Business Impacts of International Standards for Information Security Management. Lessons from Case Companies

Robert M. van Wessel[1] and Henk J. de Vries[2]

[1]*Rotterdam School of Management, Erasmus University Department of Management of Technology and Innovation P.O. Box 1738, Room T10-42 3000 DR Rotterdam The Netherlands Phone: +31-6-28257307 Fax: +31-10-4089014 e-mail: rwessel@rsm.nl*
[2]*Rotterdam School of Management, Erasmus University Department of Management of Technology and Innovation P.O. Box 1738, Room T10-42 3000 DR Rotterdam The Netherlands Phone: +31-10-4082002 Fax: +31-10-4089014 e-mail: hvries@rsm.nl*

Received 18 January 2013; Accepted 14 May 2013

Abstract

This paper describes the business impact of two international standards for information security management: ISO/IEC 27001 and ISO/IEC 27002. Six company cases show that companies had different reasons for wanting to implement these standards, but that they achieved most of their objectives. Benefits include improved service quality, higher customer satisfaction, and in some cases, new business opportunities. A number of common success factors ensure the objectives can be achieved, and financial and non-financial benefits can indeed be obtained. The lessons learnt from these cases can help other companies to also reap such benefits.

Keywords: Information security, ISO/IEC 27001, case study, standardization, business impact.

Journal of ICT Standardization, Vol. 1, 25–40.
doi: 10.13052/jicts2245-800X .122

1 Introduction

1.1 Background

In today's digital age, information has become one of the most important assets of organizations and society as a whole. Information such as credit card details, medical records, and strategic business plans is increasingly processed and stored electronically and transmitted across the Internet. Properly protecting information is vital for competitive, legal and reputational reasons. Governments and businesses face considerable risks if information is not available, not reliable or unintentionally disclosed. 'Wikileaks' demonstrated that this has a major impact on individuals, organizations and society. Information security management deals with these threats, by assessing business impact, analysing vulnerabilities and applying suitable controls to achieve a balance between security, costs, usability and other business requirements.

1.2 Standards for Information Security Management

Systematic information security management needs accepted and reliable approaches. These have been developed and are laid down in standards. Different standards are available, but the most common and generally accepted framework by information security professionals is the standard ISO/IEC 27001 [1, 2] which is part of the ISO/IEC 27000-series of standards for information security management systems. These standards are published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). They are intended to assist organizations of all types and sizes to implement and operate an information security management system (ISMS). The series provides good practices on information security management, risks and controls, and is similar in design to management systems for quality, environmental and IT service management (ISO 9000, ISO 14000 and ISO/IEC 20000 series respectively). ISO/IEC 27001 [2] specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a formalized ISMS within the context of the organization's overall business risks. The directly related standard ISO/IEC 27002 [3] provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance. These two standards originate from British Standard BS 7799, published in 1995.

At the end of 2010, at least 15,625 ISO/IEC 27001:2005 certificates had been issued in 117 countries. Most certificates were issued in Japan, India and the United Kingdom, with the highest growth in Japan, China and the Czech Republic. Figure 1 shows the growth in number of certificates [4].

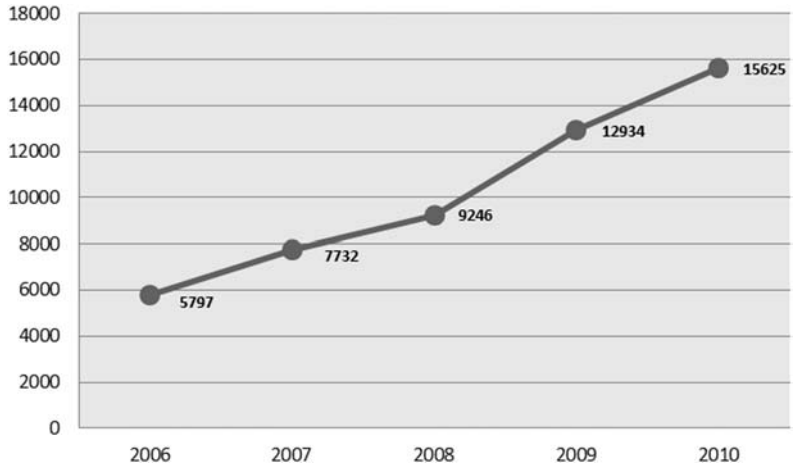

Figure 1 Number of ISO/IEC 27001 certificates [4].

