The Impact of ISO 27001 Certification on Firm Performance

Carol Hsu
National Taiwan University
carolhsu@ntu.edu.tw

Tawei Wang
University of Hawaii at Manoa
twwang@hawaii.edu

Ang Lu
National Taiwan University
iluang100@gmail.com

Abstract

The extensive organizational dependence on information technology (IT), along with worsening impact of information security incidents, has made information security one of the top management concerns. The ISO 27001 standard provides guidance to a sound information security management system (ISMS). However, implementation and accreditation costs can also be considerable. In this study, we explored whether the certification can benefit organizations by signaling the management's attitude toward security management and the appropriateness of ISMS implementation. We investigated firm performance after the ISO 27001 certification with samples from the United States and selected European countries. Different from our expectation, we found no evidence that ISO 27001 certification brought benefits to the certified firm in terms of return-on-assets and stock market performance. We attributed the results to the nature of ISO 27001 that a good information security management would be seen as an obligation, instead of a competitive advantage.

1. Introduction

The high profile information security breach incidents, such as hacking, intrusion, and identity theft, have brought enormous public attention and have highlighted that information security is an important managerial issue. Recent survey also showed that total losses incurred in a single security incident, including direct financial loss (e.g., operating losses or negative stock market reactions [1, 2]), reputational loss, and business disruption, have become more severe.

In order to facilitate the development of information security management in organizations, ISO 27001 standard has been developed and adopted by organizations worldwide. This standard is first emerged in 1995 as BS-7799, and further revised in 2005. ISO 27001 is a standard that defines a set of principles about the implementation of an appropriate information security management system. Nowadays, ISO 27001 has already become the widely regarded standard for information security. Given the public concerns of information security breaches, certification of the compliance to the ISO 27001 standard might well serve as an ideal demonstration, or a "signaling tool" [3] to the public, reflecting the manager's evaluation of the information processes or proactive attitude toward information security management. It also shows that the information processing of an organization complies with an international standard, and is thus may be more reliable and trust-worthy.

While certification can potentially bring benefit to the organization, acquiring a certification is usually costly and time consuming. During the certification process, an organization would have to pay a substantial amount to its consultant and registrar. Extensive paperwork and documentation are also required. Thus, we consider that measuring the payback of the certification would be a very interesting topic to investigate. Our research findings might provide critical strategic value in further decision making for top management on certification adoption.

This study investigates whether ISO 27001 certification brings benefits to an organization in terms of operational performance or stock market reactions. Other studies have shown the certification of international standards can bring positive impact on firms' operational and financial performance (e.g., [4, 5]. However, no studies focus on the adoption of ISO 27001. In this study, we analyze organizational performance after ISO 27001 adoption among European and U.S. firms.

The paper is organized as follows. In Section 2, we review current literature in ISO 27001 as well as prior studies about performance of certification adoption in general. Following this discussion, we develop our hypotheses. Our methodology is presented in Section 3 and empirical results are given in Section 4. In Section 5, we conclude with contributions, limitations, and areas of further research.

2. Literature review

2.1. ISO 27001 standard and certificate

1530-1605/16 $31.00 © 2016 IEEE
DOI 10.1109/HICSS.2016.600

We first present an overview of the ISO 27001 standard and certification. As mentioned in the previous section, the ISO 27001 standard, or officially named ISO/IEC 27001:2005, is an international standard published by the International Organization for Standardization (ISO) in October 2005. It belongs to the ISO 27000 family of standards. For example, ISO 27002, a guideline and code-of-practice on Information Security Management System (ISMS) implementation, is a complementary standard to ISO 27001. ISO 27002 was formerly called ISO 17799, which was evolved from BS 7799 Part 1. ISO 27005 concentrates on information security risk management, detailing the risk management approach taken by ISO 27001.

