國立臺灣大學管理學院資訊管理研究所

碩士論文

Department of Information Management

College of Management

National Taiwan University

Master Thesis

ISO 27001 認證對於企業績效之影響

The Impact of ISO 27001 Certification on Firm Performance

呂昂

Ang Lu

指導教授：許瑋元 博士

Advisor: Wei-Yuan Hsu, Ph.D.

中華民國 101 年 6 月

June 2012

ABSTRACT

In the recent years, information security has become a household name and gained enormous public attention. The extensive use and dependence on information technology (IT) of businesses and organizations, along with worsening impact that IT incidents brings has made information security one of the top concerns of the management. Moreover, individual awareness of information security would require corporations to invest and highlight their efforts in securing their handling of information to gain customer confidence. However, the extensive use of IT has made information security a complicated management issue at corporate level. The guidance of an information security management would be urgently in need. ISO 27001 standard provides guidance to a sound information security management system (ISMS). The certification of ISO 27001 further shows compliance and excellence in it. As the costs incurred during the implementation and accreditation are considerable, we would like to discover whether the certification benefits financially by acting as a competitive advantage. We took the event study methodology with samples from United States and selected European countries to investigate the impact after certification. In the results, we have found no evidence that ISO 27001 certification brings positive impact in terms of financial and stock market performance. We attribute the results to the nature of ISO 27001 that a good information security management would bee seen as an obligation, or "meeting the requirements", instead of a competitive advantage. We also took the scope of the certification as an explanation, where most of the certification only covers part of the organization, instead of a full-scope. This would be seen as a compromised commitment in information security.

Keywords: Information security, ISO 27001, ISMS, event study.

摘要

近來，資訊安全成為了家喻戶曉的重要議題。由於企業及組織對於資訊科技的使用及依賴日益增加，以及資訊安全事件對於組織帶來的負面衝擊愈加嚴重，資訊安全已經成為管理階層最為重要的考量議題之一。另一方面，由於個人對於資訊安全的意識逐漸提昇，企業必須有效提昇其資訊安全的品質以增進消費者信心。然而，隨著資訊科技在組織中的角色轉變，資訊安全已經由單純的技術議題，轉變為企業層級的管理議題。一套建立良好資訊安全管理的有效辦法，是目前企業至為需要的。ISO 27001 資訊安全標準提供了一套建立資訊安全管理系統的規範及指引。ISO 27001 資訊安全認證更進一步展示了企業在資訊安全方面的規範遵循以及優越性。然而 ISO 27001 資訊安全認證的成本極高，我們想要了解究竟此認證是否可以作為一個競爭優勢，帶給企業正向的財務方面績效。我們採用了事件研究法，針對美國以及部分歐洲國家的公司進行研究分析。我們發現無論是以財務績效衡量，或者是以股票市場績效衡量，ISO 27001 並未對認證公司帶來任何的正面衝擊。我們將這個結果歸因於 ISO 27001 的本質，即良好的資訊安全管理可能會被視為公司的責任與義務，而非競爭優勢。另一方面，我們發現大部分的樣本公司，其認證都只涵蓋了部分營業單位或廠房設施，而非整體公司的認證。這可能會被視為不盡完善的資訊安全管理規劃。

關鍵字： 資訊安全，ISO 27001，資訊安全管理系統，事件研究。

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION 1

1.1 Research Motivation 1

1.2 Research Objective 5

CHAPTER 2. LITERATURE REVIEW 7

2.1 Research Background 7

2.1.1 ISO 27001 Standard And Certification 7

2.1.2 ISO 27001 Research 10

2.1.3 IT Investment Research 12

2.1.4 ISO 9001 Certification Research 15

2.2 Hypotheses Development 19

2.2.1 Financial Approach 19

2.2.2 Market Approach 21

CHAPTER 3. RESEARCH METHODOLOGY 22

3.1 Event Study 22

3.2 Event Study on Operating Performance 24

3.3 Event Study on Stock Market Return 27

3.4 Samples 29

3.5 Control Firms 32

3.5.1 Matching Criteria for Operating Performance 32

3.5.2 Matching Criteria for Stock Market Performance 33

3.6 Statistical Test 35

CHAPTER 4. RESULTS AND ANALYSIS 37

4.1 Results 37

4.2 Analysis 42

CHAPTER 5. CONCLUSION 45

5.1 Conclusion 45

5.2 Limitations 46

5.3 Future Research 47

REFERENCE 48

LIST OF TABLES

Table 2.1 Summary of IT Investment Studies 14

Table 2.2 Summary of ISO 9001 Studies 18

Table 4.1 Student's t-test result, one-to-one matching 39

Table 4.2 Student's t-test result, portfolio matching.....39

Table 4.3 Wilcoxon signed-rank test result, one-to-one matching.....40

Table 4.4 Wilcoxon signed-rank test result, portfolio matching.....40

Table 4.5 Buy-and-Hold Abnormal Return, one-to-one matching 41

Table 4.6 Buy-and-Hold Abnormal Return, portfolio matching.....41

Chapter 1. Introduction

1.1 Research Motivation

In the recent years, information security has become a household name and gained enormous public attention. The ubiquity of information technology (IT) accompanied by real-world security breaches such as hacking, intrusion, and identity theft has help spread the idea that information security is somewhat important. And with much more extensive use and heavier dependence on IT, firms and organizations are now highly concerned about the impact brought by IT incidents and breaches. According to a recent survey, the number of IT breaches incidents taken place each year are arising, for example, 20% in the year 2010 (PwC, 2010). Moreover, incidents caused by IT failures are bringing more impact to an organization than they used to. Recent survey also showed that the loss incurred from information security breaches are intensifying. Organizations are spending more resources in response to information security incidents. Total loss incurred in a single security incident, including direct financial loss, reputational loss, and business disruption is becoming more severe. In addition, stock market will also have significant negative reaction towards IT incidences and breaches (Campbell et al., 2003; Goel & Shawky, 2009).