1.3 Lack of Research in this Domain

With the growing importance of information security for business and society, an increased interest in this topic is found in academic literature [5]. Most contributions can be found in the fields of computer science and economics. A number of studies try to quantify the economic impact of information security, and some deal with information security management systems. Few address implementation [6] and impact [7, 8], and hardly any combine information security, organizational performance and the use of standards for information security management. In [9] a procedure is proposed to select the optimal investment of the required security technology based on the quantified value of an information system and capital investment appraisal techniques, whereas [10] proposes a Balanced Scorecard approach.

1.4 Research Approach

Due to this lack of research, BSI British Standards and the Chair of Standardization of the Rotterdam School of Management, Erasmus University

initiated a common research project on the business impact ISO/IEC 27001 and ISO/IEC 27002 on companies. It provides evidence of positive impacts, and relates impacts to the way companies adopt these standards, so that other organizations can learn to also reap the benefits.

A conceptual model was used to assess the financial and non-financial impact for organizations [11]. The model includes the management and governance of the selection, implementation and use of the standard, and measuring its impact. Management of the standard is defined as the decision-making efforts associated with planning, organizing, controlling, and directing the selection, implementation and use of the standard in the organization. Governance of a standard is defined as specifying the decision rights and accountability framework to encourage desirable behavior in the selection, implementation and use of the standard in the organization. Impact is measured according to the Balanced Scorecard perspectives [12]. We use the Balanced Scorecard as it is a well-established method to measure performance, taking into account both tangibles and intangibles [13]. It includes the firm's current operating performance and its future performance drivers by measuring and tracking business performance from four perspectives: financial, customer, internal / business process, and learning & growth.

In-depth case study research was carried out at two companies in the UK and four companies in the Netherlands (see Table 1). Interviews with staff lasted between one and four hours.

All companies implemented relevant control objectives and best practice controls as specified in ISO/IEC 27002.Two companies acquired company-wide ISO/IEC 27001 certification, whereas four obtained certification for specific departments.

2 Results

The case companies adopted the standards for internal and external reasons. The most important internal ones were: 1) increasing the quality of services offered, 2) reducing the costs of security operations through standardized procedures and technical implementations to be applied in projects, and, 3) improving the company's risk profile. The most important external reasons were: 1) meeting customer requirements, 2) complying with legal requirements, and 3) improving brand and reputation.

ISO/IEC 27001/2 adoption resulted in a number of business benefits. Most companies reached most of their initial objectives and two achieved all of their objectives. One company accomplished only half of them. The primary cause

Table 1 Profile of the case companies that adopted ISO/IEC 27001/2.

Case	***Sector***	***Type***	***Country***	***Number of interviewees***	***Size***	***Certification scope***
1	Financial Services	Commercial	NL	5	Very large	Some departments
2	Computing Services	Commercial	NL	1	Very large	Some departments
3	Financial Services	Commercial	NL	2	Very large	Some departments
4	Telecommunication	Commercial	NL	2	Very large	Some departments
5	Purchasing	Public	UK	1	Large	Enterprise-wide
6	Software Development and Maintenance	Commercial	UK	2	SME	Enterprise-wide

was that it did not create standardized implementation (security) guidelines for projects. Each new project had to start from scratch, negatively impacting costs and throughput times.

In the following sections, we give a systematic overview of the impact on the business performance using the Balanced Scorecard perspectives.

2.1 Financial Perspective

The standards brought financial benefits, although the companies could not produce exact figures. Certain IT development costs increased (e.g., more project risk assessments) whereas other costs decreased, as less rework was required (e.g. no fixes due to lack of security). Operational losses fell but some operational costs rose (e.g., more vulnerability checks).

The majority of costs were incurred during the implementation of ISO/IEC 27001 or 27002. These included consultancy and certification costs. During the use phase, investments were made to guarantee secure information systems, and to develop staff training and induction programs for information security awareness. The standards resulted in better IT systems, and for some case companies, ISO/IEC 27001 certification resulted in new business opportunities and thus a positive financial impact.

