify priorities for testing and maintenance, a single framework of business continuity plans should be maintained. Plans and processes should be regularly tested and updated, and responsibility should be assigned.

4.3.13 Compliance

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual obligations. All these obligations, and the organization's approach to meet them, should be explicitly defined, documented, and kept up to date. Areas where it is worth paying extra attention are intellectual property rights (e.g. software and document copyright, design rights, trademarks, patents, and source code licenses), organizational records (e.g. accounting records, database records, transaction logs, and audit logs), data protection and privacy of personal information, and cryptographic controls. Many countries have legislation to protect against computer misuse, and it may be a criminal offence to use a computer for unauthorized purposes. All users should therefore be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorized use.

The security of information systems should be regularly reviewed to ensure that all security procedures are carried out correctly in order to achieve compliance with security policies and standards. If a non-compliance is found, managers should determine the cause of the non-compliance, evaluate the need for, and eventual implement, corrective actions, and review the corrective action taken. Technical compliance checking of the information systems should be done regularly and involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented.

The effectiveness of information systems audit processes should be maximized. For this, audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes. Access to information systems audit tools, e.g. software or data files, should be protected to prevent any possible misuse or compromise.

4.4 Benchmarking of Best ICT Security Specific Practice

4.4.1 Best Device Specific Practice

The National Statistics Office of Sweden (www.scb.se) has accomplished investigations to elucidate how Swedish companies deal with ICT security. Some of the results are compiled in the following. All data is presented in *Appendix*.

The percentage of all Swedish companies with ten or more employees that had invested in different IT security devices in 2005 (the devices in brackets show data from 2004):

- Anti-virus control or other security software	93(±1) %
- Firewalls	87(±2) %
- Data back-up outside operational environment	61(±2) %
- Servers with secure connections	53(±2) %
- (Identification systems)	48(±2) %
- (Cryptography of data)	22(±2) %

The same statistics but for companies with 200-499 employees:

- Anti-virus control or other security software	99(±1) %
- Firewalls	99(±1) %
- Data back-up outside operational environment	79(±2) %
- Servers with secure connections	78(±2) %
- (Identification systems)	71(±2) %
- (Cryptography of data)	62(±2) %

The same statistics but for companies with 500 employees or more:

- Anti-virus control or other security software	100(±0) %
- Firewalls	100(±0) %
- Servers with secure connections	89(±2) %
- (Identification systems)	82(±3) %
- Data back-up outside operational environment	81(±3) %
- (Cryptography of data)	70(±3) %

Statistics from the National Statistics Office of Sweden also show that a majority of all Swedish companies with more than 200 employees have outsourced all or parts of their IT operations (see *Appendix*).

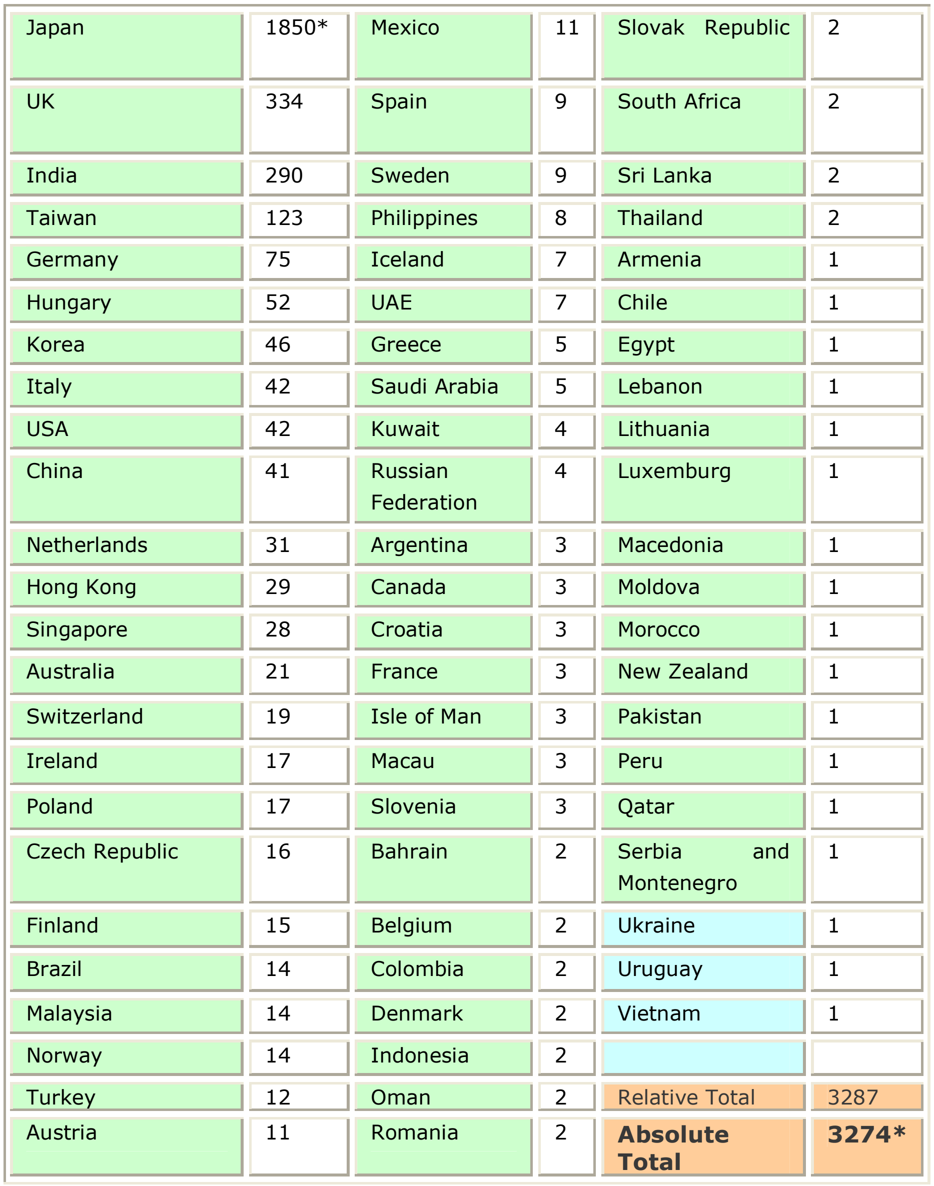
According to an article by Carl Grape on the Internet news portal idg.se (2006), analysts in general consider that protection of mobile units and identity management are the most important security issues for the moment. According to identification systems, Marie Alpman writes in Ny Teknik (2006) that the use of biometry is increasing, but that there are still too many errors to use it for example in big offices. She writes in the same article that perhaps the strongest trend in security is an increasing use of video surveillance. Walter Fumy, vice president of Security and Technology at the division of Communications in Siemens, writes in UNE (2006) that cryptography is one of the most important tools for ICT security, and he continues that the efficiency depends on factors such as the size of the key, the design of the protocol, implementation aspects, and password management.

