Formal Information Security Standards in German Medium Enterprises

David Kluge
David.Kluge@liverpool.ac.uk

Samuel Sambasivam
Computer Science Department
Azusa Pacific University
Azusa, CA 91702, USA
ssambasivam@apu.edu

Abstract

During the last ten years, the role of formal information security standards has gained importance. In several ways, they can be helpful in achieving security of business information systems. One of them is the provision of comprehensive collections of evaluation criteria and security measures. Such can be the basis of a holistic security strategy in that they can act as basis for security policies and auditing schemes. Large enterprises appear to have determined security strategies and written security policies as a matter of course and in most cases it can be anticipated that formal standards have been their origin. As for firms from the medium size sector, this is less often the case. This paper deals with the acceptance of formal standards among medium enterprises. We analyze their suitability with respect to company size and discuss typical challenges to their implementation .

Keywords: Information Security, Medium Enterprises, Formal Standards, ISO 27001, Suitability

1. INTRODUCTION

Given the growing dependence of enterprises on their corporate information systems, formal information security (IS) standards have continued to gain attention. Annual security surveys like the Global Information Security Survey by Ernst & Young (2006) demonstrate that their use increased significantly during the last years. According to the survey's results, more than 70% of the interrogated organizations make use of internal audits, and a third of them assessed their information systems against formal standards. This is a significant rise as compared to prior year's results.

There are various arguments suggesting formal standards to be an effective tool to use when starting over to develop a corporate security strategy. One of them is, their potential to aid with defining a consistent understanding of proper security management techniques. They could help to establish rating scales and hence increase the measurability of corporate security (Martins & Eloff 2001).

When it comes to formal information security standards in medium enterprises, still very few is known about their customariness. When comparing the spread of information security standards to the one of quality management (QA) standards by the example of ISO standards, we can find, that the spread of ISO 27000 (IS) is significantly lower than for example the one of ISO 9000 (QA) (ISMS 2008) (ISO 2000). As for the medium enterprises, this picture seems to be even more intense than for the large ones. Different explanations for this can be discussed including a lack of interest or acceptance as well as a minor suitability.

Nevertheless, when dealing with the security of business information systems, the special conditions within the medium enterprise sector should not be missed out. In many European countries, medium enterprises are of special importance to the domestic economy. In Germany for example more than 90% of companies subject to value added tax (VAT) belong to this sector and realize around half of all annual turnovers (ISME 2004).

Barlette and Fomin studied the suitability of formal information security standards for small and medium enterprises based on the existing literature. Since there are very few publications directly addressing this topic, Barlette and Fomin explore the domain of quality assurance standards instead and draw conclusions by analogy. In contrast to their approach we try to answer the adequacy question based on practical experience using the case study methodology.

Barlette and Fomin come to the conclusion, that small and medium enterprises are not capable of adopting formal IS standards at the present time. In our investigation, we go into deeper detail and investigate which kind of standard requirements present themselves as unattainable. This way we pave the foundation for decision making on whether a standard adoption is still beneficial - at least partwise or in a mitigated from.

2. BACKGROUND

2.1 Characteristics of Medium-Sized Companies

When talking about medium enterprises it is vital to find a working definition of how to classify them. Typically, there are two main figures through which medium enterprises are characterized. The number of employees being the first and the annual turnover being the second one. The European Union defines a medium enterprise as a company having 50 to 249 employees and having an annual turnover of between 9 and 50 million Euros. Other institutions like the German Institute for Small and Medium enterprise research use a slightly differing definition however. Aspects like the private ownership and the company's legal status in which the entrepreneur often has individual responsibility for the success and failure of the venture play a role (ISME 2004). We applied a definition similar to that of the Institute for Small and Medium Enterprise research counting all enterprises to the medium size sector which have more than 40 employees and realize a revenue of more than 2 million Euros per year.

2.2 Considered Standards

Several standards and frameworks are available in the field of information security management. Subject to our comparison have been the ISO 27000 family, the Standard of Good Practice (SoGP) by the Information Security Forum and the IT Baseline Protection Manual by the German Federal Office for IT security. The Control Objectives for Information and Related Technology (COBIT) as well as the IT Infrastructure Library (ITIL) are often mentioned in connection with IT security. Though the outcome of their implementation supports a company in establishing secure information systems, their main content deals with different matters, hence they have not been counted as IS standards.

The ISO 27000 standard family clearly plays an outstanding role in this realm. It originates from the standards BS7799 and ISO17799 respectively which are found in older literature likewise, so they sometimes lead to confusion in conceptuality. The standard itself consists of a selection of so called "control objectives" and "controls" each of which belongs to one of 13 sections representing a certain area of interest.