2.2 Customer Perspective

The standards led to increased customer satisfaction. ISO/IEC 27001/2 certification provides reassurance to customers that the company's security status meets internationally accepted criteria and demonstrates credibility and trust that customer data is protected properly. Companies became more aware of potential risks and the standard leads to better understanding and cooperation between business-driven departments and the IT department. Of course, the customers should not be bothered with security implementations of the ISMS but in our cases they could see the difference: customer satisfaction on IT delivery and support improved.

Although certification was not a prerequisite for corporate clients of the telecommunication company (case 4), they responded positively to its ISO/IEC 27001 certificate. For two companies, certification was a prerequisite. One provided white labeling services (case 1). The other required certification because its competitors were already certified (case 2). One company (case 6) reported that it had had no major security incidents since certification, which contributed to customer confidence.

2.3 Internal Perspective

All companies achieved better quality of IT services and a reduced risk level. Authorization, IT asset management and change management improved. ISO/IEC 27001/2 certification increased awareness of business continuity, reduced the number of ad hoc activities, and led to a structural approach to resolve incidents. In a number of cases, availability of information systems increased. Little impact was found on time to market new services and time to develop and support IT.

Generally, staff were mildly positive about the standards. They became more aware of potential information security risks (threats and vulnerabilities). IT staff, however, were less positive as they considered many control measures to be bureaucratic, leading to an increase in workload. Staff opinions about the complexity and attractiveness of the standards depended on how the standards were implemented, ranging from a blindfold implementation of 133 control measures (negative) to selecting those that addressed high business risks first (positive). We also found that certification (enterprise-wide or at department level) improved the overall quality of the services offered and the risk profile of the company more than "just" being ISO/IEC 27001/2 compliant.

2.4 Learning & Growth Perspective

With relation to learning, a key advantage of the standards is that their broad acceptance in the information security profession leads to a common understanding of controls and vocabulary. Proven methods are used and staff do not need to reinvent the wheel. The standards can be considered as a framework for quality improvement in general, such as release management, version control and document management. Furthermore, the standards increase the level of quality thinking and risk awareness. With relation to growth, scalability of the IT infrastructure is easier because of the precautionary measures and these measures reduced the number of ad hoc security measures.

In some cases, ISO/IEC 27001 certification was a prerequisite for maintaining current business levels (cases 1, 2, 3 and 6), whereas for others it resulted in opportunities for new business. The telecommunication company (case 4) improved its competitive position through certification. For the most mature company (case 5), ISO/IEC 27001 was seen as business enabler. New jobs were created by developing new value-added secure service offerings.

Most of the case companies indicated positive effects during implementation and use due to familiarity with other quality management system standards, such as ISO 9001 and ISO 14001. Companies improved their market

position by adopting an integrated set of such management system standards. One of the information security managers explained: "*Information security and green IT actually co-exist beautifully. Computer virtualization is a good example of this co-existence. It requires fewer resources as multiple computers systems are put logically on one machine, and security can be met more easily. Wherever you see a green policy, you see a security one that goes with it and vice versa. Why? Both are common sense, it is the right thing to do!*"

3 Analysis: Success Factors

Based on these case studies, we identified a number of success factors that ensure that the objectives and business benefits of ISO/IEC 27001/2 initiatives can be achieved.

3.1 Involvement of Business-Driven Departments

Probably the most important element of successful implementation is to ensure that ISO/IEC 27001/2 implementation is a business- rather than an IT-driven activity. Information security requirements should be determined by business-driven departments that can identify areas of weakness in risk assessments. Subsequently, these departments should implement controls that really add value, using a risk/benefit trade-off. Adequate governance and management of the ISMS is a key requirement.

In one of the companies (case 6), ISO/IEC 27001 was IT-driven as the IT director had initiated the project. At first, the steering committee met monthly. It took a while for management team to realize that without them actually proactively participating and filtering information down to their teams, the project was doomed. In another company (case 5) which had worked with ISO/IEC 27001 for many years, information security encompassed the entire company and was incorporated in everything the company did.