An article in Computer Sweden (2006) presents an interview with a security consultant working with physical information security. He says that most companies have done a good job restricting the access to the data centres, i.e. systems to stop unauthorized persons from entering and to trace who has been in the data centre. However, he continues that it is often too easy to get access to secret information in other ways, for example via a network. To stop this, it is important to restrict the access to the entire office building, using gates and access cards. Employees working from outside the office should only have access to parts of the information, and all employees should be trained in being observant of unknown persons in the office. A data centre is, according to the Internet encyclopaedia Wikipedia, a facility used to house mission critical computer systems. It generally includes environmental controls, redundant/back-up power supplies, redundant data communications connections, and high security.

Many organizations are using data centres to get a protection as complete as possible against security related threats. New technology makes the data centres cheaper to operate and easier to administrate. Two current trends are that many small data centres are merged to a few big ones serving local offices all over the world, and that higher security requirements make that more organizations have at least two data centres with a long distance in between (Åsblom, 2006). Mats Lövgren has been writing about data centres in Nätverk & Kommunikation (2006). He writes that analysis companies predict physical as well as economical problems for the data centres. According to Gartner, in 2009 70 % of all data centres will not fulfil operational and capacity demands without some kind of renovation, extension or relocation. IDC predicts that already next year the costs of power and cooling will exceed the costs of hardware. He writes further that the technology that really will change the rules for the data centres is virtualization. Virtualization means that one single physical server works as if it was several servers. This saves space in the data centre, reduces the need of personnel, and decreases the consumption of electricity. According to the articles, 76 % of all companies are already using virtual servers, or are planning to do it.

4.4.2 To what Extent do Organizations become ISO/IEC 27001:2005 Certified?

The following table shows an international register of ISMS accredited certificates, awarded to organisations that have gone through an accredited certification process in line with the ISMS standard ISO/IEC 27001:2005. The total number of ISO/IEC 27001 certificates was 256 in August 2006, and 669 in January 2007. (www.iso27001certificates.com)



Japan	1850*	Mexico	11	Slovak Republic	2
UK	334	Spain	9	South Africa	2
India	290	Sweden	9	Sri Lanka	2
Taiwan	123	Philippines	8	Thailand	2
Germany	75	Iceland	7	Armenia	1
Hungary	52	UAE	7	Chile	1
Korea	46	Greece	5	Egypt	1
Italy	42	Saudi Arabia	5	Lebanon	1
USA	42	Kuwait	4	Lithuania	1
China	41	Russian Federation	4	Luxemburg	1
Netherlands	31	Argentina	3	Macedonia	1
Hong Kong	29	Canada	3	Moldova	1
Singapore	28	Croatia	3	Morocco	1
Australia	21	France	3	New Zealand	1
Switzerland	19	Isle of Man	3	Pakistan	1
Ireland	17	Macau	3	Peru	1
Poland	17	Slovenia	3	Qatar	1
Czech Republic	16	Bahrain	2	Serbia and Montenegro	1
Finland	15	Belgium	2	Ukraine	1
Brazil	14	Colombia	2	Uruguay	1
Malaysia	14	Denmark	2	Vietnam	1
Norway	14	Indonesia	2		
Turkey	12	Oman	2	Relative Total	3287
Austria	11	Romania	2	**Absolute Total**	**3274***

*Figure 8. Statistics presented in January 2007. The Absolute Total represents the actual number of certificates. The Relative Total reflects certificates that represent multi-national registrations or are dual-certifications. * includes the number of ISMS certificates in Japan only available in Japanese.*

The nine ISMS accredited certificates in Spain belong to the following organizations:

Organization	*Industry*
Axalto Barcelona	ICT
Bankinter, S.A.	Finance
Caja Madrid	Finance
Ericsson España, S.A.	ICT
Izenpe, S.A.	Certifications
Nextel, S.A.	ICT
Oficina de Armonización del Mercado Interior	Administration
T-Systems ITC Services, S.A.U.	ICT
Verio Europe	ICT

The nine ISMS accredited certificates in Sweden belong to the following organizations:

Organization	*Industry*
Bofors Defence AB	Defence
C2 Management AB	ICT and Consult.
CMA Small Systems AB (two cert.)	ICT
GESAB Engineering AB	Technology Consult.
Posten Sverige AB Corporate Security Group	Post Services
Primärvården Falkenberg et al.	Medical Services
TietoEnator oy, Processing and Networks	ICT
YIT Building Systems Facilities Management	Administration

Figure 9. All the ISMS accredited certificates in Spain and Sweden.

4.4.3 Trends and the Current Debate

Andersson and Mollayani (2006) write in their thesis work that many companies create their own customized systems for information security, which are built upon for example ISO/IEC 27000 or other standards, and that they do not consider there is a need to become certified. They add that companies offering IT solutions are more inclined to become certified. However, it is seldom an entire company becomes certified. More often, the companies choose to certify parts of their business. An article written by Johan Cooke in the Swedish newspaper Computer Sweden (2006) points in the same direction. The article says that many Swedish companies follow ISO/IEC 27000 in principle, but without taking the last step to become certified. It says further that the interest for information security increases heavily among Swedish companies, but as ISO/IEC 27000 is a relatively new standard, it is still to early to tell if it will have an upswing.

Andersson and Mollayani (2006) present a study of the principal reasons to become certified, realized in 2002 by Ezingeard and Birchall among 18 British companies certified with BS 7799, the precursor of ISO/IEC 27001:2005. The principal reasons are, according to this study, the following:

- Competitive advantage
- Facilitation of external relations as well as internal communication

The principal findings made by Andersson and Mollayani (2006) among Swedish companies are that the principal reasons not to become certified are that the organizations do not see any surplus value in becoming certified, principally for two reasons:

- There is no customer demand for a certification. Thus, a certification does not give any important competitive advantage.
- A certification does not imply a motivated augmentation of the security. The security is already considered high enough and the investments will not be paid back.

Moreover, many companies find a certification process too hard and costly, and also the organizational culture and the level of acceptance among management and employees may be an obstacle. The differences between the study made by Ezingeard and Birchall and the one made by Andersson and Mollayani should be accentuated. The former includes more companies, and all companies are certified. The companies in the latter are not certified. Moreover, the studies are realized in different countries, and during different years.

Johan Cooke writes in Computer Sweden (2006) that companies have two principal reasons to become certified. The first is to show current and potential customers, suppliers, and partners that the company is able to handle their information in a secure way. The second is internal benefits.

SWEDAC, the Swedish authority whose principal assignment is to act as the national body for accreditation says, according to Andersson and Mollayani

(2006), that the most common incentive to introduce ISO/IEC 17799:2005 without the aim to become certified is to get operation controls in a good order. SWEDAC continues that if the company already has a well-working management system for quality and environment, it is very good to implement the information security as well. SWEDAC also says that Sweden not is best practice when treating ISO/IEC 17799:2005. The reason is that not the right people are building these systems in Sweden. It is often IT consultants and not management consultants. This is because ISO/IEC 17799:2005 is seen as a standard regulating ICT, but it is much more about it than that. Information security is on a higher level and the most difficult part is often the administrative one.