The arising concern on information security reflects the subtle yet radical change of role that information technology plays in an organization. Since business nowadays relies much heavier on IT for its day-to-day operation, IT has transformed from a supporting character to a must-have fundamental for organizations. As information technology becomes ubiquitous and essential to all kinds of business today, it is suggested that the management should now put more emphasis on managing the risk IT component creates

than focusing on its utilization for more competitive advantage (Carr, 2003). Because of this nature, an IT incident might now pose much greater threat to much greater extent, sometimes even a matter of business survivability.

Meanwhile, the way information is processed and stored has changed radically due to a new form of business ecosystems. As internet-based, or "cloud" based services grew rapidly and drew huge market attention, sensitive information is no longer sealed within its owner; confidential information is now sometimes stored or processed in an external service provider. For example, there are Software-as-a-service (SaaS) providers that run cloud-based CRM or ERP systems for their customers. These services are usually aimed at enterprise or business customers. No doubt the information that CRM or ERP processes is highly confidential. Information security will have its role even more respected in two aspects from this radical change: first, the customers, or the buyers, will concern more about information security. Since they are having important and confidential information processed externally, they would like their service provider to be capable of handling their information appropriately. On the other hand, from the service provider's perspective, they would emphasize on information security even more, since an insecure IT could cause a catastrophic damage to its reputation. Moreover, a security breach in one service provider can cause leakage to all customers being served. Not only the reputation will be damaged, considerable monetary losses and extensive legal issues are also expected.

Moreover, the fear of leaking private information does not only worries enterprises and business organizations, but also individuals. The public is now highly aware of individual privacy issues, such as identity theft. End-users would be more careful in terms of privacy when they are engaging a transaction with other entities. For example,

a user buying merchandise online will now care more about how his or her credit card information is handled, or a potential credit card fraud may take place and cause losses. Recent security breaches on well-known internet-based services have raised this public awareness. The settlement of such breaches is very costly, which includes compensation for the victims, and for most of the time, a considerable amount of penalty imposed by governments. On the other hand, the loss caused from leaking information might not only be financial or reputational loss, but even legal obligations. The legislators around the world are now highly aware of privacy issues, and privacy-related laws are enacted in several countries. These laws usually hold service-providing businesses responsible for the loss that incurs from failing to keep their customers' information confident. There is also regulatory pressure that drives firms to take action to improve their information security. For example, the Sarbanes-Oxley Act of 2002, or SOX, requires firms to assess its internal control on a regular basis, and require it to be external audited. As IT played an important part in nearly all business cycles today, information security will be a key component in this assessment (Schultz, 2004).

As we can see, information security has become a major concern for everyone in the recent days. In the discussions above, we have not only presented the extensiveness that information security makes impact, but also the complication that handling information security has to be today. Generally, information security has mostly been defined as CIA – confidentiality, integrity, and availability. While in the old days, these characteristics of information security can be well achieved in mere technical ways – encrypted communications, backup systems and supplementary power supplies – they no longer suffice in today's environment. Organizations today handle much more information than they used to. As the flow of information processing have been

extended to every corner of the organization, the substantial involvement and usage from non-IT personnel into an organization's IT function has made Information security transformed from an IT focused issue to a business management issue (von Solms, 2000). Besides, information is not meant to be sealed inside a safe deposit box. Information creates value for organizations if appropriate used, including reasonable sharing with other organizations (Ashenden, 2008). The way to treat information is not to simply confine them from disclosure; a well-planned usage of information under adequate control that prevents undesirable risks is the one of the goals of information security management today.

As a summary, information security has changed from a technical, independent issue to an organization-wise management issue. And the public awareness of information security has made it one of the top concerns for the organizations. Information security management is without doubt one field that organizations need to invest heavy attention and resources to survive in the world today.

1.2 Research Objective

As we discussed above, information security is without doubt a vital issue to organizations. Yet, information security has become much more complicated due to the essentiality of IT in an organization and the extensive usage throughout the organization. IT is virtually involved with every business functions. While general firms are no experts in this area, an explicit guideline that suits all firms will be very helpful. On the other hand, securing itself is maybe not enough. Customers have no way to understand how secure a firm is. After all the effort firms have made to strengthen their information security, they would like to demonstrate it to gain customer attention and confidence. Standards and certification serves as a great tool to achieve these two goals. Standard provides a direct and explicit guideline for organizations to follow. After following the standard, there usually exists a companion certification that assesses whether the implementation complies with the standard. Since certification is issued by an independent and widely-trusted agency, it works as a great demonstration to the public.

The standard for information security is ISO 27001, which has become very popular and is seeing steady growth in adoption. First emerged in 1995 as BS-7799, and further revised in 2005, the ISO 27001 is a standard that defines a set of principles about the implementation of an appropriate information security management system, or ISMS. We will provide a detailed overview on ISO 27001 standard and certification in the later chapter. ISO 27001 has already become the widely regarded standard for information security. Along with the escalating public awareness of information security, organizations' adoption of ISO 27001 standard is also seeing a steady growth. As mentioned above, IT itself may no longer bring any competitive advantage. But demonstrating a secure and appropriately managed IT might do. A certification of

compliance to the ISO 27001 standard might well serve as an ideal demonstration, or a "signaling tool" (Terlaak & King, 2006) to the public, showing that the information processing of an organization complies with the security standard, and is thus more reliable and trust-worthy. However, acquiring a certification is usually money and time costing. An organization usually needs to pay a substantial amount to its consultant and registrar. Extensive paperwork and documentation are also required. Thus, measuring the payback of the certification would be a very interesting topic to investigate. The exact answer to this question might provide critical strategic value in further decision making for top management on certification adoption. However, this question might not be directly answered. But investigating how ISO 27001 certification is working for organizations in certain terms still helps us to get an idea of the whole.