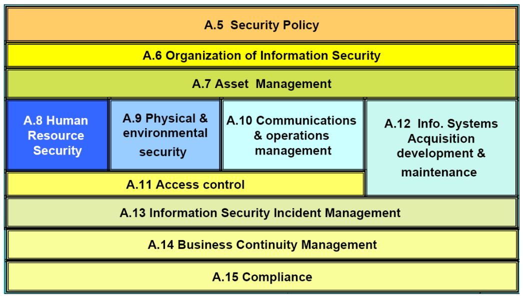

A.5 Security Policy
A.6 Organization of Information Security
A.7 Asset Management
A.8 Human Resource Security
A.9 Physical & environmental security
A.10 Communications & operations management
A.12 Info. Systems Acquisition development & maintenance
A.11 Access control
A.13 Information Security Incident Management
A.14 Business Continuity Management
A.15 Compliance

Figure 1: 11 Security domains of ISO 27001. Source: Ambi (n.d.)

ISO 27001 takes a "process approach" to security . That is, instead of describing security technology it defines operational procedures. These procedures are expected to be filled out with technical measures but the standard itself is not very determined as to which these measures shall be.

IT Baseline Protection is an initiative of the German Federal Office for Information Security. The IT Baseline Protection Manual consists of „standard security safeguards, implementation advice and aids for numerous IT configurations which are typically found in IT systems today (Grundschutz 2004, p.1)." Generally the purpose of this manual is similar to the one of ISO 27000. Nevertheless, IT Baseline protection distances itself from the existing ISO standards arguing that these contained hardly any concrete technical descriptions of how to establish security measures. IT Baseline Protection is an interpretation of ISO 27001 and claims a higher degree of management and regulation. Consequently the Baseline Protection catalogues are comprehensive documents having a high level of detail. Above all they are even product specific and cover tasks like the introduction of specific encryption schemes.

The Standard of Good Practice for Information Security is a work by the Information Security Forum. Its latest version has been released in 2007 which makes it a very current document. It shall provide a „practical basis for assessing an organization's information security arrangements (SOGP 2007, p. 1)". Unlike ISO 27000, the Standard of Good Practice is not that much process focused. It leverages both organizational and technical measures which are concrete to a medium level meaning that they are more detailed than the code of practice corresponding to ISO 27001 but wider than the IT Baseline catalogues. The document reads itself very contiguous and it is a high level definition which is open to all kinds of manufacturers and products but still makes explicit suggestions of implementations and technologies.

The ISO 27000 standard family can be seen to be dominating the "standard-market". It appears to be most often referred to and above all it is the only standard for which a certification can be obtained. All other before mentioned standards including ITIL and COBIT and Grundschutz refer to ISO 27001 when it comes to certification (Szakats 2004) (ISACA 2007) (FOIS 2004).

3. METHODOLOGY

We analyzed the suitability of formal standards with respect to company size by discovering typical challenges to their implementation. To do so, we chose case study research as methodology. Finally we used an online survey to poll key data from further enterprises in order to allow for cross case replication of the case study results.

Without giving a complete content wise comparison, it is evident that the mentioned standards are similar in substance. It was not feasible to conduct a case study on the suitability for each single standard, therefore we chose to focus on ISO 27001. The aforementioned fact, that the remainder of the enumerated standards are also intended to prepare for an ISO certification, implies that they do not reflect a generally different conception of information security management. One might therefore expect, that switching standards will not make a tremendous difference in terms of achievability.

3.1. Case Study

To discover possible difficulties that might hinder medium enterprises adopting ISO 27001, we accompanied a typical representative from that sector in its adoption efforts.

To gather insights, we conducted an on site audit and examined different sources of information from within the company. In common understanding, the goal of an audit is to evaluate an organization which is believed to be standard compliant already. In this picture, an audit is the finalization of an adoption process (NSAA 2001). Our approach was to go the other way around beginning with an initial audit which expects not all evaluated control to be fulfilled. It served as tool for assessing the company's ability to fulfill a control rather than determining the state for now.

The currently existing policies and documentation of company working procedures were evaluated. Additionally, first hand observations at the company's site were considered, which is because for some controls measures could have been de facto present though a documentation isn't present.