Andersson and Mollayani (2006) writes that more and more regulations are set up by the EU, authorities and purchasing organisations, in order to secure the treatment of information. Today, there are laws regulating ISO/IEC 17799:2005 within a limited number of fields but that number may augment in the future. This is underlined by Johan Cooke in Computer Sweden (2006), who writes that the law makes higher and higher demands on information security and at the same time accountants, and to some extent even customers, call for higher security levels.

The analysis company Gartner and Swedish security expertise think, according to an article by Björn Norberg in the Swedish newspaper Ny Teknik (2004), that it is important that IT security is seen as a strategic issue handled by CEO and the board of directors, and that this would give better security to a smaller cost. The article says further that physical security and internal control on one hand, and IT and IT security on the other, often are segregated to the disadvantage of security. It also says that there is often an overconfidence in technical solutions, and that 80 % of the security incidents in Sweden in 2003 were caused by internal errors or incorrectly handling, and not by external attacks.

A panel debate invited by Microsoft concluded the following points as crucial for better information security (Eriksson, 2006):

- Increased awareness among users and managers
- Improved handling of documents
- Diminish the gap between technology and management
- Show the product's security related costs more clear
- Better follow-up to show which security measures that give result
- Better measurements of the probability of different threats

A study realized in nine countries by the company Burson-Marsteller found that technology and IT security are the most important questions for company executives. (Jerräng, 2006)

Hans Peterson, Chief Security Officer (CSO) at the insurance and finance company Skandia, says that the biggest problem for information security is social engineering, i.e. someone uses lies to get information or employees are unreliable and spread the information deliberately. Another problem is, according to Hans Peterson, that employees lack a sufficient understanding about what information security really is. He says that negligence and ignorance are bigger problems than external threats. (Eriksson, 2006)

Human Firewall Council, and organization aiming to improve the working methods for information security, says according to the Internet portal Säkerhetscentret.se (2004) that it is important to make an inventory of what should be protected and against what before designing the security system. They also emphasize the need of education. Amutio, López, and Marcelo write in UNE (2006) that to be able to manage the security systems, it is necessary to understand the risks and how good they are.

Finally it can be stated that there are a lot of articles about ICT security in the trade press. This indicates that there is a big interest for these topics. As an example has IDG, the world's largest media company within IT, technology, and business, started two new information channels dedicated for information and ICT security: the newspaper CSO Sweden, and the web site Säkerhetscentret.se. There are not many articles about ISO/IEC 27000, but the discussions are primarily focused on other measures than the technical. This is in line with, and supports the implementation of, ISO/IEC 27000.

5 COMPARING ISO/IEC 27000 WITH BEST PRACTICE

5.1 *Introduction*

The chapter contains comparisons between ISO/IEC 27000 on one hand, and Best Organizational Practice, represented by Matheson's and Matheson's theory of the Smart Organization (1998), and Best ICT Security Specific Practice, represented by the benchmarking study, on the other hand. The comparison with Best Organizational Practice is done on the basis of ISO/IEC 27001:2005, because this is the part of the ISO/IEC 27000 family that contains processes how to conduct the ICT security work. Each part of ISO/IEC 27001:2005 is compared with the principles of the Smart Organization. The comparison with Best ICT Security Specific Practice is done on the basis of the trends found in the benchmarking study; does ISO/IEC 27000 advocate the same processes and controls as the current debate?

5.2 *Comparison to Best Organizational Practice*

The core of any kind of security system is to deal with calculated uncertainties. The implementation of a security system means that the uncertainty is not denied, but managed and communicated and hence Embraced in accordance with the principles of the Smart Organization. Matheson and Matheson write (1998, page 154) that ”good companies have well-honed processes for just about everything they do”. ISO/IEC 27001:2005 presents a process approach for the implementation of an Information Security Management Systems (ISMS). The processes are structured with the “Plan-Do-Check-Act” (PDCA) model. This model forms a circle symbolizing continual improvement in a way comparable to the Decision Quality Chain.

The process approach on which ISO/IEC 27001:2005 is based should be realized within the context of the risks the organization faces, and the PDCA model takes inputs from interested parties. This should be compared with the principle Outside-In Strategic Perspective, which says that important strategic decisions should begin by understanding the broad territory in which the organization operates, i.e. its context. The core of all activities, according to the principle of

Outside-In Strategic Perspective, must be a knowledge about what customers want and need.

The customers of ACT Systems are not the same as the end-users of the services supplied by ACT Systems' clients. There may therefore be different demands at different stages in the value system. For example, demands from end-users can affect demands from service providers and so on. The principle Systems Thinking accentuates the importance to understand different cause-and-effect relationships.

The Appropriate Frame, starting the quality decision process presented as best practice for the Smart Organization, forms the background, setting, and context for the decision. It helps the company to solve the right problem. The process approach on which ISO/IEC 27001:2005 is based shall be realized within the context of the organization's overall business activities and the risks it faces. Establishing the ISMS, the first part in the PDCA model, is about understanding the organization's information security requirements, and defining the scope, boundaries, and policy, i.e. setting the appropriate frame.

When establishing the ISMS, the risks must be identified, as well as the impacts that losses of confidentiality, integrity, and availability may have. The core of the principle of Systems Thinking is to understand cause-and-effect relationships, i.e. what impacts different events may have. When the risks are identified, the risk levels must be estimated by assessing the impacts that may result from security failures and the realistic likelihood of each failure. These estimates are in accordance with the disciplined process of the Decision Quality Chain. The process of establishing the ISMS described in ISO/IEC 27001:2005 also includes to identify and evaluate options for the treatment of risks. Both Nine Principles of a Smart Organization and the Decision Quality Chain point at the importance of creating alternatives.

The processes for implementing and operating the ISMS have no directly corresponding principles describing the Smart Organization. However, the processes are not in opposition to the theory of the Smart Organization. The process of operating the ISMS includes to define how to measure the effectiveness of selected controls and the Decision Quality Chain accentuates the importance of reaching a conclusion based on evidence. ISO/IEC 27001:2005 also states that the operation process must include training and awareness programs. The principle of Continual Learning says that in the Smart

Organization, personnel and resources are available for learning and experimentation.

Findings from monitoring and reviewing activities shall be used to continually improve the effectiveness of the organization's ISMS. One of the principles is Continual Learning, and in the Smart Organization bad news are used to initiate improvements. The Decision Quality Chain points at the importance of collecting Meaningful, Reliable Information. In accordance with the principle of Outside-In Strategic Perspective, ISO/IEC 27001:2005 states that the organization also should apply lessons learnt from security experiences of other organizations.