The ISO 27001 standard provides a specification for ISMS. Officially, ISO 27001 define ISMS as "a management system that carries out the establishment, operation, maintenance, monitor, and continuous improvement of information security" [6]. The establishment of policies for ISMS is based on a risk management approach. The definition of policies starts with the understanding of the environment of the business and the evaluation of resources and processes, in order to identify information security risks that might take place. After identifying risks, the firm assesses each of the risks, evaluates the potential impact, and comes up with strategies in managing the risks. The steps above require extensive involvement of the management as well as the employees that carry out the operations. As the environment and the business processes differ from organization to organization, the risk identified and the strategy developed would also differ. That is, the ISO 27001 standard provides the requirements and specification to an ISMS implementation, but the ISMS is tailored for every ISO 27001 adopters.

Prior literature has investigated issues related to security standards. For example, Ku, Chang and Yen [7] analyzed the key factors of successful ISMS implementation based on BS 7799. Boehmer [8] discussed and examined how management should make decisions about selecting appropriate controls while implementing ISO 27001 with case studies. Hsu [9] investigated the behaviors of different social groups involved in the ISO 27001 implementation processes. The behavior of an individual was affected by what one experienced, how one perceived and how one interpreted. Based on a case study conducted in Taiwan, the study demonstrated how different roles held different ideas and took different actions during the implementation period. Boehmer [10] evaluated the efficiency and effectiveness of ISMS implementation of ISO 27001 by using Key Performance Indicators (KPIs) and concluded that the KPIs of these two dimensions are trade-offs.

Overall, the majority of current ISO 27001 studies focus on the implementation process, including the decision-making during the implementation, the motive and objective of the implementation, and the appraisal of the effectiveness of the ISMS implementation. There is no study examining the financial performance after the adoption.

2.2. Value of certification

In order to have a better understanding of the relation between certification adoption and performance, we review the literature to see how existing studies addressed ISO certification, the ISO 9001 certification in particular, on the outcome of the certification. We focus on ISO 9001 studies for two main reasons. First, the ISO 9001 standard is very similar to ISO 27001. For instance, they are both standards on management systems. They are all based on related managerial concepts, such as continuous improvement, and their certification approaches are nearly identical. Second, ISO 9001 is the mostly adopted ISO standards in practice, and also the mostly studied ISO standard by academic scholars. A simple search in EBSCO of ISO 9001 returned 543 results, while a search of ISO 27001 returned only 11. Though this does not reflect the actual numbers of the studies in the literature, it shows that ISO 9001 has drawn considerable attention among researchers. We believe that ISO 9001 studies can provide some insights in this related research area.

For example, Jeng [11] conducted an empirical study on Taiwanese ISO 9000 certification to investigate whether the efforts made in ISO 9000 implementation turns into performance improvement. The results showed that although not all managers expect ISO 9000 certification to be a major booster, ISO 9000 certification indeed performed in line with the original expectation by the adopting companies. Casadesús and Giménez [4] also conducted a study with similar approach with Spanish firms. They surveyed and received 288 valid responses from Spanish companied with either ISO 9001, 9002 or 9003 certification. The benefits were classified into two main categories: internal benefits, such as improvements on the procedures, or external benefits, such as improvements on the market or client relations. The findings indicated that 65% of the companies enjoyed both internal and external benefits from the adoption of ISO 9000-series certification.

Other studies also used financial measures such as operating performance or stock market returns to evaluate the performance of ISO 9000 certification.

For example, Simmons and White [12] hypothesized that ISO 9000 certification would increase profitability. Its conclusion was based on excessive sales and financial returns after the certification. In addition, Lima, Resende and Hasenclever [5] reported similar results based on Brazilian firms. It used financial report figures to investigate excessive performance in profitability after ISO 9001 certification. Their conclusion were confirmative, but suggested a deeper inspection, especially on efficiency after ISO 9000 adoption. Corbett, Montes-Sancho and Kirsch [13] analyzed efficiency and profitability of American firms with ISO 9000 certification. They argued that firms comply with ISO 9000 would be more efficient in their manufacturing process, in terms of lower defect costs. As the cost of defects would generally be accounted as cost of goods sold, it was used by the studies as the measurement for manufacturing efficiency. They also reported significant excess of performance in both efficiency and profitability. They concluded that ISO 9000 certification had a positive impact on the certified firm's performance.