By checking these explicitly and implicitly present working procedures, against the standard, its controls could be ranked into three categories

(1) compliant
(2) attainable
(3) not attainable

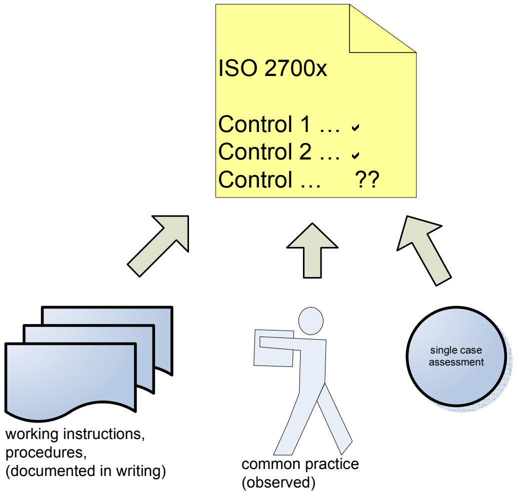

ISO 2700x
Control 1 … ✓
Control 2 … ✓
Control … ??
working instructions, procedures, (documented in writing)
common practice (observed)
single case assessment

Figure 2: Sources of Information

Standard controls ranked in category three are the ones of special importance. As they constitute the obstacles within the adoption process they were discussed further. For this purpose the company's IS management was asked for its assessment of the requirement in question and the outcomes were analyzed for plausibility.

For the sake of simplicity, not applicable controls have been ranked compliant rather than introducing a fourth category such as "N/A". This is because for the company's overall standard implementation capabilities it does not make a difference for which reason the control does not have to be worked on.

3.1.1 Subject of Study

The audited company is a manufacturer of laboratory-equipment and automation systems which realizes an annual turnover of approximately 2.5 million Euros. Altogether there are about 50 employees working in different departments from engineering over software development to product manufacturing.

3.1.2 Formal Case Study Requirements

According to Yin (2003, pp. 33 ff) the quality of a case study can be judged according to four criteria. (1) Construct Validity, (2) Internal Validity, (3) External Validity and (4) Reliability.

Construct Validity is maintained by minimizing investigator subjectivity (Tellis 1997). To achieve the maximum objectivity during a study, a "sufficiently operational set of measures" is put forth on which decisions can be made (Yin 2003, p. 35). Subjective judgments which are rather prone to error should in turn be minimized. In our case the question of whether a certain standard section/control has been fulfilled is an objective one, hence construct validity can be considered to be maintained for these. The question of whether a not fulfilled section/control is attainable is harder to answer. At a first glance, this leaves room for subjectivity. The judgments made were however discussed and a sound justification was sought after.

Internal Validity means that the methodology used produces valid results, which is the case when the studying process draws correct conclusions. This can be at risk if not all evidence is collected and attended to and/or false causal relationships are drawn (Yin 2003, p.36). The study must therefore be complete with regards to the evidence. When it comes to conclusions, explanation building must be done with care and in due consideration of alternative perspectives. Rival explanations need to be constructed to test the findings for their validity. Finally it must be made sure, that the investigation/observation process does not influence the target of observation and therefore does not "measure itself" (Dawson 2005, p.33). In the case under consideration such interferences were unlikely to be on hand because most evidence was collected from written documentation which has been created prior to the auditing process. As for the interview questions such an effect had to be considered since the trial situation could have encouraged the interviewees to answer questions in a slightly different light than how they really are. People's abilities and level of skills as well as intents and levels of awareness are rather subjective values which could be slightly biased. Space for variations has however not been found large enough to significantly influence the findings.

The requirement for *External Validity* refers to the necessity of findings to be valid beyond the investigated case. Findings which hold true in the investigated case should apply to every analogue case. In this connection it must be clearly distinguished between the diff-ferent methodologies that underlie case study and survey research as these are frequently confused. In survey research, findings are generalized from a sample to a larger universe. The underlying principle is statistical generalization. The sample structure is thus decisive for whether the external validity of a survey is maintained. Case studies again rely on analytical generalization and therefore don't constitute a sample which must be picked according to statistical rules (Yin 2003). The generalized findings should however be tested e.g. by replicating them across cases and test for whether they hold true or not. The online survey has in some instances been used to do so. Using a multi method approach, coherences discovered during the study were tested against the survey results to test if the statistical data support the analytically gained findings.

Reliability is the fourth quality criterion of a case study and it is said to be achieved when the investigation process adheres to well documented standards assuring that a later investigator would come to the same conclusions about a case if he followed them. For this purpose Yin (2003, p.37) suggests the usage of a study protocol which beneath an overview over the project contains all procedures carried out as well as the study questions. Since the case study is based on an audit which itself is a well documented process, this requirement is naturally fulfilled.

3.2 Online Survey

The online survey was used to gain empirical data beyond the single case at hand. For this purpose, key business figures and some security relevant details were polled. (See appendix for more details on the survey instrument)

3.2.1 Target Population

The target population of the survey was the entirety of medium sized enterprises preferable with a number of employees between 40 and 100.

To cover all industries alike, we drew a random sample of this population by participants via email and phone. The information base for the invitations has been taken from different sources like yellow pages, the chamber of commerce and trade directories obtained from industrial estates. All respondents participated voluntarily and no inclusion or exclusion criteria were defined.