ISO/IEC 27001:2005 states that management commitment includes communicating the importance of meeting information security objectives and conforming to the information security policy, and the need of continual improvement. This aims to ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives. The principle of Alignment and Empowerment says that everyone in the organization must be aligned around common goals, and the Decision Quality Chain says that the full commitment from all involved people is needed in order to get a successful implementation.

There are also two aspects where ISO/IEC 27001:2005 is in opposite to the theory of the Smart Organization. Firstly, the standard says that the organization shall communicate actions and improvements to all *interested* parties. According to the principle of Open Information Flow, *everyone* needs open access to the information. The second difference is that ISO/IEC 27001:2005 describes that management approval and authorization must be obtained as the last point when establishing the ISMS. The principle of Disciplined Decision Making says that in the Smart Organization, top executives participate already from the beginning of a new project, and continue to participate at important stages of the process.

Also the really core of ISO/IEC 27001:2005, i.e. to protect information, differs from the theory of the Smart Organization. The principle Open Information Flow says that the Smart Organization creates open and virtually unrestricted information flows, even across functional boundaries. The principle also says that there is a risk that the protection of information destroys more value in terms of poor decision making that it creates by the benefits of secrecy.

5.3 Comparison to Best ICT Security Specific Practice

All information from the benchmarking study has been compiled into 21 different processes and controls identified as best practice. These have been compared with ISO/IEC 27000, according to the following list. In the remaining part of this chapter, the numbers in brackets refer to the corresponding chapter in this master thesis. The following controls have been identified:

- *Anti-virus and other security software:* Treated in ISO/IEC 17799:2005 chapter 10.4 "Protection against malicious and mobile code" (4.3.8).
- *Firewalls:* Mentioned at various places in ISO/IEC 17799:2005, for example in chapter 10.6 "Network security management" and chapter 11.4 "Network access control" (4.3.9).
- *Data back-up outside operational environment:* Mainly treated in ISO/IEC 17799:2005 chapter 10.5 "Back-up" (4.3.8). The standard also states that the back-ups should be stored in a remote location.
- *Servers with secure connections:* ISO/IEC 17799:2005 never uses the term servers with secure connections, but the standard recommends on various places controls both for log-on and for software entering the network.
- *Identification systems:* Treated in ISO/IEC 17799:2005 chapter 11.2 "User access management" (4.3.9). The standard mentions biometry as an alternative to passwords, but in the benchmarking study biometry is found too unreliable to use in for example big offices.
- *Cryptography:* Cryptographic controls are mentioned several times in ISO/IEC 17799:2005, but are principally treated in chapter 12.3 "Cryptographic controls" (4.3.10). For a good efficiency, the benchmark has found factors such as the size of the key, the design of the protocol, implementation aspects, and password management. All these factors are considered by ISO/IEC 17799:2005 chapter 12.3.
- *Video surveillance:* Even if video is not mentioned, ISO/IEC 17799:2005 chapter 9.1 "Secure areas" (4.3.7) contains several monitoring controls where video surveillance should be considered.
- *Physical information security:* Access control to buildings using gates and access cards is an important issue in the current debate. This is covered by ISO/IEC 17799:2005 chapter 9.1 "Secure areas". Data centres, i.e. facilities to house mission critical computer systems, are not mentioned in ISO/IEC 27000. However, chapter 9 "Physical and environmental security" can be considered as a description of a data

centre. ISO/IEC 27000 does not say anything about the problem with a high energy consumption in the data centres.

The following processes have been identified:

- *Protection of mobile units:* Different aspects of this issue are treated at different places in ISO/IEC 17799:2005. Chapter 7.1 "Responsibility of assets" (4.3.5) treats asset inventories, chapter 9.2 "Equipment security" (4.3.7) treats the use of equipment off-site, chapter 10.8 "Exchange of information" (4.3.8) treats media during transportation, and chapter 11.7 "Mobile computing and teleworking" (4.3.9) is self explaining.
- *ICT security should be seen as a strategic issue handled by CEO and the board of directors:* Treated in ISO/IEC 17799:2005 chapter 6.1 "Internal organization" (4.3.4). This chapter treats management commitment, and says that management responsibilities could be handled by a dedicated management forum or an existing management body, such as the board of directors. However, the standard does not accentuate the level of the management in the same way as the expertise in the benchmarking study. Also ISO/IEC 27001:2005 chapter 5.1 (4.2.4) treats management commitment, but without mentioning anything about appropriate level of management.
- *Physical security, internal control, and ICT security should be seen as one single issue:* Covered by ISO/IEC 27000, as all these aspects are treated in the same ISMS.
- *There is often an overconfidence in technical solutions. The gap between management and technology should be diminished:* This point is in the really core of the ISMS, where ICT security is treated with a process approach.
- *Increased awareness among users and managers:* Covered by ISO/IEC 27001:2005 chapter 5.2.2 "Training, awareness and competence" (4.2.4).
- *Improved handling of documents:* Covered by ISO/IEC 17799:2005 chapter 7 "Asset management" (4.3.5).
- *Show the products' security related costs more clear:* Not covered by ISO/IEC 27000.
- *Better follow-up to show which security measures that give result:* Covered by ISO/IEC 27001:2005 chapter 4.2.3 "Monitor and review the ISMS" (4.2.3).
- *Better measurements of the probability of different threats:* Mentioned in ISO/IEC 17799:2005 chapter 4.1 "Assessing security risks" (4.3.2), but without detailed instructions. Will eventually be treated in the not yet

published standard ISO/IEC 27005 “Information security risk management”.

- *To obstruct social engineering:* One part of this is covered by ISO/IEC 27001:2005 chapter 5 “Management responsibility” (4.2.4). Another part is covered by ISO/IEC 17799:2005 chapter 10.1.3 “Segregation of duties” (4.3.8), and to some extent by ISO/IEC 17799:2005 chapter 8.3 “Termination or change of employment” (4.3.6).
- *To make an inventory of what should be protected before designing the security system:* Covered by ISO/IEC 17799:2005 chapter 7 “Asset management” (4.3.5).
- *To understand the risks and how good the security systems are:* ISO/IEC 27001:2005 chapter 4.2.1 “Establish the ISMS” contains for example identification, analysis, and evaluation of risks. ISO/IEC 27001:2005 chapter 4.2.3 “Monitor and review the ISMS” contains for example measurements of the effectiveness of controls (4.2.3).
- *Outsourcing of IT operations:* This is neither supported by, nor in contrary to, ISO/IEC 27000. ISO/IEC 27000 does not treat outsourcing explicitly, but states that outsourced activities should be supervised and monitored.

The only finding that is in contrary to an overall augmentation of ICT security and to ISO/IEC 27000 is the use of data back-up outside operational environment among the generally best protected companies, that is non-increasing or even slightly diminishing.

The thesis work presented by Andersson and Mollayani (2006) only considers ISO/IEC 17799:2005, and not ISO/IEC 27001:2005. It expresses the opinion that a certification process is too hard, and also that information and ICT security often is seen as a technical problem, while it should be seen as an administrative problem. Today, ISO/IEC 27001:2005 is developed to take care of these aspects.