This study will be aimed at investigating whether ISO 27001 certification brings benefit to an organization in a financial term. Financial figures, usually figures fetched from financial statements or stock market, are sometimes the easiest way to understand the status or performance of a business. Also, as the compilation of the financial statements must comply with the accounting standards and must be audited by accountants before release, it is a reliable source of information that could be trusted. It serves as an excellent measurement for this topic.

In the following chapters, this study will first present a literature review, a development of theories, the data and methodology used in this analysis, and the results, related discussion, and conclusions.

Chapter 2. Literature Review

2.1 Research Background

2.1.1 ISO 27001 Standard And Certification

We first present an overview on 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 ISO in October 2005. It belongs to the ISO 27000 family of standards. ISO 27000 is a growing series of information security standards rooted in earlier information security standard efforts. For example, ISO 27002, a guideline and code-of-practice on ISMS implementation, is a complementary standard to ISO 27001. ISO 27002 is formerly called ISO 17799, which is evolved from BS 7799 Part 1. There are also some developing standards, such as ISO 27005 on information security risk management, detailing the risk management approach taken by ISO 27001.

The ISO 27001 standard provides a specification for Information Security Management System, or ISMS. Officially, ISO 27001 define ISMS as "a management system that carryout the establishment, operation, maintenance, monitor, and continuous improvement of information security" (Calder, 2006). The goal of ISMS is to provide a sound management with explicit policies that effectively put processes and business functions under reasonable control in terms of information security. It can be viewed as a counterpart of ISO 9001's quality management system, only focusing on different topic and having some different approaches. ISO 27001's ISMS contains a set of policy that defines the control strategies and control objectives. As business functions and processes are connected to each other, the information security policy can't be defined

independently. The controls or policies of ISO 27001's ISMS are not disjointed, but rather interrelated to each other. The policies require a commitment from the management to ensure its effectiveness, and are to be carried out within the entire ISMS coverage.

The establishment of the policies of ISMS is based on a risk management approach. The definition of policies will be started by understanding the environment of the business, evaluating the resources and processes, in order to identify the risks to information security that might take place. After the risk identification, the firm would assess each of the risks, evaluate their impact, and then come up with the strategies that treat the risks in a reasonable manner. The steps above require extensive involvement of the management as well as the employees that actually carry out the operations. As the environment and the business processes differ from organization to organization, the risk identified and the strategy developed to treat against would also differ. That is, the ISO 27001 standard provides the requirement and specification to an ISMS implementation, but the ISMS is tailored for every ISO 27001 adopters according to their situation.

Meanwhile, ISO 27001 also adopted the Plan-Do-Check-Act (PDCA) cycle of continuous improvement. After the initial policies are defined, the firm constantly review and adjust the established policies if needed. Also, as new risks might rise in the changing business environment and business functions, new policies are also defined in response to them. The PDCA cycle help the ISMS stay vigorous and effective.

Finally, an ISO 27001 certification can be acquired by having an external auditor to examine the implementation of ISMS. As we mentioned, the certification helps showing

the information security management system is ISO 27001 compliant. To acquire a certification, organizations need to go under an auditing process conducted by an accredited external certification body. Then, the certification will be honored, usually with a three-year validity (Calder, 2006). The certification requires follow-up review, or renewal, on a regular basis.

2.1.2 ISO 27001 Research

We now look at the literature to understand how existing studies have addressed the topic of implementation outcome of ISO 27001. We found that the majority of current ISO 27001 researches focus on the implementation process, including the decision-making during implementation, the motive and objective of implementation, and the appraisal of effectiveness of the ISMS implementation.

Tong et al. (2003) demonstrated an implementation process of BS 7799, the predecessor of ISO 27001, of a picture archiving and communication system (PACS) majorly for clinical use. It showed a step-by-step preparation, design and documentation of the implementation process. It discussed the benefit that BS 7799 brings. Ku et al. (2009) also analyzed the key factors of successful ISMS implementation based on BS 7799. Boehmer (2009) discussed that how management should make decisions about selecting appropriate controls while implementing ISO 27001, and examined their approach based on case studies. Hsu (2009) discussed about the behavior of different social groups involved in the ISO 27001 implementation process. The main concept of this study is that the behavior of an individual is affected by what one experiences, how one perceived and how one interpreted. Based on a case study conducted in Taiwan, it separates the individuals into different groups to see their understandings and behaviors. It demonstrates how different roles hold different ideas and take different actions during the implementation period in detail.

As we are majorly focusing on the outcome of acquisition of ISO 27001 certification, literatures on the outcome of the certification or its predecessors are reviewed in the first place. We found that among the studies that are ISO 27001 related, we can hardly

find one that has taken our desired approach. Most of the studies are concerned about the management issues during the ISO 27001 implementation process or decision-making, rather than delivering an appraisal of the outcome after the implementation process is done.

We also reviewed other approaches of ISO 27001 studies. For example, Boehmer (2008) evaluates the efficiency and effectiveness of ISMS (Information System Management System) implementation based on ISO 27001 using KPIs (Key Performance Indicators) as the measurement. It developed KPIs with a quantitative approach for efficiency and effectiveness. They concluded that these KPI of these two dimensions are a trade-off. However, these researches are aimed at the successfulness of an ISMS implementation. Our goal is to see whether ISO 27001 implementation brings benefit to an organization. We can conclude that there exists no study examining the financial value after the ISO 27001 implementation.