3.2.2 Structure and Content of the Survey

The survey was divided into three sections (A, B, C). Section A polled general information which allow for a classification according to the number of employees, working domain, annual turnover etc. and could be used for sample stratification. Section B polled framework conditions of the company. As opposed to section A, it did however focus more on the inner structure and workings than on external figures such as the turnover. Section C reflected the current state of the company's IT security or related matters. Especially it asked for whether certain technologies or techniques are used.

4. RESULTS

4.1 Case Study Results

From the 133 controls contained in ISO 27001, we found 35 of them to be attainable with the available means, staff and skills. 68 controls were even found to be already compliant as a result of documented working procedures evolved without prior knowledge of the standard and derived from the company's intuitive understanding of security. 30 controls have been marked as unattainable when attempting to implement it. Reasoning brought up four main rationale:

(A) A too weak market position. Large enterprises closing large deals with their business partners can justify demands such as including IT security terms into acquisition or cooperation contracts. The studied company does not invest enough turnover to make such demands (is applicable to controls 8.1.2, 10.2.1, 12.1.1).

(B) Technical Difficulties. Some controls require technical equipment which is not available. Off the shelf vendor software does not always satisfy requirements (10.6.1, 11.4.1, 11.4.4) but no better substitute can be found in the same price range. Also, procedures like testing a disaster recovery case cannot be fully carried out because fallback hardware is only available to a limited degree i.e. IT systems are not 100% redundant and testing anyway would interrupt the operation of the daily business (14.1.5). With the IT environment being a grown structure, inhomogeneity is common among the products used. Despite the small size of the network, vulnerability management is an exhausting task in the absence of affordable technical solutions. This results in the need to manage vulnerabilities manually. The same is true for regular reviews of user access rights (12.2.4) and source code management (12.4.3). Both tasks could be automated if better affordable solutions were available. Since they are not, it overworks available manpower.

(C) Skill/Staff shortage. With most employees being trained in the businesses main fields of activity, specialist knowledge in computer forensics and law is rather not available (6.1.5, 10.8.1, 13.2.3, 15.1.1, 15.1.4).

Among other techniques, ISO 27000 utilizes segregation of duties as an organizational measure to achieve transparency and therewith security. Segregation however requires individuals between which duties can be segregated. Given the small number of IT employees a segregation is often not achievable (10.1.3, 10.10.4, 15.3.1).

Some demanded security management tasks are in the nature of their work attainable, the time needed to carry them out lies however by far beyond what is available to IT staff. Additional employees would be needed to keep track with them. Examples are a complete asset management, functionally testing each software update or patch as well as input/output validation for vendor products (10.3.2, 12.2.1, 12.2.2, 12.2.4, 12.5.4, 12.6.1).

Doubtful Cost-Benefit Relation. Some measures like the physical barriers and entry controls (9.1.1, 9.1.2) have a doubtful cost-benefit relation. The same is true for the helpdesk service management (9.2.4) and an even more detailed incident response plan (13.2.1).

Due to its fields of activities, some controls do not apply to the audited company. Controls 10.9.1 through 10.9.3 for example deal with security in electronic commerce systems. Since no such system is in place, they could be skipped.

4.2 Survey Results

The survey had a total amount of some 30 valid and plausible responses which fall under the working definition of medium enterprises. As for the companies' working domain, the IT industry makes up the largest group of industries, however it doesn't constitute the majority of answers. Reaching from construction engineering over media to controlling, the sample covers several industries.

The response rate of the survey was around 5 percent. While it is obviously desirable to have higher rates, the relatively low rate does not necessarily prevent results from being generalizable to a bigger population.

Non-response can have different causes and it is important to highlight, that a low response rate taken by itself does not imply a low quality of the sample. Whether a result is generalizable despite a low response rate depends on its reasons. More precisely: A high response rate is neither essential nor sufficient. Schnell et al. (2005) point out that the generalizability of sample results depends on whether the participation behavior is linked to the matter of study. Further they state that if there is no link present one can assume that responses are "missed at random" so that there is not necessarily a skew at hand.

4.2.1. Answers

Practically all responding companies stated that their company IT was business critical to them (96%) but only a small part of them (17%) had a written IT security policy in place.

Key business figures and security policies. Furthermore, the annual turnover can be found to have no measurable influence on whether the company makes use of formal standards or not.

Nearly a third of the interrogated companies stated that they had experienced security related incidents in the past. This was usually more than once and in two instances the company even filed a complaint. There is no recognizable correlation between company size and the frequency of occurrence of security incidents. Except in one case, all companies that had experienced security incidents didn't have a written security policy and vice versa.