6 ANALYSIS

6.1 Introduction

The preceding chapter presents the comparisons between ISO/IEC 27000 and best practice. In this chapter, these comparisons are analysed. Analysed is also the results from the benchmarking of the current debate, as well as whether ISO/IEC 27000 supports ACT Systems' technology strategy.

6.2 Analysis of the Conformity to Best Organizational Practice

The processes in ISO/IEC 27001:2005 support the following principles of the Smart Organization:

- Continual Learning
- Creating Alternatives
- Alignment and Empowerment
- Outside-In Strategic Perspective
- Embracing Uncertainty
- Systems Thinking

They also support the following links in the Decision Quality Chain:

- Appropriate Frame
- Creative, Doable Alternatives
- Meaningful, Reliable Information
- Commitment to Action

The most important contribution from ISO/IEC 27001:2005 in order to become a smart organization lies within Embracing Uncertainty, because the core of ISO/IEC 27000 is to deal with, and communicate, uncertainties in terms of risk.

The principle Value Creation Culture is missing in the list above. However, if it is considered that a certification for ISO/IEC 27001:2005 creates customer value, also this principle is supported by the standard.

Another principle missing above is Disciplined Decision Making. If certain minor adjustments of ISO/IEC 27001:2005 are realized, the standard is at least not contradictive to this principle. However, the processes presented in ISO/IEC 27001:2005 support the identification of important decisions.

The principle which causes the most difficulty in relation to ISO/IEC 27000 is Open Information Flow. The purpose of ISO/IEC 27000 is to protect information, and it is often stated in the standard that access to information should be restricted. In contrary, the principle Open Information Flow says that it should be a free flow of information even across organizational boundaries, and that secrecy policies often destroy more value than they create. However, both ISO/IEC 27000 and the principle Open Information Flow say that it should be evaluated what information that should be protected. If this is done with great accuracy, with both the standard and the principle in mind, ISO/IEC 27000 and the principle Open Information Flow can cooperate instead of counteract each other.

6.3 Analysis of the Conformity to Best ICT Security Specific Practice

An analysis of the results from the benchmarking of best practice on a device specific level among Swedish companies shows that the general trend in Sweden is that the need for ICT security devices is increasing. This is valid for companies in all industrial sectors and of all sizes. The analysis also shows that anti-virus and firewalls are the most commonly used devices for ICT security in all industrial sectors and among companies of all sizes. It has also been seen that a large majority of all Swedish companies with more than 200 employees have invested in anti-virus controls or other security software, firewalls, data back-up outside operational environment, servers with secure connections, identification systems, and cryptography of data. A majority of all Swedish companies with more than 200 employees have outsourced all or parts of their ICT operations. The most surprising is that the generally best protected companies show a noticeable weak augmentation in their use of data back-up outside operational environment. To this, it can be added that the use of all kinds of security devices in all industrial sectors and among companies of all sizes is augmenting with one single exception: data back-up outside operational environment among companies with more than 500 employees, a group of companies generally well protected. Still, 81 % of these companies use data back-up outside operational environment today.

The general trend, both in the statistics and in the verdicts from experts, is that the use of ICT security is increasing, which means that the importance of ICT security is increasing. This means eventually that the importance of information security standards, like ISO/IEC 27000, will increase. This is supported by the fact that during the period for the realization of this project, the number of ISO/IEC 27001:2005 certificates worldwide increased with 161 %. However, more than a year after the introduction of ISO/IEC 27001:2005 there are still only 669 certificates issued all over the world. This is very few, even if most of them are ICT companies like ACT Systems. Half of all ISMS accredited certificates in Sweden and Spain are held by ICT companies. It should also be taken into account that for example in Sweden, the press release announcing the new standard was not published until the middle of February 2006. This implies that the standard practically speaking is from the first quarter of 2006, and not from the fourth quarter of 2005 as the notation of the standard indicates.

The benchmarking study shows three common alternatives for the use of ISO/IEC 27000:

- Certify the entire organization
- Certify parts of the organization, e.g. a certain activity or service
- Use ISO/IEC 27000, to a smaller or bigger extent, as a reference for the work with information security, without seeking accreditation

According to the benchmarking study, see chapter 4.4.3, the most important questions to ask are (1) whether a certification will give competitive advantage, i.e. if the customers will demand it, and (2) to what degree a certification will increase the organization's information security, i.e. if the investment will pay back in terms of smaller problem related costs. These are the most important arguments both from companies that have decided to become certified and from those whom have decided not to.

The compilation of the benchmarking study contains 21 processes and controls, of which 17 (or 81 %) are covered by ISO/IEC 27000. The probably most emphasized single practice in the current debate is to not have overconfidence in technical solutions. This is exactly what ISO/IEC 27000 helps the organizations to prevent. Something of current interest for ACT Systems is data centres, i.e. facilities used to house mission critical computer systems. The term data centre is not mentioned in ISO/IEC 27000, but data centres still have a detailed description.

There are some important aspects that have been found in the benchmarking study that is missing in ISO/IEC 27000. The aspects have been equally emphasized:

- The standard says nothing about controls to diminish the energy consumption in the data centres. This is a prominent topic in the debate. However, this is maybe not an ICT security topic, and thus it maybe should not be treated by the standard.
- Expertise emphasizes that CEO and the board of directors should be involved in the ICT security process. ISO/IEC 27000 emphasizes management commitment, but without accentuating any specific level of management.
- ISO/IEC 27000 contains no instructions about how risk can be measured. However, it is probable that this will be covered by the not yet published standard ISO/IEC 27005 "Information Security Risk Management".

If all findings from the benchmark and analysis of Best ICT Security Specific Practice are compiled, many findings support a certification of ISO/IEC 27000, but there are also findings that make it more doubtful whether or not ACT Systems should become certified. The major findings that support a certification are the following, presented without any particular order:

- ISO/IEC 27000 contains a great majority of all processes and controls found in the benchmarking study. Among them is the most accentuated practice, i.e. not having overconfidence in technical solutions. ISO/IEC 27000 can therefore be considered to represent Best ICT Security Specific Practice.
- The interest for ICT security is increasing, and more legislations and regulations are to be expected. ACT Systems wants to develop its business abroad, and an international standard may be advantageous in order to deal with different legislations in different countries.
- Many organizations use ISO/IEC 27000 as a reference without becoming certified. This means that the standard is more widespread than the statistics shows. That many companies use the standard without trying to get a certification means that they use the standard principally to improve their ICT security.

- Because ACT Systems already has both ISO 9001:2000 and ISO 14001:2004 certifications, an implementation and certification of ISO/IEC 27001:2005 should go relatively smooth and easy.
- In southern Spain, where ACT Systems has its main business, consultancy companies promote ISO/IEC 27000 and they give beneficial offers to conduct the implementation of the standard. They do this with the hope to create a critical mass of certified organizations. If their venture succeed, ISO/IEC 27000 will eventually become a threshold capability. The companies that become certified now have the opportunity to gain first mover advantages.