2.1.3 IT Investment Research

Due to the very limited amount of existing ISO 27001 researches on the outcome, we now turn to see how similar topics are evaluated. As we discussed in the previous chapter, we would like to investigate that does ISO 27001 benefit after all the tremendous costs and efforts by bringing competitive advantage. One very similar topic that has been extensively reviewed is the outcome of an IT investment. In fact, we can view the acquisition of ISO 27001 certification as an IT-related investment. We then turn to the topic of IT investment.

The studies of the outcome of an IT investment are usually based on its announcement. Most of the studies investigate the improvements in performance after the IT investment announcement. Weill (1992) conducted an empirical study based on financial performances. They found that IT investment brings positive impact to firm profitability, also brings sales and productivity growth. These improvements are made from two aspects: internal improvements, and external advantages. As new IT systems are adopted, effectiveness and efficiency are enhanced. These improvements lowered costs and brought up productivity. On the other hand, as IT investments are made known to the public, the firm would gain attention and confidence from potential customers. These reputational improvements contribute directly in sales.

Dos Santos et al. (1993) examined the impact that IT investment announcements make in terms of firm's market value. By conducting an event study, it is aimed to compare how firms with IT investment announcements perform in stock market against the ones that do not. It concluded that in general, IT investment announcements do not bring any significant improvement. But interestingly, if further distinguishing the investments into

innovative and non-innovative (follow-up) ones, thy found out that innovative IT investments do increase the market value of the firm. Similarly, Im et al. (2001) and Chai et al. (2011) also assess the impact that IT investment brings. Again, based on stock market performance evidences, they have similar conclusion that after IT investment are announced, firms will gain significant improvements in stock market return. They attribute this improvement to the investors' confidence. As IT investment are announced, potential investor may be more interested in the firm's stock, as performance and profitability are expected to be improved. Generally, a rational investor would be more likely to purchase stock of a firm if the firm would perform better. An improving firm would be more likely to have a higher profit, and then the stock price.

Lastly, Anderson et al. (2003) investigated the relation between IT spending and the future earnings. They analyzed the impact of the IT spending on the return of the firm, which is measured by return on assets (ROA), which is defined as the ratio of net income to total assets. They further decomposed ROA into two parts: profit margin and assets turnover. The former indicates the profitability on each items sold, where any improvement can be contributed by lower costs from better process, or higher sales price. The latter indicates the efficiency of asset usage. That is, how many times of sales does one unit of asset produces. They found that IT spending is positively related to future earnings, especially to profit margin. This indicates that IT spending announcements help firms gain improvements in by cost recovery more than asset utilization.

As we have seen, there are many existing studies that focused on IT investments and its impact to organizations in terms of financial performance improvements and stock

market return increases. We have suggested that ISO 27001 can be seen as an IT-related investment, and the methodologies used on IT investment studies are very applicable to ISO 27001, since they are both based on an announce or advent of an IT-related event. We believe that a similar methodology can be applied to the context of ISO 27001 information security standard.

Author	Hypotheses	Methodology	Findings
Chai et al. (2011)	IT investment leads to abnormal stock returns	Event study (Stock Return)	Supportive
Anderson (2003)	IT spending announcement leads to positive buy-and-hold portfolio return	Event study (Stock Return)	Supportive
Im et al. (2001)	Trading volume will positively react to IT investment announcement; Stock price will react more positively to smaller firm size, to financial industry than to manufacturing firms	Event study (Stock Return)	Supportive; no price reaction to larger firms
Dos Santos et al. (1993)	IT investment announcement brings positive stock market reaction	Event study (Stock Return)	Supportive; Zero NPV for non-innovative investments
Weill (1992)	IT investment has positive impact on ROA, sales growth, and productivity	Event study (Operating Performance)	Significant for IT transactional investments

Table 2.1

Summary of IT Investment Studies

2.1.4 ISO 9001 Certification Research

We then look at the literature to see how existing researches have addressed another ISO certification, the ISO 9001 certification, on the outcome of the implementation and certification. We reviewed and present the ISO 9001 studies for majorly two reasons. First, the ISO 9001 standard has multiple similarities to ISO 27001. To name a few, they are both standards on management systems, they are all based on very similar managerial concepts such as continuous improvement, and their certification approaches are nearly identical. We have detailed the similarity of the two standards in the previous chapter. We believe that with the similar nature of the two standards, a comparison of studies towards them can be considered fair and appropriate. Second, ISO 9001 is the mostly adopted ISO standards, and also the mostly studied ISO standard. 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. This fact along with the longer history of ISO 9001 standard made its studies more sophisticated. We believe that ISO 9001 studies can provided an ideal study approach toward an ISO standard.

We now present a review on studies of ISO 9001 implementation outcome. There are basically two types of studies in this field. One type is based on questionnaires, where the assessment of the outcome is based on responses from the management of sample certified firms. Then, appropriate statistical methods, basically regressions, are applied to the responses received to understand the general idea of the management's assessment of an ISO 9001 implementation.

For exmple, Jeng (1998) conducted an empirical study on Taiwanese ISO 9000 certification to investigate whether the efforts made in ISO 9000 implementation turns into performance improvement. Their analysis is based on a questionnaire of 40 elements, divided into 6 major sections of the defined performance indication. There results are appraised by a discriminant analysis based on linear regression. They found that although not all managers expect ISO 9001 certification as a major booster, ISO 9000 certification made contributions to perform in line with original expectation.

Casadesus & Gimenez (2000) also conducted a study with similar approach on Spanish firms. They surveyed and received 288 valid responses from Spanish companied with either ISO 9001, 9002 or 9003 certification. They asked for their self-assessment of benefits received from acquirement of the certification. The benefits are 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. They reported that 65% of the companies enjoyed both external and external benefits from adoption of ISO 9000-series certification.