Impact of general business regulation on security management. Several of the responding companies said their business underlay a governmental regulation such as those for engineering disciplines, quality standards for food production or manufacturing of pharmaceuticals. We anticipated that regulated professions could make more frequent use of formal standards as they could display proper handling of potential security risks to regulatory authorities. We found however no connection between the regulation of businesses and the application of formal security standards – that is, companies operating in regulated businesses do not have written security policies more often. The same is true for the adoption of and certification according to other standards such as ISO 9000 for process quality management. In fact even most (otherwise) certified companies did not have a written security policy, and those which had a security policy in place, did not have any (other) certification.

Cooperation and mutual agreements. Some formal security standards such as ISO 27000 require organizations to have mutual security agreements and require cooperating parties to maintain the same level of security standards. All companies which had a written IT security policy did also have cooperation contracts with other parties. The reverse is however not true. Several companies did not have a security policy despite the fact that they were in a contractual (cooperation) relationship with other organizations. The research assumption that cooperation contracts could therefore lead to companies encouraging others in elaborating a policy cannot be affirmed based on the data at hand. It might however still be the case. Eventually this can just not be shown because so few medium enterprises do use IS standards. When two companies not adhering to standards set up a cooperation relationship, there is no encouraging motivation existent. Pointedly analyzing standard compliant companies could reveal more on this.

Security policies and workload. Another aspect of interest is the burden of workload imposed by implementing a formal standard. Intuitively it should be expected, that as the amount of manpower grows, so does the capability to implement a standard and hence the company is more likely to use one.

We polled the amount of IT manpower available to the organization and determined the proportion of the total amount of employees to the amount of IT personnel. Proportions did however display a big variance so it was not possible to conclude that with a growing amount of employees, IT staff or a better proportion in both of them it would be more likely for the company to have a security policy.

As for the overall amount of time needed to implement a policy, responses indicated a workload between one and twelve months depending on the company size.

Availability of key qualifications. Some key qualifications are requirements for the successful implementation of a security standard. A data protection policy for example is a prerequisite but for its elaboration, the essential skills must be present within the organization. Concerning this, the survey asked for the existence of a legal department, employees trained in data protection law and computer forensics. As expected, all companies which have a security policy, also have a data protection policy in place. Companies do however have a data protection policy three times as often as they have a security policy. A legal department again is an uncommon thing among respondents and nearly all companies that have one anyway are the ones having a security policy. All employees trained in computer forensics work in a company having a security policy. Legal skills as well as those in computer forensics fall together with the existence of a security policy. It is remarkable, that external help appears typically not to be sought.

Appraisal of business decisions. Some questions in survey section C were designed to spot check the current state of IT security within the organization. It has been anticipated, that only few respondents have made use of an IS standard. To verify if the waiver of IS standards can be rationalized from a technical and from a business perspective, some questions tried out if the company's current IT environment is based upon a profound basis taking information security into account.

The survey asked how IT system maintenance responsibilities are arranged, whom security related incidents are reported to and how properly IT facilities having different security levels are separated from each other. Finally it asked if the business value of certain services and therefore the financial damage in case of outages is known to the company's management.

All these aspects of IT security are handled in the considered IS standards but would at the same time be explicable by common sense. Their accomplishment would argumentatively assist the company's negligence of IS standards. Failing them however hints to a potential misconception of what is necessary to maintain the company's IT environment's security.

Practically all respondents did answer they had clearly lined out responsibilities for IT tasks. At the same time nearly half of them stated that non-IT staff were involved into maintaining IT systems, which according to expectations is more likely to lead to mishandling.

Nearly one fourth mixes private information processing facilities with corporate ones which is an ideal prerequisite for information leakage in either direction.

Approximately half of the companies have not determined whom security incidents are reported to. Instead they follow a per incident strategy and decide in the event of a disaster, which does neither support a prompt incident response nor does it guarantee, that IT staff can obtain eventually required authorization of far reaching measures that might be necessary for system recovery.

Most companies are not able to estimate the business value of their IT services and the losses that occur in case of downtime. In consequence, the business decisions about if and how to protect these assets have been made without knowledge of their actual value to the company.

4.3 Generalization of results and comparison with case study results

As pointed out above, four main rationale for why the audited company cannot straightforwardly implement ISO 27001 have been observed during the case study. Assuming that "structural conditions" in medium enterprises in general are similar to those at the studied company, we conclude that these will probably apply to a larger picture. This assumption is supported by the survey results.

Some elements of uncertainty remain. In 3.1.2 we mentioned that the attainability of standard controls has been determined on the basis of the company's own assessment. Though most assessments were based on rather invariant facts like the availability of certain management software on the retail market, or the availability of manpower, this assessment could be more or less distinct in other cases. However, while single standard controls could be assessed with another outcome in different cases, it appears unlikely that the proportion of attainable and unattainable controls would be completely different.