In addition to operating performance, other studies focus on stock market returns as the measure of financial performance. Hendricks and Singhal [14] showed that after the announcement of Total Quality Management (TQM) award, the stock market reacted positively especially for larger firms. Docking and Dowen [15] also showed a positive stock market reaction after ISO 9000 certification. Both studies contended that ISO 9000 brought confidence to and drew attentions from the potential market investors. The empirical evidence further showed that an ISO standard might be posed as a signaling tool.

As discussed, studies focused on the financial performance of ISO 27001 adoption are very limited. Drawing from the prior studies on ISO 9001, we would like to examine if ISO 27001 brings positive benefits on firm performance.

2.3. Financial performance

Financial performance directly reflects a firm's overall performance. Any improvement either originated internally or externally may contribute to a positive impact on the firm's financial performance. For example, a better quality control system will be able to lower defect rates, which may lead to an increase in the firm's gross income, since the cost of defects is lowered [16]. On the other hand, if a firm gains an improvement that have external effects, such as a quality award, its potential customers will have a higher confidence in the firm and will be more willing to buy the firm's product or service due to its better reputation [3]. This will result in more sales or service revenues to the firm and better financial performance.

In our context, we focus on the advantages a certification may bring, such as increased customer confidence or investor preference, which can be directly contributed by the certification. In addition, it is impractical to focus on cost reduction in the context of information security. Studies on ISO 9000 expect that the quality management system can improve production processes, thus decrease the cost of defects. In our context, we expect that an ISMS based on ISO 27001 can decrease the cost of security breaches and IT breakdowns. However, unlike the manufacturing production scheme that production costs are incurred in a regular and systematic manner, IT breaches are highly independent from one to another. This makes it inappropriate to value all IT breaches and malfunctions in the same way. Individual inspection and investigation would be necessary. Thus, our first hypothesis focuses on the increase of revenues instead of the reduction of costs. Formally,

Hypothesis 1: ISO 27001 Certification is positively associated with the certified firm's financial performance.

As mentioned earlier, certification can also work as a signaling tool that reflects the management's perception of the firm's certified field and shows the excellence of an entity on its corresponding certified field. Prior studies showed that stock market reacts positively to favorable information [17, 18]. In our context, we believe that the announcement of ISO 27001 certification will result in a positive stock market reaction as ISO 27001 certification may increase investors' confidence in the reliability of the information provided by the firm and the continuity or the reputation of the firm in the future. Specifically,

Hypothesis 2: ISO 27001 Certification is positively associated with a firm's stock market performance.

3. Research methodology

In this section, we discuss our sample and measures of firm performance. Specifically, we collect a list of firms with and without ISO 27001 certificates. By comparing the firm performance between these two groups, we investigate how ISO 27001 certificate is associated with firm performance.

3.1. Measures of firm performance

We considered two different measures of firm performance as discussed in our hypotheses: one is accounting-based, and the other is market-based. As stated in Hypothesis 1, we expected ISO 27001

contributes to firm performance through higher sales or service revenues. Accordingly, the first measure we used was return on assets (ROA), which was defined as operating income divided by total assets.

The second measure was market-based. We considered the buy-and-hold abnormal returns (BHAR). Buy and hold abnormal return (BHAR) is widely used in prior studies and can be used when the announcement dates are unclear. Since the adoption of ISO 27001 does not have a clear date and does not seem to draw immediate market reactions, we believe BHAR is the appropriate measure for our study and provide a long-term (e.g., one year or three years) performance measure. BHAR was calculated by the differences of the buy-and-hold returns between firms with and without ISO 27001 certificate. BHAR for firm i for period t from 1 to n is defined as:

$$BHAR_{in} = \prod_{t=1}^{n}\left(1+R_{it}\right) - \prod_{t=1}^{n}\left(1+E\left(R_{it}\right)\right) \qquad (1)$$

where R_{it} is the actual market return for firm i at period t, and $E(R_{it})$ is the expected market return for firm i at period t.