The other type of study uses financial figures as their research material. Interestingly, these approaches are nearly identical to those reviewed in our previous IT investment section. Instead of having any responses from the management, they collect financial data, such as financial figures or stock prices as the measurement of the performance. As ISO 9001 certification is also an individual event, the methodology widely adopted in the previous section, event study, is also seeing extensive use in the following review.

For example, Simmons & White (1999) hypothesized that ISO 9001 certification would increase profitability. A similar approach as adopted in literatures discussed in the

previous chapter, event study, is utilized to examine the excess in performance after ISO 9000 adoption. Its conclusion is based on excessive sales and financial return after the certification. Lima et al. (2000) reported similar result 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 the efficiency after ISO 9000 adoption.

Corbett et al. (2005) analyzed efficiency and profitability of American firms with ISO 9001 certification. Since ISO 9001 is a quality management standard, firms comply with ISO 9001 would be more efficiency in their manufacturing process, in terms of lower defect costs. As the cost of defects would generally be accounted as cost of goods sold (COGS), it is used by the studies as the measurement for manufacture efficiency. Again, with ISO 9001 certification, firms would attract more customers. It would attract more sales. Return on assets, which is calculated as dividing total operating income by total assets, is taken as the measurement of profitability. They also adopted event study methods, and reported significant excess of performance in both efficiency and profitability. They conclude that ISO 9001 certification makes positive impact to firm's performance.

In addition to the measurement of operating performance, there are also studies focusing on stock market returns. Hendricks et al. (1996) studied on the impact that TQM award brings to a firm. It showed that after an announcement of TQM award, stock market would react positively, and the effect is especially significant for larger firms. The methodology it adopted are very similar to the ones adopted by researches aimed at IT investment. Docking & Dowen (1999) have similar findings that stock market return increases after ISO 9001 certification. Both researches are based on the same rationale

as the IT investment researches have, that ISO 9000 brings confidence to and draw attentions from the potential market investors. These empirical evidences have further showed that an ISO standard might well pose as a signaling tool that work as we expected.

We have seen so far that there is an apparent lack of studies focusing on the outcome of ISO 27001 certification, while studies in the same manner are frequently seen in the IT context (IT investments) and certification of other ISO standard (ISO 9001) using a nearly identical approach of research. We believe that the outcome of ISO 27001 can also be investigated in the same manner.

Author	Hypotheses	Methodology	Findings
Corbett (2005)	ISO 9001 increases ROA, Tobin's Q, Relative Sales, and decreases COGS	Event study (Operation Performance)	All supportive
Heras (2002)	ISO 9001 increases Sales, ROA	Event study (Operation Performance)	No significant improvement
Simmons et al. (1999)	ISO 9001 increases profitability	Event study (Operation Performance)	Supportive
Docking et al. (1999)	ISO 9001 brings positive market reaction	Event study (Stock Return)	Supportive
Hendricks et al. (1996)	ISO 9001 increases market stock return	Event study (Stock Return)	Supportive, especially for large firms

Table 2.2

Summary of ISO 9001 Studies

2.2 Hypotheses Development

As seen above, we now discovered that our desired approach of studying ISO 27001 is widely carried out in researched about other ISO certifications. Also, in the IT context, studying the outcome of IT investment is also popular. Similar studies focused on ISO 27001, however, is very limited, if not none. It would be very meaningful to conduct such a study at this point of time. As discussed in earlier chapters, we would like to examine if ISO 27001 brings positive impacts on firm performance. The following hypotheses are some different dimensions that we are interested in.

2.2.1 Financial Approach

Financial performance presents a firm's overall performance in a direct way. Any improvement, either originated internally or externally, can contribute to a positive impact in 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 (Terziovski et al., 2003). 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 (Terlaak & King, 2006). This will bring more sales or service revenue to the firm, resulting in a better financial performance.

We would like to point out explicitly that we will focus on the latter form of impact in our study for the following reasons: First, we would like to focus on the advantage that a certification brings, and that advantage comes from increased customer confidence or investor preference that is directly contributed by the certification. We would like to

discover that whether certification works as a signaling tool, even in the context of information security. This approach much better suits our intention and goal of our study, as described in Chapter 1.

Another reason that we wouldn't take the "cost reduction" approach is that it is impractical to do so within the information security context. In the literature, studies on ISO 9001 expect that the quality management system can improve the production processes, thus decreasing the cost of defects. If we apply the notion above to the information security management system, we will be expecting 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 one. This makes it inappropriate to value all IT breaches and malfunctions in the same way. Individual inspection and investigation would be necessary. Thus, for the above reasons, we will concentrate only on the advantage that ISO 27001 certification brings.

Hypothesis 1: ISO 27001 Certification brings positive impact on firm financial performance.

2.2.2 Market Approach

As discussed in the literature review, certification can also work as a signaling tool. Certification would show the excellence of an entity on its corresponding certified field. Stock market reacting positively to favorable information is a widely acknowledged concept (Foster, 1973; Woolridge & Snow, 1990). Also, according to efficient market hypothesis, stock market prices will react to the information disclosure. Under these circumstances that stock market react positively to a favorable information disclosure, we believe an announcement of ISO 27001 certification will also cause stock market impact. ISO 27001 certification may work as a positive signal to the stock market investors, increase investors' or potential stockholders' confidence. This will lead to a higher willingness of purchasing the firm's stock, and eventually causing a risen stock price. There are events that impact positively to firm's stock market performance, such as a generous dividend announcement, or release of a favorable financial statement. If ISO 27001 certification is taken as an event that makes positive contribution with enough significance, it would have the same impact, though might be different in magnitude, as the dividend announcement or financial report release do.