The too weak market position (rationale A) is due to the company's overall amount of turnover and the part of it that is invested into IT. Since the term medium enterprise is for the one thing defined based on the company's turnover it can be anticipated, that this situation will not be significantly different in other companies.

The technical difficulties stated in rationale B are due to a lack of available technical off the shelf solutions in a price range that is affordable measured by the company's IT budget. So the potential generalizability of this point goes back to rationale A.

The same applies to rationale D (doubtful cost-benefit relation).

In terms of the skill and staff shortage (rationale C), it is visible that the structure drawn by the survey is quite similar to the one observed at the audited company. In this aspect the survey militates in favor of the generalizability of the case study.

5. CONCLUSIONS

Most literature on the topic of formal information security standards approaches this topic from the regulatory compliance side hence putting an emphasis on business aspects. The effectiveness and technical aspects of formal standards are discussed in a series of papers such as those by Spionen (2006), Hoehne & Eloff (2002) and Rahmel (2007). Data about the customariness of standard driven security strategies as well as statistics on which of them are used predominantly can be found in popular annual survey reports like those by Ernst & Young and Deloitte Touche. Anyhow, until now literature typically illuminates the subject without specific regards to medium enterprises. As an empirical investigation, we delivered an insight into the information security culture of medium sized enterprises and therewith contributed to closing this gap.

It has been determined how common it is for medium enterprises to make use of formal information security standards and put formal security policies into place. Using a case study as research methodology it has been assessed which parts of today's most common formal standards are unattainable and would therefore justify negligence or mitigation of parts of their content. By auditing a medium sized enterprise's current state of IT security and its implementation capabilities of ISO 27001 as an example standard, it could be demonstrated, that the object of study could implement 77% of the overall requirement. While this means, that not all requirements can be met right away, it also demonstrates, that the great majority can. In line with (BSI100-2), the amount of compliant and attainable controls represents the pareto-part of all possible security measures.

The fact that 51% of standard controls were not implemented at the audited company but were attainable right away, reflects the generally accepted view, that formal standards help companies to complement their own list of imaginable security incidents against which the organization is to be protected. The fact that formal standards are beneficial contributions towards a holistic security strategy applies to medium enterprises just as it does to large ones.

Medium enterprises often dispose of fewer means as compared to large enterprises. This causes hurdles on theses companies' way to implement standards. At the same time however, their sometimes more constrained field of activity leads to several requirements not being applicable and therefore checked off without need for further action.

7. BIBLIOGRAPHY

Ambi, K.D.: Introduction to Information Security Standards (n.d.)
http://egovstandards.gov.in/states_repositories/andhra-pradesh/brainstroming_sessions/andhra-pradesh/network-information-security-standards/egsworkshopfile.2006-12-13.0649253072/at_download/file

Anderson & Moore: The Economics of Information Security (2006)
http://www.cl.cam.ac.uk/~twm29/science-econ.pdf

Anderson, Ross: Why Information Security is Hard - An Economic Perspective (2001)
17th Annual Computer Security Applications Conference
http://www.acsac.org/2001/papers/110.pdf

Barlette & Fomin: Exploring the suitability of IS security management standards for SMEs (2008)
Proceedings of the 41st Hawaii International Conference on System Sciences 2008
Available at:
http://csdl.computer.org/comp/proceedings/hicss/2008/3075/00/30750308.pdf

BS ISO/IEC 27001: 2005 Information technology. Security techniques. Information security management systems. Requirements

BS ISO/IEC 27002:2005, Information technology. Security techniques. Code of practice for information security management (2005)
http://www.bsonline.bsi-global.com/server/PdfControlServlet/bsol?pdfId=GBM24%2F30166440&format=pdf

BS7799-1: Information security management, Part 1: Code of practice for information security management (1999)

BSI-Standard 100-1 Information Security Management Systems (ISMS) (2005)
http://www.bsi.de/english/publications/bsi_standards/standard_1001_e.pdf

BSI-Standard 100-2: IT-Grundschutz Methodology (2005)
http://www.bsi.de/english/publications/bsi_standards/standard_1002_e.pdf

BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz (2005)
http://www.bsi.de/english/publications/bsi_standards/standard_1003_e.pdf

Dawson, Christian W.: Projects in Computing and Information Systems (2005)
Addison Wesley ISBN: 0-321-26355-3

Ernst & Young: Achieving Success in a Globalized World: Is Your Way Secure? - Global Information Security Survey (2006)
http://www.ey.com/global/assets.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf

Federal Office for Information Security: Guideline IT security [German] (2007)
http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Federal Office for Information Security: IT-Grundschutz Manual (2004)
http://www.bsi.de/english/gshb/manual/download/modules.pdf

Flyvbjerg et al: Five misunderstandings about case-study research (2004)
Sage Publications
http://flyvbjerg.plan.aau.dk/MSFiveMis9.0SageASPUBL.pdf

Höne, Karin & Eloff, J. H. P.: Information security policy — what do international information security standards say? (2002)
Computers & Security, Volume 21, Issue 5, 1 October 2002, Pages 402-409
doi:10.1016/S0167-4048(02)00504-7, Elsevier Science Ltd.