The major finding that supports not to become certified is that ISO/IEC 27000 is neither widespread nor very salient in the current debate.

6.4 Analysis of the Conformity to ACT Systems' Technology Strategy

The core in the technology strategy of ACT Systems is the disposal and management of data centres, both for internal use and for outsourcing, housing, and hosting to third parties. A data centre is a facility used to house mission critical computer systems. ISO/IEC 17799:2005 chapter 9 "Physical and environmental security" (chapter 4.3.7 in this master thesis) gives an extensive description of data centres. This description is in line with what has been found as being best practice, according to the analysis in chapter 6.2. For the outsourcing, housing, and hosting services, an information security certificate seems important as these services include the management of parts of the information security for the companies using the service. Also the information systems part of the company's technology strategy is supported by ISO/IEC 27000. This implies that ISO/IEC 27000 supports the internal processes of ACT Systems' technology strategy.

ACT Systems also hopes that a certificate will give them competitive advantage. But according to the theory of Dodgson (2000), ISO/IEC 27000 has no strategic potential because it is too easily imitable. If ACT Systems becomes certified and it turns out being a success, other organizations will do the same thing. As long as ISO/IEC 27000 is waiting for its breakthrough, it also has strategically equivalent substitutes. This implies that an ISO/IEC 27001:2005 certificate will not give sustainable competitive advantage.

7 CONCLUSIONS

7.1 Introduction

The results from the comparison with Best Organizational Practice and Best ICT Security Specific Practice, as well as the analysis whether ISO/IEC 27000 is in line with and supports the technology strategy of ACT Systems, are in this chapter compiled. The overall contributions to industry and academy are summarized so that the reader see the whole picture.

7.2 Final Conclusions

ISO/IEC 27000 is found to be an important tool in fulfilling the principle of Embracing Uncertainty, and most of the other principles presented by Matheson and Matheson are supported by the standard. The principles that not are directly supported by the standard are not counteracted. Thus, ISO/IEC 27000 represents Best Organizational Practice.

ISO/IEC 27000 comprises Best ICT Security Specific Practice, and the standard supports ACT Systems' technology strategy. However, the idea with ISO/IEC 17799:2005 is to include all controls for an improved ICT security, i.e. the standard comprises best practice but there are also a lot of controls that are not mentioned as best practice. This type of benchmarking can never be comprehensive, and it is quite possible that controls or processes that should have been identified as best practice have not been categorised so. However, the presence of a process or control in the debate increases with its importance and the benchmarking study has been conducted on a wide front. This means that the more salient the control or process is in the debate, the bigger the probability that it has been found by the benchmarking study.

ACT Systems should become certified if ISO/IEC 27000 makes its breakthrough and becomes a threshold capability, or if legislations demand a certification. However, the standard is still waiting for the breakthrough, and it is hard to tell what the future will bring. ICT security is more and more important and there is a big debate going on, but it should be underlined that ISO/IEC 27000 is very sparsely mentioned in this debate. A certification has no strategic potential and will not give sustainable competitive advantage. On the other hand, to become certified now can give first mover advantages.

Finally, the conclusion is that ISO/IEC 27000 is in line with both Best Organizational Practice and Best ICT Security Specific Practice, as well as with ACT Systems' technology strategy. This means that ACT Systems' internal processes will be supported in the best possible way. It is possible that ISO/IEC 27000 will be a threshold capability in the future, but it is less probable that it will give ACT Systems sustainable competitive advantage.

8 RECOMMENDATIONS

8.1 Introduction

With the conclusions from this master thesis in mind, this chapter presents some suggestions for further studies. These suggestions have been addressed to ACT Systems and to the academy. Suggestions for the academy can be addressed by future thesis works.

8.2 Recommendations for ACT Systems

Managers at ACT Systems consider that the company would gain benefits from a certification, but according to the theories of Dodgson (2000) a certification will not give sustainable competitive advantage. The most important recommendation to ACT Systems is to conduct a customer analysis. When doing this, it is important to not only look at current customers, but also at new potential customers. This is the most important recommendation because everything ACT Systems does, it does for its customers. The main purpose with this study would be to determine the probability that ISO/IEC 27000 will become a threshold capability.

If the European Union or the Spanish government legislates in the area of information and ICT security, a certification like ISO/IEC 27001:2005 may be necessary. Another recommendation is therefore to try to forecast future legislations as this can give valuable knowledge.

8.3 Recommendations for the Academy

Two interesting benchmarking studies that are different from the one conducted in this master thesis are recommended. In the first one, a more profound study of some of the ISMS certificated organizations presented on www.iso27001certificates.com could be conducted. It is also recommended to compare some of these companies with companies that not have chosen to become certified. The other recommended benchmarking study starts with a profound investigation to distinguish a few companies that have an excellent ICT security. A more focused benchmarking could after that be conducted on these companies.

In this master thesis, the theory of the Smart Organization has been used as best theoretical practice. Are there other theories that could serve as best practice? How does ISO/IEC 27000 support these theories?

9 CRITIQUE

9.1 Introduction

This chapter is a self evaluation of the master thesis, aiming to throw light upon the methodology and project realization.

9.2 Self Evaluation

The benchmarking conducted in this master thesis takes a general point of view. If more time had been at the project's disposal, it could have been investigated which specific companies that actually represent best practice followed by a deeper analysis of some of these. Alternatively, as a complement to the study of secondary data an extensive survey could have been conducted.

The Decision Quality Chain describes best practice for decision making, and is therefore not optimal to compare with ISO/IEC 27000 in order to evaluate Best Organizational Practice. However, the main analysis is based on the Nine Principles of a Smart Organization. The Decision Quality Chain is included mainly for its first link, i.e. Appropriate Frame.

This method to compare ISO/IEC 27000 with best practice must be seen as a complement, and not a replacement, to a market analysis. However, the master thesis is conducted with the reservation that there is a certain demand from customers.

REFERENCES

Standards

ISO/IEC 17799:2005 (2005). Geneva, ISO/IEC

ISO/IEC 27001:2005 (2005). Geneva, ISO/IEC

Literature

Andersson, Bengt; Mollayani, Anoshe (2006): *Motiv och drivkrafter för certifiering mot ISO 17799*. Thesis work at the Department of Computer and System Sciences, Stockholm University/Royal Institute of Technology.

Dodgson, Mark (2000): *The Management of Technological Innovation: An International and Strategic Approach*. Oxford, Oxford University Press.

Johnson, Gerry; Scholes, Kevan; Whittington, Richard (2005): *Exploring Corporate Strategy, 7th Edition*. Harlow, Pearson Education Limited.

Matheson, David; Matheson, Jim (1998): *The Smart Organization: Creating Value through Strategic R&D*. Boston, Harvard Business School Press.