Hypothesis 2: ISO 27001 Certification brings positive impact on firm's stock market performance.

Chapter 3. Research Methodology

3.1 Event Study

To measure the outcome of the implementation and certification of the ISO 27001 standard, different approaches can be adopted. As presented in the previous chapter, there are two major approaches that are widely adopted in the literature: one is based on questionnaires, or self-reported data; the other is based on financial figures or stock prices. In this study, we will adopt the approach that based on financial figures since we are interested in assessing the financial aspect of the impact from ISO 27001 implementation.

To assess the impact that a single event brings, event study is a very common method used by studies of related topics . Its analysis is based on a single event, and it examines the existence of the extra performance, or in the event study terminology, the abnormal return, that the event brings. By comparing the performance between entities under the impact from the event and the ones that do not have the impact, the difference in performance can be attribute to the target event. Any excess in performance, or abnormal return, can be explained as a contribution from the event, since the entities that experienced the impact enjoyed extra performance that the others don't.

Ideally, the only factor that contributes to the abnormal return after the advent of the event would best be only the event itself. In this situation, we can attribute the difference solely to the occurrence of the event. But there might be other factors that have effect in the performance while the event takes place. This interference might be contributed from individual or market-wide effects. To narrow down the cause and focus only on the event, the event study approach does not simply compare the

performance before and after the event takes place. It introduces the construction of an "expected return" as the base for comparison. The expected return is constructed based on performance of entities without the effect of the event, or a portfolio or market index. Such target for comparison is called the control entity (or market index). By comparing the performance of the entity with the event to the expected return, we can see the effect of the event, and with adequate cancellation of unwanted market-wide effects.

After constructing Statistical tests can help identifying whether the abnormal returns exist. One can draw to a conclusion that the event has a contribution, or a positive impact, to the performance. This approach would be very ideal for our study, as the event being ISO 27001 certification. In fact, in the literatures we previously reviewed, the ones that take financial figures as their research samples all uses event study. For these reasons, we chose event study to be the research methodology. However, the result of event study may not be able to tell the whole story, especially the underlying technic of the improvements. It merely tells that whether the performance changed positively after the event. We will report these concerns in the later part of this study.

3.2 Event Study on Operating Performance

To analyze the effect on operating performance, we need to establish a measurement for it. Net income would be a very straightforward measurement for operating performance. Net income is defined as the total amount of the revenue or gain received in a given period deducted by the expenses or losses paid. It is the net increment (or decrement in case of loss) to the stockholder's equity for the firm in the reporting period. Although net income is the final result from the operation in the period, direct use of net income as the measurement for operating income is not favorable. There are two reasons for this: First, direct comparison of net income between firms would neglect the effect of the firm size. In general, we can expect that bigger firms would earn proportionally more that smaller firms under the same performance of profitability. To overcome this problem, we need to eliminate the size different in the measurement. We can achieve this by using two approaches: either dividing the income by total shares of (common) stock outstanding, or by the total assets of the firm. The former measure is EPS, or earning per share. The latter one is ROA, or return on assets. Return on assets is the ratio of income to total assets, meaning how many times of the assets are the assets making profit. Both of the measurements are very regularly seen. We prefer using ROA as our measurement, since EPS is prone to be affected by change in equity structure, for example, stock splits (Barber & Lyon, 1996).

The second reason is that net income includes too many items that distract the result from our research focus. Reported net income contains all revenues and costs incurred in the reporting period, including the revenue from sales or services, cost of goods sold, and/or other revenues that originated by the firm's major operating activities, along with the ones that is otherwise incurred, such as investment, tax, and extraordinary revenue

and expenses. As in our hypothesis that we expect ISO 27001 makes contribution to firm performance through higher sales or service revenue, only income from major operating activities are expected to be impacted. Any inclusion of other revenues and expenses would be irrelevant to the event of certification, thus contaminating our measurement of operating performance. For the above reasons, instead of using net income, we will use operating income, which consists of only revenue and costs from only major operating activities, to avoid distraction and contamination that would have unwanted effects in our results. Thus, we will use ROA based on operating income in our study.

We now precisely define our measurement of operating performance, the Operating ROA, as follow:

$$Operating\ ROA = \frac{Operating\ Income}{Total\ Assets}$$

After deciding the measurement for operating income, we now describe the methodology of event study. To define abnormal return precisely, we first define P_{it} as the performance of event entity i at period t. To make the comparison, we define PI_{it} as the performance of the control entity of the event entity i at period t. We then use the difference (improvement or decrease) of the control entity performance of two periods (for example, t-1 and t) to estimate the performance of the event entity. That is,

$$E(P_{it}) = PI_{it} - PI_{it-1} + P_{it-1}$$

Where $E(P_{it})$ is the expected performance of event entity i at period t, PI_{it} is the performance of the control entity or market index i at period t. Lastly, we compare the actual performance of event entity i at period t with the estimated performance $E(P_{it})$.

The difference between the two figures will be the abnormal return for period t:

$$AR_t = P_{it} - E(P_{it})$$

Abnormal return, in ideal conditions, states the difference of performance between event and non-event entities. To ensure that the comparison is least contaminated by other non-event factors, for example, market-wide influences, the matching between an event entity and its control entity is critical. The ideal way will be finding the most similar entity of an event entity to be its match. There are several approaches to measure the similarity of the firms. We can match the firm by similar size, similar operating performance, or by both. To match by firm size, total assets would be a direct favorable measurement. To match by performance, return on assets, or ROA, is usually preferred. We also match firms by comparing both firm size and ROA. We will report all three sets of sample-control firm matches in our results.