3.2. Firms with and without ISO 27001 certificates

Our initial sample consisted of a list of firms with ISO 27001 certificates in the United Kingdom, the United States, Germany and Spain. We focused on these four countries because they were the top four countries with the most ISO 27001 certified companies in the world as given on iso27001certificates.com. Note that the name of the registrant of ISO 27001 certificate may represent a site, an organization or a business entity. A site can be a business entity or an organization. It can also be one office, facility, or operational unit of a company. That is, depending on the extent of the certification, the registrant can range from a local office to a whole company. In addition, the information provided on the website is based on the location of the certified site. For example, a certified office or operation unit in the United Kingdom would be categorized into the UK regardless the origin of the organization, which may be a foreign company outside the UK. In order to make sure that our sample captures the certification of the whole company and only includes publicly-traded company, we manually examined the scope of each certification and determined whether the company was publicly-traded. We found that most of the certificated companies were privately-held or non-for-profits organizations. This sampling characteristic was very different from that in the studies of ISO 9000 which dramatically decreased the size of valid samples. We also collected the certification announcement dates. In order to verify the dates on the website mentioned earlier, we manually checked all the dates, if any, from the detailed information provided by the certification registrars, the information on the registrants' websites and/or the press releases. Firms without clear certification dates were excluded from our study. Our resulting sample consisted of 25 firms in Europe and U.S.

Next, we formed a list of control firms which did not have experience in adopting ISO 27001 certificate. In particular, we first constructed a list of candidate control firms consisting of all firms from Compustat. Then we performed the match based on pre-certification performance and firm size for firms in the same industry (two-digit SIC code). Our matching was based on the respective criteria at the beginning of t-2 year (i.e., two years before) where t is the year when the firm was ISO 27001 certified. In this vein, when the performance measure is ROA, we used (1) total assets, (2) ROA and (3) total assets-ROA combined as the matching criteria. That is, any firm within the 50% to 200% range were considered to be a matched firm as in Corbett et al. (2005). We report all three sets of control firms in our results. For BHAR, we used market value of equity (MVE), which equals the total shares of common stock outstanding times the closing stock price within the 50% to 200% range. For the matching, we performed both one-to-one and portfolio matching.

3.3. Methodology

In order to test our hypotheses, we compared the ROA and the BHAR of the firms with and without ISO 27001 certificate from time t-2 to time t+2 (i.e., two years before and after the certification) where time t is the year when the firm is certified. Our statistical tests were based on the null hypotheses that the performance is in different between the certified firms and the non-certified firms.

4. Empirical results

Results of the comparison of ROA (the first hypothesis) are presented in Table 1 through Table 4. Each table provides the results based on t-test or Wilcoxon rank test. We also demonstrate the results based on the one-to-one matching or the portfolio matching. In each table, we present the results under three matching criteria in five periods. Again, year t is the year when the firm gained ISO 27001 accreditation. All the values in the tables are p-values showing the significance of the tests. For example, Table 1 shows the results based on one-to-one matching and t-test. In Table 1, the first cell shows 0.9914 which is at time t-2

and the matching criteria is total assets. That is, 0.9914 is the *p*-value of the *t*-test between the mean ROA at time *t*-2 of the certified firms and the mean ROA at time *t*-2 of the non-certified firms, which were determined by a one-to-one matching on total assets. As shown in Table 1 to Table 4, none of the results are significant. The non-significance of our test has failed to reject our null hypothesis that the mean ROA differences are zero. That is, we do not observe statistical evidence of ISO 27001 accreditation on a firms operating performance, which is inconsistent with our first hypothesis.

Table 1. Results based on *t*-test and one-to-one matching for ROA

Matching Criteria	*t*-2	*t*-1	*t*	*t*+1	*t*+2
(1)	0.991	0.926	0.909	0.672	0.903
(2)	0.976	0.794	0.651	0.922	0.133
(3)	0.914	0.109	0.926	0.170	0.779

Table 2. Results based on *t*-test and portfolio matching for ROA

Matching Criteria	*t*-2	*t*-1	*t*	*t*+1	*t*+2
(1)	0.393	0.554	0.922	0.446	0.808
(2)	0.432	0.537	0.664	0.572	0.384
(3)	0.215	0.553	0.594	0.480	0.579