Institute for SME Research BONN: SMEs in Germany - Facts and Figures (2004) http://www.ifm-bonn.org/ergebnis/sme-2004.pdf

ISACA: COBIT 4.1 Executive Summary (2007) http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172

ISMS User Group: Certificate Register (2008) http://www.iso27001certificates.com

ISO: The ISO Survey of ISO 9000 and ISO 14000 Certificates(2000) http://www.iso.org/iso/survey10thcycle.pdf

Martins, A & Eloff, J.H.P.: Measuring Information Security (2001), Proceedings of Workshop on Information Security – System Rating and Ranking, Virginia

National State Auditors Association & U.S. General Accounting Office: Management Plannig Guide for Information Systems Security Auditing (2001) http://www.gao.gov/special.pubs/mgmtpln.pdf

Rahmel, J.: Einfuehrung in die Informationssicherheit [German] (2007) http://www.wi2.uni-trier.de/de/cms/teaching/Sommersemester2007/VorlesungInformationssicherheit/InfoSec-1-Informationssicherheit-070603.pdf

Rea, Luis M. & Parker, Richard A.: Designing and Conducting Survey Research (2005)
Third Edition – Wiley ISBN 0-7879-7546-X

Schnell et al: Methoden der empirischen Sozialforschung (2005)
[Empirical social research methodology]
Oldenbourg - ISBN: 3-486-57684-4

Siponen, Mikko: Information Security Standards Focus on the Existence of Process, not its Content (2006)
Journal Commun. ACM
http://doi.acm.org/10.1145/1145287.1145316

Szakats, Daniel: IT Maturity and Sourcing Strategies (2004)
http://www.ifi.unizh.ch/egov/Diplomarbeit_Szakats.pdf

Tellis, Winston: Introduction to Case Study (1997)
The Qualitative Report, Volume 3 Number 2 [Online]
http://www.nova.edu/ssss/QR/QR3-2/tellis1.html

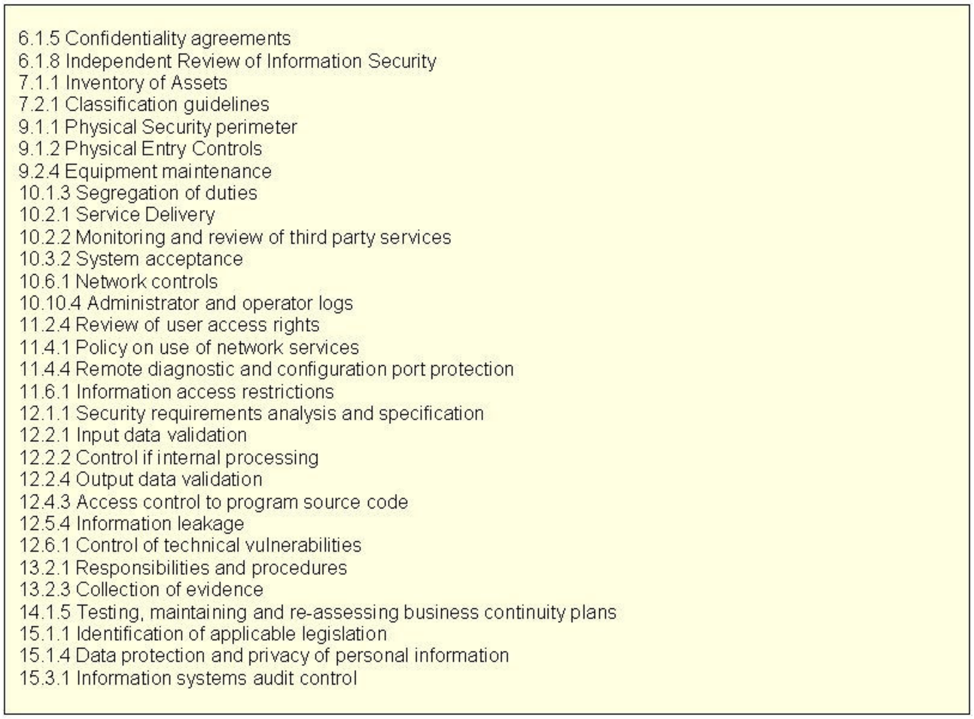
Thelen, Mary J.: Integrating process improvement, ISO 9000 and TQM in SITA Research and Development (1997)
The TQM Magazine - Volume: 9 Issue: 4 Page: 265 – 269
ISSN: 0954-478X - DOI: 10.1108/09544789710181880 - Publisher: MCB UP Ltd