3.3 Event Study on Stock Market Return

The abnormal return derived above will only suit operating performances, such as financial report figures. To compare the stock market performance of an event entity to a non-event entity (or market index), there are two major methods to be adopted. Hendricks & Singhal (1997) adopted the Cumulated Abnormal Return (CAR) in their study of TQM award's impact on stock market performance. CAR calculates the abnormal return of the event and control entity period by period, and report the summation of these period-wise abnormal returns. CAR can be defined as:

$$CAR_i = \sum_{t=1}^{n} (R_{it} - E(R_{it}))$$

Where R_{it} is the market actual return, and $E(R_{it})$ is the market expected return. We can see CAR as the summation of abnormal returns of each period.

While CAR is very common among event studies on firm stock performance, Buy and Hold Abnormal Return (BHAR) is also widely used in event studies with stock price. Differently, BHAR aggregates the period abnormal returns by multiplying them. Barber & Lyon (1997) conducted an extensive discussion about the difference between the methods. They found that CAR is more suitable for short-term (for example, one day or one week) analyses, while BHAR is for long-term (one year, three years) studies. In this study, BHAR is more preferable mainly due to the time frame in the design of this research. Although an efficient stock market will react fast to the disclosure of new information, in this study, however, it is very hard to identify the exact time of the information release. In addition, we expect this information will not likely to draw immediate market attention, since it is not directly related to a firm's financial or

operating situation, such as dividend announcement or financial report release. We believe short-term market return, or CAR results, is not preferable in our research topic. On the other hand, prior researches, such as Barber & Lyon (1997), recommend BHAR for its overall better performance. We will adopt BHAR in our stock market analysis.

BHAR calculates the difference the buy-and-hold return between event entity and non-event entity. BHAR for firm i from period t from 1 to n is defined as follow:

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

Where R_{it} is the actual market return (or the market return of the event entity) for firm i at period t, and $E(R_{it})$ is the expected market return for firm i at period t.

A significant BHAR shows that holding the event entity's stock would have significant excess return, which is attributed to the advent of the event. There are also a variety of statistic methods used to test BHAR results. In out study, we will use BHAR to measure that whether ISO 27001 brings positive impact to firm's stock market performance after accreditation.

3.4 Samples

To carry out an event study based on financial figures, there are several datasets required. According to the event study methodology described in the previous chapter, the core of event study, which is the measurement of abnormal return, is established by performance of event entities and non-event entities (or market-wide performance). We first obtained a list of worldwide ISO 27001 certified firms from iso27001certificates.com[1]. Each registration of ISO 27001 certificates is listed with the name of certificate site. We would like to clarify in particular the difference between "site" and an organization, enterprise or business entity. A "site" can be a whole business entity or organization, but can also be just one office, facility, or operational unit of a company. It depends on to what extent the certification covers. Moreover, the list is categorized by location of certificate 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, as it might be a foreign company to the UK.

As our research is aimed at examining financial figures and stock market returns, we need to trim the list by removing firms that this information are not available for. We examined the list firm-by-firm and identified the firms that are publicly listed. Listed firms are obligated to release their financial results at least annually, as usually required by accounting standards or law in most countries. These publicly available financial results serve as a great source of financial performance of a firm. Furthermore, as these results are prepared by the management of the firms and are audited by accountants. For those unlisted or private firms, they are unfortunately invalid for our research.

[1] http://www.iso27001certificates.com/; retrieved in October 2011

However, only a very small portion of firms on the list is suitable. We found out that most of the certificated firms are either private, non-listed, or are non-profits. This is very different from the studies of ISO 9000. This dramatically decreased the size of valid samples. We will elaborate this issue in the later chapters.

Although the certificate list obtained from iso27001certificates.com provides very important information, it still lacks one critical key attribute – the certification date. This information is fundamental in our design of research. However, there is no one-stop data source to retrieve all certification dates for all certificates. We reviewed all valid samples one-by-one for the certification dates. Some certification registrars provide detail certification information for each of their clients, mainly for verification requests from the public. We utilized these services to gain part of the certification dates. For those whose registrar does not provide this service, we looked up their websites and for information on certification. If they were not available, we look at the press releases for their announcement of the certification. Firms with no certification dates are excluded from our study. This process further decreases our valid samples.

As there are some major challenges in our sampling process, we have taken steps to ensure the amount of samples is adequate. Since there is a major proportion of ISO 27001 certificated firms that are whether private or not listed, this means that we have no access to their financial figures, and they do not have any stock market performances. To retain the available amount of samples for our study, we decided to perform a worldwide study. We chose the countries that have most ISO 27001 certificates, which are United Kingdom, United States, Germany and Spain. Other countries that have only limited number of ISO 27001 certificates are not included in this research. Although we do no often see an event study conducted under a global scope, we still believe that by

carrying out an event study correctly with appropriate matching of control firms, the result are still reliable. In the next chapter, we will introduce the matching technics of control firms. We will also discuss about our global scope of sample firms in the following chapters.

3.5 Control Firms

Control firms are the core part of an event study, as it is the key to construct expected performance for the calculation of abnormal return. The performance of control firms is taken as "how the firm should perform without the event". Thus, the selection of control firm should suffice the following two characteristics: (1) it has no experience in the event, (2) it can best present the firm's performance in absence of the event. In the past, many studies have used different criteria to match up the control firms. As event study methodology for operating performance and stock market return are very different, so would the matching schemes be. We will introduce the matching criteria for two different performances respectively as follows.