Table 3. Results based on the Wilcoxon rank test and one-to-one matching for ROA

Matching Criteria	*t*-2	*t*-1	*t*	*t*+1	*t*+2
(1)	0.546	0.854	0.729	0.671	0.734
(2)	0.768	0.803	0.579	0.987	0.182
(3)	0.725	0.270	0.725	0.388	0.541

Table 4. Results based on the Wilcoxon rank test and portfolio matching for ROA

Matching Criteria	*t*-2	*t*-1	*t*	*t*+1	*t*+2
(1)	0.602	0.496	0.837	0.498	0.626
(2)	0.695	0.452	0.328	0.782	0.352
(3)	0.334	0.516	0.658	0.582	0.854

Table 5 and Table 6 present the results for Hypothesis 2 (i.e., based on BHAR). In each table we show the result based on *t*-test and the Wilcoxon rank test. Again, the numbers are *p*-values. The results also show that there is not significant different BHAR between certified firms and non-certified firms which is different from our expectation in Hypothesis 2.

Table 5. Results based on buy-and-hold abnormal returns and one-to-one matching

Student t-test	0.1997
Rank Test	0.5000

Table 6. Results based on buy-and-hold abnormal returns and portfolio matching

Student t-test	0.3522
Rank Test	0.6257

Although the results are not consistent with our hypotheses, we found the results very interesting in multiple aspects. First, we would like to highlight the nature of the ISO 27001 certification for possible explanations regarding why it brings no advantages in terms of financial and stock market performance. As indicated in the literature review section, most studies showed that ISO 9000 consistently makes positive contributions to the firm's financial performance and stock market value. Originally, we anticipated that by sharing the similar management concept, ISO 27001 should present similar financial performance as what was found in the case of ISO 9000 adoption. However, our results did not offer empirical support to this hypothesis. We consider that it might be related to the context of information systems. The nature of ISO 9000 is about quality management, which is based on the Total Quality Management (TQM). The goal of such management is to continuously improve the quality of the products and production processes in order to achieve customers' satisfactory. ISO 27001, on the other hand, is more about "prevent loss through management," which is very different from ISO 9000. The design of the management system is based on a risk-based approach. The approach is to identify, control, and treat the risks that exist in the organization's IT environment. Minimization of the effects that the risks might potentially bring, along with the continuous improvement to ensure the survivability of the organization, is the goal of the standard. That is, ISO 9000 is aimed at quality improvement to meet customer satisfactory, which implies better competitive advantage, while ISO 27001 takes a total defensive role that protects the organization from the negative impacts associated with potential IT failures or breaches. A successful information security implementation would be seen as what the organization should do, as an obligation, while a successful quality management system that helps make products of superior quality is definitely an advantage. Thus, an ISO 27001 certification would only be seen as "meeting the requirement," instead of a competitive

advantage. This would explain why there is no reaction from the market toward the certification.

Another reason might be the scope of the certification. When we conducted a detailed review of each awarded ISO 27001 certificate, we found that many firms did not apply for the certificate at firm level. Instead, most of the firms only held a certificate that covers part of the organization, for example, a business unit or a facility. However, it is best to manage the risks at the organizational level. Enterprise Risk Management (ERM) is a risk management framework that helps enterprises to develop strategies to protect themselves from undesirable impact brought by all kinds of risks. The most common version of ERM is introduced by COSO (Committee of Sponsoring Organizations of the Treadway Commission) in 2004. It is an expansion on common internal control concepts, aimed to provide guidance on enterprise-level risk management that helps protect the enterprise. COSO's ERM framework consists of eight major components, starting from understanding the environment, through risk identification, assessment and treatments, and finishing with monitoring the ongoing activities (COSO 2004). This approach is nearly identical to what ISO 27001 requires, but focuses on the enterprise level. As ERM has become a popular framework in the context of risk management, people might take a non-organization-level ISO 27001 certification as a limited risk management commitment. We believe that a full-scope certification can be more convincing and conveys a more secure image to the customers or investors.

5. Conclusion

This study provides an overview of the impact of ISO 27001 certification on firm performance. As information security becomes a public concern, this research investigates whether a certification on information security management system (ISMS) would benefit the certified firms through competitive advantages. Though there are many studies regarding the adoption of other certificates, such as ISO 9000, we are not aware of any study of ISO 27001 regarding the performance after the adoption. We believe that the nature of ISO 27001 certification results in the insignificant findings as ISO 27001 is more an obligation instead of a competitive advantage. In addition, the scope of the certification is also a concern, since most of our sample firms only have a partial coverage of certification, instead of having certified at the organizational level.