University of Melbourne: IT & ITIL based Glossary of Terms (2008)
http://servicedesk.unimelb.edu.au/knowledgebase/itservices/a-z/p.html

Yin, Robert K.: Case Study Research – Design and Methods (2003)
Applied Social Research Methods Series Volume 5, Third Edition – Sage Publications ISBN 0-7619-2552-X

8. APPENDICES

8.1 : Enumeration of not attainable standard controls



6.1.5 Confidentiality agreements
6.1.8 Independent Review of Information Security
7.1.1 Inventory of Assets
7.2.1 Classification guidelines
9.1.1 Physical Security perimeter
9.1.2 Physical Entry Controls
9.2.4 Equipment maintenance
10.1.3 Segregation of duties
10.2.1 Service Delivery
10.2.2 Monitoring and review of third party services
10.3.2 System acceptance
10.6.1 Network controls
10.10.4 Administrator and operator logs
11.2.4 Review of user access rights
11.4.1 Policy on use of network services
11.4.4 Remote diagnostic and configuration port protection
11.6.1 Information access restrictions
12.1.1 Security requirements analysis and specification
12.2.1 Input data validation
12.2.2 Control if internal processing
12.2.4 Output data validation
12.4.3 Access control to program source code
12.5.4 Information leakage
12.6.1 Control of technical vulnerabilities
13.2.1 Responsibilities and procedures
13.2.3 Collection of evidence
14.1.5 Testing, maintaining and re-assessing business continuity plans
15.1.1 Identification of applicable legislation
15.1.4 Data protection and privacy of personal information
15.3.1 Information systems audit control

8.2 Online Survey Instrument

Section A - Company Classification
1. Question: How many employees does your company have? (approx.)
2. Question: What is your average annual turnover? (approx. in USD)
3. Question: What domain are you working in?
4. Question: Is your profession underlying some kind of governmental regulation e.g. Engineering, Quality Standards for manufacturing pharmaceuticals or the like?

Section B - Company Structure and Organization
5. Question: Has your company obtained some kind of standard certification such like ISO 9000?
6. Question: How many full time IT staff do you have?
7. Question: How many of your employees serving in non-IT positions do perform IT tasks anyhow? E.g. Sales person responsible for (technically) administering certain services such as a CRM database.
8. Question: Does your company IT have a set out budget? If yes: how much is it?
9. Question: Do you have clearly set out responsibilities for IT tasks?
10. Question: Do you have a data protection policy?
11. Question: How many of your employees are Teleworking e.g. using VPN and/or Terminal Services?
12. Question: Do you have personnel that is trained in data protection law applicable to your company's country of registration?
13. Question: Does your company have a legal department?
14. Question: How many training events (in any subject) has your average employee been on during the last year?
15. Question: Do you have co-operation contracts with other companies? E.g. collaborative research and development projects?
16. Question: Have any of your IT services been outsourced? (includes customization of business applications)
17. Question: Do you have IT personnel that have been trained in Computer Forensics?

Section C- Current State of IT Security
18. Question: Is the correct operation of your IT services business critical?
19. Question: How many security related incidents have you experienced within the last 3 years?
20. Question: Did you file a complaint?
21. Question: Do you have a written IT security policy in place?
22. Question: How many employees have been involved in elaborating it?
23. Question: How many months did it take to set it up?
24. Question: Are you using mobile technologies such as WLAN?
25. Question: Do you make use of PKI services?
26. Question: Has your company been issued a certificate by a certificate authority like Verisign© or the like?
27. Question: Have you obtained a certification such as BS7799/ISO17799/ISO27001?
28. Question: If you have obtained any other IT security related certifications, please name it here:
29. Question: Can you estimate the loss in USD that would occur if one of your core services such as Email system, VoIP PBX would fail for a certain amount of time? E.g. 6 hours of Online Shop Downtime would result a loss of XY$ revenue.
30. Question: Does your company premises have structural conditions that allow being partitioned into different sections so that different levels of physical access can be granted to personal?
31. Question: Do you have an information classification scheme which allows you to determine which of your business information needs to be kept secret and how such information shall be handled?
32. Question: Is it technically imaginable that teleworkers gain access to your company network via VPN using non-company computing equipment such as home PCs?
33. Question: Whom are security related IT events reported to? (CEO CIO/CSO not determined yet, will be decided then)