3.2 Senior Management Commitment

A second key element is to ensure commitment and endorsement for ISO/IEC 27001/2 at senior management levels. Although bottom up approaches may be successful to a certain extent, without the active support of senior management such initiatives will result in suboptimal results at best. For example, at the telecommunications company (case 4), the CFO initiated ISO/IEC 27001/2 adoption without top management endorsement. However, the chief

information security officer ensured that full executive commitment was achieved, and the Board of Directors approved ISO/IEC 27002 implementation enterprise-wide. Again, adequate governance during selection and implementation determined the level of success.

3.3 Staff Involvement During Implementation

Another key element is to create awareness in all business-driven departments and the IT department, at both management and staff level. Prerequisite to success is continuous attention (e.g., weekly agenda item on implementation progress) by local MTs since these have to enable implementation. In the company cases, awareness was developed through activities such as workshops on risk assessments, asset classifications, business impact analyses, controls selection, and progress meetings

Based on the case company findings, the preferred implementation sequence was a combination of top-down activities (setting strategic objectives, policies and standards) and local bottom-up initiatives. A gradual implementation process was more successful than a 'big bang' approach, especially for the larger companies. For small companies, the big-bang approach was successful as well. Furthermore, a pragmatic and focused tactic (e.g., resolve major incidents, or requirements from regulators) was very effective. For example, one company started to tackle issues with logical access control by focusing on the five to ten most critical applications per business unit, and consequently the business-driven department became more involved. Furthermore, it turned out to be better not to speak in terms of specific controls (e.g. has control 10.4.2 "Controls against mobile code" been implemented?) but to discuss business implications of control measures. The following steps can be taken: 1) identify what should be protected, 2) determine the stakeholders, 3) perform risk analyses based on a standardised template, and 4) implement controls that really add value based on the specific risks (risk/benefit trade-off).

3.4 Continuous Improvement

Successfully completing an ISO/IEC 27002 implementation project and acquiring ISO/IEC 27001 certification are important milestones. However, ongoing improvement is vital to achieve and sustain long-term business benefits. We identified several key elements to success in this area. One is the importance of feedback from the user and project community about specified policies and standards. Policies and standards should be updated regularly as specified in Deming's well-known plan-do-check-act quality management cycle. The

same holds true for implementation of (security) guidelines for projects to meet control measures. If the information security department creates standards or guidelines on how to implement measures such as access control, encryption or two-factor authentication, projects can get a head-start and project managers do not have to reinvent the wheel. For example, this will have a positive impact on costs, time to market, and interoperability.

Furthermore, disseminating information security policies, standards and best practices as part of security awareness is vital. Although information security awareness may exist among staff, when it comes to actual behavior, they often perceive information security controls as a hindrance to their normal routine. To maintain an acceptable level of security, information security awareness campaigns should be carried out twice a year and supported by website articles, emails, and warnings about hot topics. One of the companies (case 1) used desktop wallpapers as daily reminders of the importance of adequate information security behavior. Management should regularly assess staff satisfaction with the policies, standards and services offered by the information security department.

3.5 Clearly Defined Deviations Process

Another key element to the success of an ISO/IEC 27001/2 implementation project is the way a company deals with deviations from the prescribed controls. These controls should be mandatory but a number of case companies offered the possibility to temporarily deviate from these control measures, if accompanied by sound business rationale and mitigating factors. Other case companies did not allow any deviations but incorporated amended control measures into the ISMS if the current controls were no longer effective. Such decisions are all founded on proper risk-based analyses. The exception process differed per company. As long as the company considers this process adequately, the business-driven community will support information security. If not, it will find ways to circumvent the controls.

3.6 Experience with other Management System Standards

Another element of successful ISO/IEC 27001 implementation is familiarity with other management system standards. In one company (case 4), experience with ISO 9001 was an important success factor. Experience with the ISO 9001 quality management system resulted in 50% less time and effort spent on the implementation of ISO/IEC 27001 because improvement management, control mechanisms, context diagrams, and overviews of staff and systems

were already available. One of the interviewees recommended companies to first implement ISO 9001 and only then ISO/IEC 27001. In another company at local management level (case 2), the general attitude towards using ISO/IEC 27001/2 was positively affected because of this same reason. During the ISO 9001 implementation project, management had initially opposed the quality management system. However, management had a much more positive attitude towards ISO/IEC 27001. This suggests a positive relationship between ISO 9001 and ISO/IEC 27001 adoption. The same is expected for similar management systems standards such as ISO 14001.