The main limitation of this research is the number of available certified firms. Though there are more than thousands of ISO 27001 certificates around the world, not all the certified firms have publicly available financial information. In this case, we are not able to the information necessary for our analyses.

Given the potential benefits and costs associated with ISO 27001, our empirical investigation is a starting point to examine the financial returns resulting from ISO 27001 certification. We believe that much more empirical evidence through reviewing, surveying, and interviewing key decision makers in the firms about the ISO 27001 adoption as well as certificate registrar or consultants would greatly expand the magnitude of this study.

6. References

[1] Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", Journal of Computer Security, 11(3), 2003, pp. 431.

[2] Goel, S., and H. A. Shawky, "Estimating the Market Impact of Security Breach Announcements on Firm Values", Information & Management, 46(7), 2009, pp. 404-410.

[3] Terlaak, A., and A. A. King, "The Effect of Certification with the ISO 9000 Quality Management Standard: A Signaling Approach", Journal of Economic Behavior & Organization, 60(4), 2006, pp. 579-602.

[4] Casadesús, M., and G. Giménez, "The Benefits of the Implementation of the ISO 9000 Standard: Empirical Research in 288 Spanish Companies", The TQM Magazine, 12(6), 2000, pp. 432 - 441.

[5] Lima, M. A. M., M. Resende, and L. Hasenclever, "Quality Certification and Performance of Brazilian Firms: An Empirical Study", International Journal of Production Economics, 66(2), 2000, pp. 143-147.

[6] Calder, A., Information Security Based on ISO 27001/ISO 17799: A Management Guide, Van Haren Publishing, 2006.

[7] Ku, C.-Y., Y.-W. Chang, and D. C. Yen, "National Information Security Policy and Its Implementation: A Case Study in Taiwan", Telecommunications Policy, 33(7), 2009, pp. 371-384.

[8] Boehmer, W., "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001", in Proceedings of the International Conference on Availability, Reliability, and Security, Fukuoka, Japan, 2009, pp. 392-399.

[9] Hsu, C. W., "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization", European Journal of Information Systems, 18(2), 2009, pp. 140-150.

[10] Boehmer, W., "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001", in Proceedings of the Second International Conference on Emerging Security Information, Systems, and Technologies, Cap Esterel, 2008, pp. 224-231.

[11] Jeng, Y.-C., "Performance Evaluation of ISO 9000 Registered Companies in Taiwan", The TQM Magazine, 10(2), 1998, pp. 132 - 138.
[12] Simmons, B. L., and M. A. White, "The Relationship between ISO 9000 and Business Performance: Does Registration Really Matter?", Journal of Managerial Issues, 11(3), 1999, pp. 330.
[13] Corbett, C. J., M. J. Montes-Sancho, and D. A. Kirsch, "The Financial Impact of ISO 9000 Certification in the United States: An Empirical Analysis", Management Science, 51(7), 2005, pp. 1046-1059.
[14] Hendricks, K. B., and V. R. Singhal, "Quality Awards and the Market Value of the Firm: An Empirical Investigation", Management Science, 42(3), 1996, pp. 415-436.
[15] Docking, D. S., and R. J. Dowen, "Market Interpretation of ISO 9000 Registration", Journal of Financial Research, 22(2), 1999, pp. 147.
[16] Terziovski, M., D. Power, and A. S. Sohal, "The Longitudinal Effects of the ISO 9000 Certification Process on Business Performance", European Journal of Operational Research, 146(3), 2003, pp. 580.
[17] Foster, G., "Stock Market Reaction to Estimates of Earnings Per Share by Company Officials", Journal of Accounting Research, 11(1), 1973, pp. 25-37.
[18] Woolridge, J. R., and C. C. Snow, "Stock Market Reaction to Strategic Investment Decisions", Strategic Management Journal, 11(5), 1990, pp. 353-363.