Articles

Alpman, Marie (2006): Video ersätter väktare. In: *Ny Teknik*. Internet: www.nyteknik.se/art/45986 (Oct 19 2006)

Amutio Gómez, Miguel A.; López Crespo, Francisco; Marcelo Cocho, Julián (2006): La gestión de los riesgos de tecnologías de la información. In: *UNE (magazine of AENOR)*. Issue 203, February 2006. p 27-29.

Cooke, Johan (2006): Svenska företag går inte hela vägen – Säkerhetsfrågan splittrad. In: *Computer Sweden*. Internet: www.idg.se/2.1085/1.80117 (Dec 21 2006)

Cooke, Johan (2006): Våg av nya regler. In: *Computer Sweden*. Internet: www.idg.se/2.1085/1.80118 (Nov 14 2006)

Eriksson, Ola (2006): Användarna största säkerhetshotet. In: *Computer Sweden*. Internet: www.idg.se/2.1085/1.83410 (Jan 8 2007)

Fumy, Walter (2006): Normas de seguridad para el mundo empresarial actual. In: *UNE (Revista de AENOR)*. Issue 203, February 2006. p 20-22.

Jerräng, Marcus (2006): Tekniken viktig för företagsledare. In: *Computer Sweden*. Internet: www.idg.se/2.1085/1.87703 (Jan 8 2007)

Lövgren, Mats (2006): Företag har svårt att beräkna besparingseffekterna av virtualisering. In: *Nätverk och Kommunikation*. Internet: http://nok.idg.se/2.1046/1.77099 (Nov 6 2006)

Lövgren, Mats (2006): Joe Tucci: Virtualisering kommer att förändra spelreglerna för datacentren. In: *Nätverk & Kommunikation*. Internet: http://nok.idg.se/2.1046/1.64676 (Nov 6 2006)

Lövgren, Mats (2006): Sun levererar datacenter på burk. In: *Nätverk & Kommunikation*. Internet: www.idg.se/2.1085/1.79237 (Nov 6 2006)

Norberg, Björn (2004): IT-säkerhet en ledningsfråga. In: *Ny Teknik*. Internet: www.nyteknik.se/art/37429 (Dec 21 2006)

Unknown author (2006): Fönstret öppet för dataintrång. In: *Computer Sweden*. Internet: www.idg.se/2.1085/1.82987 (Jan 8 2007)

Åsblom, Joel (2006): Trender 2007: Jättehallarna blir färre. In: *Computer* Sweden. Internet: www.idg.se/2.1085/1.89440 (07.01.08)

Internet

12manage.com. An independent Internet based management portal. www.12manage.com/methods_benchmarking.html (Nov 13 2006)

ACT Systems company website. www.actsistemas.es

the Ayesa Group company website. www.grupoayesa.es

Eurostat.
http://epp.eurostat.ec.europa.eu/portal/page?_pageid=1090,30070682,1090_33076576&_dad=portal&_schema=PORTAL (Oct 30 2006)

Gilså, Tomas (2004): Undersökning underkänner infosäkerhet. In: *Säkerhetscentret.se*. Internet: http://sakerhet.idg.se/2.1070/1.70591 (Jan 8 2007)

Grape, Carl (2006): IDG satsar ännu mer på säkerhet. In: *idg.se*. Internet: www.idg.se/2.1085/1.82880 (Jan 8 2007)

the International Electrotechnical Commission organization website. www.iec.ch

the International Register of ISMS Certificates. www.iso27001certificates.com

Nationalencyklopedin.
IT, www.ne.se/jsp/search/article.jsp?i_art_id=214244 (Jan 4 2007)
IT-säkerhet, www.ne.se/jsp/search/article.jsp?i_art_id=676090 (Jan 4 2007)

National Statistics Office of Sweden.
www.ssd.scb.se/databaser/makro/Produkt.asp?produktid=IT0101 (Oct 30 2006)
www.scb.se/templates/tableOrChart____28141.asp (Oct 30 2006)

www.foretagsregistret.scb.se/sni/050829snisorterad.pdf (Nov 7 2006)

OECD organization website. www.oecd.org/sti/ict/broadband (Nov 6 2006)

Swedish Standards Institute – Press Release Feb 14 2006. www.sis.se/upload/632754419654687235.pdf (Nov 15 2006)

Valuebasedmanagement.net. An independent Internet based management portal. www.valuebasedmanagement.net/methods_benchmarking.html (Nov 13 2006)

Wikipedia.org.

Data centre, http://en.wikipedia.org/wiki/Data_centre (Jan 31 2007)

APPENDICES

Benchmarking of the Swedish Market

IT security amongst companies (with 10 or more employees) assorted after kind of security device and company size. (www.ssd.scb.se/databaser/makro/Produkt.asp?produktid=IT0101)

Security device	Kind of company	2003 (%)	2004 (%)	2005 (%)
Firewalls	All companies	69(±2)	82(±2)	87(±2)
	200-499 employees	98(±1)	98(±1)	99(±1)
	500+ employees	98(±1)	99(±1)	100(±0)
Data back-up outside operational environment	All companies	47(±2)	59(±2)	61(±2)
	200-499 employees	73(±2)	76(±2)	79(±2)
	500+ employees	82(±2)	85(±3)	81(±3)
Identification systems	All companies	47(±2)	48(±2)	..
	200-499 employees	66(±2)	71(±2)	..
	500+ employees	80(±3)	82(±3)	..
Cryptography of data	All companies	25(±2)	22(±2)	..
	200-499 employees	63(±2)	62(±2)	..
	500+ employees	72(±3)	70(±3)	..
Servers with secure connections	All companies	43(±2)	49(±2)	53(±2)
	200-499 employees	72(±2)	76(±2)	78(±2)
	500+ employees	82(±3)	88(±3)	89(±2)
Anti-virus control or other	All companies	85(±2)	92(±1)	93(±1)

security software				
	200-499 employees	98(±1)	99(±0)	99(±1)
	500+ employees	97(±1)	100(±0)	100(±0)

In the survey of 2003, it was asked about cryptography to secure confidentiality. 2004, it was asked about cryptography of data. The changed formulation makes the results not directly comparable.