3.7 Governance and Management

Based on the case studies, we identified the following successful governance mechanisms. These support the findings of [11].

- Strategic and operational alignment of business-driven departments and the IT department in the selection process and operational phase. Business representatives should be more involved than IT staff. In all case companies, decisions about information security investment objectives and resource allocations were driven by the level of risk or based on regulatory requirements. The companies used a cost/benefit analysis to make these decisions.
- The integration of the controls, templates, etc. into existing processes and governance structures of the organisation. This includes, but is not limited to, strategy and year plans, project management, incident and change management, and IT service management tooling. In one of the organizations (case 4), information security project participation was first reactive, but the organization successfully leveraged its innovation structures and processes making it proactive.
- A convergence of functions in the security domain (information security, physical security, operational risk management, etc.). Functional embedding of information security differed per case company and most companies had a centralized set-up in either the IT or the corporate Risk Management departments. In the most mature organization, it was positioned just below board level.

We also identified the following successful management mechanisms:

- A positive attitude of management towards ISO/IEC 27001/2, such as commitment, priority setting and endorsement of the standard.Information security awareness programs. Awareness sessions for staff, evalua-

tions for management and workshops for both are essential to maintain and develop awareness.
- Information security staff should be attentive to changes in the organisation by anticipating changes in business needs, changes in management (structure), or new technology.
- An adequate waivers and dispensation process that allows companies to (temporally) deviate from the ISO/IEC 27001/2 standard and its related control measures.

4 Conclusions

The more organizations depend on information, the more important it is to ensure the confidentiality, integrity and availability of information systems. International standards have been developed to assist in this field. Standards provide a benchmark and good practice examples, guarantee that support is available (courses, consultancy, etc.), and certification signals achievements to external parties.

The international standards ISO/IEC 27001 and ISO/IEC 27002 are widely accepted by the information security profession. They are generally perceived as clear, pragmatic and logically structured, and contain proven concepts based on good practices. These standards accommodate a common language, improve awareness, communication and understanding of information security, increase customer satisfaction, enable the organization to offer more products; create business opportunities, and ISO/IEC 27001 provides the opportunity to acquire certification. Some organizations use ISO/IEC 27002 as a checklist that provides baseline measures. More experienced information security staff warn that this is the major pitfall as ISO/IEC 27002 has a vast number of control measures (133). The standard helps staff to think in terms of risk and risk management. Because of its risk based approach, a company only needs to mitigate those risks that are applicable to their business. Although not part of our case study, we anticipate the standards to be also beneficial for non-commercial organizations. Some of our case companies provide crucial services for society, such as public procurement, core financial services and telecommunications. In this way, the standards also contribute to a well-functioning society.

Our research contribution is threefold. First, we describe the business impact of ISO/IEC 27001/2. Many studies are available on the business impacts of other management standards, in particular ISO 9001 [14, 15, 16] and ISO 14001 [17]. We extend this by providing a study on the impact of a management

standard in another domain. Second, this study shows that ISO/IEC 27001/2 adoption has led to overall improvements in service at both the technical and procedural level. Third, we have identified a number of good practices. By ensuring the success factors discussed earlier, the positive impact of ISO/IEC 27001/2 can be maximised. This study also confirms Taiwanese specific findings [6] that support from top management (section 3.2), awareness and education (section 3.4), and past experience with other standards (section 3.6), are important factors that influence the results of ISMS implementations. Other good practices include involvement of business-driven departments, commitment of senior management, an implementation process that combines top-down activities and local bottom-up initiatives, ongoing improvement of the ISMS, and a clear deviation process. In addition, experience with other management standards and effective governance and management mechanisms during the selection, implementation and use phases have a positive impact on a company's performance.

To conclude, companies can reap substantial benefits from the adoption of the international standards for information security management ISO/IEC 27001 and IEC 27002. The more the organisation depends on information systems, the more impact there is on performance. Our lessons on how to implement and use the standards may therefore be informative for many organizations.

Acknowledgements

The authors thank the case companies for their willingness to share their experiences, and BSI and Netherlands Standardization Institute NEN for their support.

References

[1] J. Backhouse, C.W. Hsu, L. Silva. Circuits of Power in creating de jure Standards: Shaping an International Information Systems Security Standard. *MIS Quarterly*. 30, 413-438, 2006.

[2] ISO/IEC, *ISO/IEC 27001 Information technology–Security techniques– Information security management systems–Requirements.* Geneva, Switzerland: International Organization for Standardization, and International Electrotechnical Commission, 2005.

[3] ISO/IEC, *ISO/IEC 27002 Information Technology—Code of Practice for Information Security Management.* Geneva, Switzerland: International Organization for Standardization, and International Electrotechnical Commission, 2005.

[4] ISO, "The ISO Survey of certifications 2010", Geneva, Switzerland: International Organization for Standardization, 2011.
[5] S. Ransbotham, S. Mita, "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information Systems Research*, 20 (1), 121–139, 2009.
[6] C.Y. Ku, Y.W. Chang, D.C. Yen, "National information security policy and its implementation: A case study in Taiwan", *Telecommunications Policy*, 33(7): 371-384, 2009.
[7] A.G. Kotulic, J.G. Clark, "Why There Aren't More Information Security Research Studies", *Information & Management*, 41 (5), 597-607, 2004.
[8] J. L. Spears, "Institutionalizing Information Security Risk Management: A Multi-Method Empirical Study on the Effects of Regulation", Ph.D. Dissertation, Pennsylvania State University, 2007.
[9] R. Bojanc, B. Jerman-Blazic, "An economic modelling approach to information security risk management", *International Journal of Information Management,* 28 (5), 413–422, 2008.
[10] T. Herath, H. Herath, W.G. Bremser, "Balanced Scorecard Implementation of Security Strategies: A Framework for IT Security Performance Management", Information Systems Management, 27 (1), 72-81, 2010.
[11] R.M. van Wessel, "Toward Corporate IT Standardization Management. Frameworks and Solutions", Hershey, PA, USA: IGI Global, 2010.
[12] R.S. Kaplan, D.P. Norton, "The Balanced Scorecard - Measures that Drive Performance", *Harvard Business Review*, January-February 1992, 70 (1), 71-79, 1992.
[13] L. Willcocks, Information management. The evaluation of information systems investments, London: Chapman & Hall, 1995.
[14] E.L. Psomas, C.V. Fotopoulos, "A meta analysis of ISO 9001:2000 research - findings and future research proposals", *International Journal of Quality and Service Sciences*. 1, 128-144, 2009.
[15] B. Rusjan, M. Aliè, "Capitalising on ISO 9001 benefits for strategic results", *International Journal of Quality and Reliability Management*, 27, 756-778, 2010.
[16] P. Sampaio, P. Saraiva, A.G. Rodrigues, A.G., "ISO 9001 certification research: questions, answers and approaches", International Journal of Quality & Reliability Management. 26, 38-58, 2009.
[17] H.J. de Vries, D.K. Bayramoglu, T. van der Wiele (2012) "Business and environmental impact of ISO 14001", *International Journal of Quality & Reliability Management*, 29 (4), 425-435, 2012.

Biography

Robert M. van Wessel holds a Master in Electrical Engineering from Twente University and a PhD in Business Administration from Tilburg University (Department of Information Systems and Management). He works as a Business Architect in the financial services industry and is associated with Rotterdam School of Management, Erasmus University. Robert's research interests relate to the interaction of Business and Information Technology, in particular Business Performance and the Value of IT, Enterprise Architecture, IT Governance, Portfolio Management, Information Security Management and IT Standardisation and Standards.

Henk J. de Vries is Associate Professor of Standardisation at the Rotterdam School of Management, Erasmus University, Department of Management of Technology and Innovation. His research and teaching focus on standardisation from a business point of view. Henk is President of the European Academy for Standardisation EURAS, Chair of the International Cooperation for Education about Standardization ICES, and Special Advisor to the International Federation of Standards Users IFAN. He is (co-)author of more than 300 publications in the field of standardisation. See http://www.rsm.nl/hdevries and http://www,rsm.nl/is.