IT security amongst companies (with 10 or more employees) assorted after kind of security device and industrial sector.
(www.ssd.scb.se/databaser/makro/Produkt.asp?produktid=IT0101)

Security device	Industry	2003(%)	2004(%)	2005(%)
Firewalls	Manufacturing industry	68(±4)	82(±3)	88(±3)
	Electricity, gas, heating and water supply	95(±4)	99(±1)	100(±0)
	Construction industry	53(±8)	68(±7)	80(±7)
	Wholesale and retail trade, reparations, hotels and restaurants	69(±4)	83(±3)	87(±3)
	Transportations and Storage companies, Travel agencies, Shipping agents	57(±8)	73(±7)	79(±6)
	Post and telecommunication companies	90(±6)	92(±5)	96(±4)
	Financial institutions and insurance companies	94(±3)	99(±1)	98(±1)
	Real estate, renting and business activities	83(±5)	92(±4)	93(±4)
	Motion picture, video, radio and television businesses and other service businesses	65(±5)	71(±6)	86(±5)
Data back-up outside operational environment	Manufacturing industry	45(±4)	61(±4)	63(±4)
	Electricity, gas, heating and water supply	70(±8)	73(±8)	73(±8)

	Construction industry	36(±8)	46(±8)	51(±8)
	Wholesale and retail trade, reparations, hotels and restaurants	47(±4)	58(±4)	62(±4)
	Transportations and Storage companies, Travel agencies, Shipping agents	44(±8)	44(±8)	48(±7)
	Post and telecommunication companies	73(±9)	79(±8)	75(±9)
	Financial institutions and insurance companies	77(±5)	83(±5)	86(±3)
	Real estate, renting and business activities	55(±6)	68(±6)	69(±6)
	Motion picture, video, radio and television businesses and other service businesses	44(±7)	56(±6)	57(±7)
Identification systems	Manufacturing industry	45(±4)	46(±4)	..
	Electricity, gas, heating and water supply	60(±9)	67(±8)	..
	Construction industry	39(±8)	35(±8)	..
	Wholesale and retail trade, reparations, hotels and restaurants	48(±4)	53(±4)	..
	Transportations and Storage companies, Travel agencies, Shipping agents	42(±8)	36(±7)	..
	Post and telecommunication companies	63(±9)	67(±10)	..
	Financial institutions and insurance companies	74(±5)	83(±5)	..
	Real estate, renting and business activities	54(±6)	53(±6)	..
	Motion picture, video, radio and television businesses and other service businesses	42(±7)	48(±6)	..
Cryptography of data	Manufacturing industry	21(±3)	21(±3)	..
	Electricity, gas, heating and	41(±8)	50(±8)	..

	water supply			
	Construction industry	10(±5)	7(±4)	..
	Wholesale and retail trade, reparations, hotels and restaurants	26(±4)	20(±3)	..
	Transportations and Storage companies, Travel agencies, Shipping agents	21(±6)	15(±5)	..
	Post and telecommunication companies	68(±9)	72(±9)	..
	Financial institutions and insurance companies	64(±6)	71(±5)	..
	Real estate, renting and business activities	35(±5)	34(±5)	..
	Motion picture, video, radio and television businesses and other service businesses	31(±6)	22(±5)	..
Servers with secure connections	Manufacturing industry	36(±4)	46(±4)	50(±4)
	Electricity, gas, heating and water supply	50(±8)	70(±8)	70(±8)
	Construction industry	23(±6)	31(±7)	33(±8)
	Wholesale and retail trade, reparations, hotels and restaurants	44(±4)	48(±4)	56(±4)
	Transportations and Storage companies, Travel agencies, Shipping agents	41(±8)	40(±7)	42(±7)
	Post and telecommunication companies	74(±8)	83(±8)	77(±9)
	Financial institutions and insurance companies	74(±5)	86(±4)	79(±4)
	Real estate, renting and business activities	58(±6)	63(±6)	68(±6)
	Motion picture, video, radio and television businesses and other service businesses	40(±7)	53(±6)	47(±6)
Anti-virus control or other security	Manufacturing industry	88(±3)	94(±2)	95(±2)

software				
	Electricity, gas, heating and water supply	96(±3)	99(±1)	100(±)
	Construction industry	84(±6)	93(±4)	93(±4)
	Wholesale and retail trade, reparations, hotels and restaurants	82(±3)	88(±3)	92(±2)
	Transportations and Storage companies, Travel agencies, Shipping agents	74(±7)	85(±6)	85(±6)
	Post and telecommunication companies	90(±6)	92(±5)	96(±4)
	Financial institutions and insurance companies	93(±3)	99(±1)	98(±1)
	Real estate, renting and business activities	93(±3)	96(±3)	96(±3)
	Motion picture, video, radio and television businesses and other service businesses	78(±5)	82(±5)	88(±5)

In the survey of 2003, it was asked about cryptography to secure confidentiality. 2004, it was asked about cryptography of data. The changed formulation makes the results not directly comparable.

Share of companies that have outsourced, i.e. left in a specialist company's hands, all or parts of their IT operations (2005).
(www.scb.se/templates/tableOrChart____28141.asp).

TOTALLY	**35(±2)**
9.2.1 Size of company	
10-19 employees	29(±3)
20-49 employees	38(±4)
50-99 employees	52(±9)
100-199 employees	47(±4)
200-499 employees	52(±3)
500+ employees	69(±3)

A Note on the Different Industries

The different industries are defined by the Swedish standard SNI200, which is built upon the EU standard NACE. In the following, some comments upon the industries included in the statistics are presented, with the focus on the interest of ACT Systems. (www.foretagsregistret.scb.se/sni/050829snisorterad.pdf)

- Construction includes inter alia site preparation, building of complete constructions or parts thereof and building installations including installations of electrical wiring and fittings (but not telecommunication systems). On the other hand, architecture and consultancy are not included.
- Post and telecommunications comprise post and courier activities, including delivery of daily papers and other delivery activities, and telecommunications. Telecommunications include network operations (inter alia Internet access supply, network operator services, operation and maintenance of telecommunication networks and telecommunication services), radio and television broadcasting and cable television operation.
- Real estate, renting and business activities comprise the following parts:
    - Real estate activities
    - Renting of machinery and equipment without operator and of personal and household goods
    - Computer and related activities, including hardware consultancy and software consultancy and supply. This includes development and consultancy of both standardized and customized systems and software. This sector also includes data processing (computer operation, operation and service of computer networks, server operation etc.), data base activities and computer security consultancy.
    - Research and development (R&D)
    - Other business activities. Comprise architectural and engineering activities and related technical consultancy, including construction, consultancy and project management. These activities also comprise legal, accounting and business consultancy, call centre services etc.

Motion picture, video, radio and television activities and other service activities. Other service activities include washing and dry-cleaning of textile and fur products, hairdressing and other beauty treatment, funeral and related activities, physical well-being activities etc.

A Note on the Data

Presented by the National Statistics Office of Sweden in connection with the presentation of the data. The results showed in the table proceed from the investigations “Use of IT in companies 2003” and “Use of IT in companies 2004”, which have been realized by the National Statistics Office of Sweden during the years 2003 and 2004. In these surveys, the selection is a randomly made probability selection. Hence, the percentage numbers shown are estimates marred by uncertainty. The uncertainty is shown as a margin of error, equalling the double standard deviation of the percentage estimate, which depends both on the size of the percentage number and the number of observations made – the more observations, the smaller the confidence interval. The interval formed by the percentage estimation ± the margin of error forms a 95 % confidence interval, i.e. an interval that with a probability of 95 % includes the real value for the population, presupposed that no systematic errors exists. Estimates with a margin of error superior than 10 percentage units are considered too uncertain to be presented and are therefore shown as (..). Also numbers that can not occur, for example questions that have not been asked certain years, are shown with (..).