3.5.1 Matching Criteria for Operating Performance

Choosing the matching criteria would be very important as it affects the construction of expected return profoundly. In the literature, there are basically two approaches in control firm matching. There are size-based matching that matches firms of similar size. Firm size is usually measured by total assets of a firm. Some other studies match firms by their pre-event performance. There are a plenty of measurement for firm's financial performance, as we discussed in the previous section. Both of the approaches also took the firms' industry into consideration. This is usually done by matching by the SIC code of the firms. Barber & Lyon (1996) also conducted an extensive overview on selection of the matching criteria. It believed that matching by pre-event performance (ROA) provided the best results, while matching by size is also acceptable. We will adopt all three matching schemes as did in Corbett et al. (2005): matching by size (total assets), matching by performance (ROA), and matching by both of them. All three matching are accompanied by matching of industry (SIC). The matching of industry is done by

searching for 4-digit SIC matching. In case that no matching firm can be found, we will use 3-digit, then 2-digit matching. Any firms does not match at least 2-digit SIC is considered not eligible.

We constructed a candidate control firm pool consisting of all firms available from COMPUSTAT. For ROA abnormal returns, as suggested by Barber & Lyon (1996), and adopted by several other researches, we adopted the Total Assets, ROA and Total Assets-ROA combined as the matching criteria for our event study with ROA. That is, any firm lies within a certain range or ratio of the measurements will be taken as valid match. We followed Corbett et al. (2005) to use 50% to 200% as our valid range. That is, any firm lies in 50% to 200% of the matching criteria (for example, 50% to 200% of ROA) can be accepted as the control firm. To eliminate undesired effect that might contaminate the event study, it would be the best to match the firms with similar pre-certification performance together. Thus, all the matchings will be based on pre-certification performance or firm size.

3.5.2 Matching Criteria for Stock Market Performance

For event study on stock market performance, such as BHAR, we will take stock market performance matching along with firm size into consideration while matching. We will use market value of equity (MVE) as the measurement, which fits the two considerations above. MVE is the market worth of the firm, or to be more precisely, the total market value of outstanding common stock, which is defined as follows:

$$MVE = Total\ Shares\ of\ Common\ Stock\ Outstanding \times Balance\ Sheet\ Date\ Stock\ Price$$

In addition, stock price of all sample and firms in control firm pool is also necessary. We gathered all daily closing stock price in the research time period. For MVE calculations, we multiply common shares outstanding by its corresponding financial report day closing stock price. Then MVE matching is performed using the figure derived above using the same 50% to 200% criteria. We also perform both one-to-one and portfolio matching.

3.6 Statistical Test

After appropriate matching, we can calculate abnormal return based on methods described above. We then use appropriate statistical method to see whether the abnormal return is significant. The goal is to see whether the observed set of abnormal return exists. We can achieve this by testing the abnormal returns for their mean or median. A zero mean or median of abnormal return shows that the impacts do not statistically exist. Student's t-test provided a straightforward and easy method to carry out such test. The null hypothesis of Student's t-test is that the set of the data has a mean of a designated value, which is zero in our case. If the results reject our null hypothesis that the mean abnormal return is zero, it would be evidence that the abnormal return we measured do actually exist. On the other hand, if the results have failed to reject the null hypothesis, it would show that the mean abnormal return is not statistically different from zero, which suggests that abnormal returns do not exist. Student's t test is defined as follow:

$$t = \frac{\bar{x} - \mu_0}{\frac{s}{\sqrt{n}}}$$

Where $\bar{x}$ is the sample mean, μ_0 is the designated mean value, s is the sample standard deviation, and n is the sample size. In our analysis, μ_0 will always be 0, as our null hypothesis is that the mean abnormal return (the sample mean) is zero.

As Student's t test is a favorable and straightforward statistical solution to the studies like ours, however, there are researchers seeking for a better method to measure the results of an event study. Barber & Lyon (1996) did an extensive in-depth review of the methods that suits operating performance studies. The study reviewed the conventional

Student's t-test, as well as Wilcoxon's singed rank test. Wilcoxon's singed rank test, sometimes also called Wilcoxon's T test, is a nonparametric test to assess the difference between pair of samples. It can be used as an alternative to Student's t-test as they are of similar purpose. There are several key differences between the two tests: (1) Student's t-test assumes that the population is normally distributed, while Wilcoxon's signed rank tests does not make any assumption on the distribution of population; (2) Student's t-test, in this case, has a null hypothesis of zero mean, while Wilcoxon's signed rank test hypothesize a zero median; and (3) Wilcoxon's signed rank test well suits smaller sample size.

After extensive experiments with empirical data, the study concludes that Wilcoxon's singed rank test is overall more powerful that Student's t-test. It recommends the use of the test in studying of any sample situations. However, other researches also include the results of Student's t test, as it is still most common in detecting significance of differences between values and widely reported in similar studies. We will adopt both of two tests in our results in the later analyses.

Chapter 4. Results and Analysis

4.1 Results

We now present the results of our study. We hypothesized that ISO 27001 certification has positive contribution firms after accreditation, in terms of both financial performance and stock market performance. Results of the first hypothesis are presented in Table 4.1 to Table 4.4. Each table presents the result under different statistical test (Student's t-test and Wilcoxon Singed Rank Test) and matching approach (one-to-one and portfolio matching) respectively. In each table, we present the result under three matching criteria in five periods. Year t is the year that the firm gained ISO 27001 accreditation. Our matching is based on the respective criteria in t-2 year.

For the hypothesis that ISO 27001 would have positive contribution to firm stock market performance, we present the result in Table 4.5 and 4.6 under the same two matching approaches. In each table we present the result derived from the two statistical tests as we conducted above.

All the result values are p-values showing the significance of the tests. It is usually considered that a p-value under 0.1 indicates a significant test result. In this study, our statistical tests are based on the null hypotheses that the test samples (abnormal return from each performance indicator and matching criteria) have mean values of zero. If the tests results are significant (have a p-value under 0.1), the null hypothesis would be rejected, meaning that the abnormal returns do exist and thus supports our initial hypothesis that the ISO 27001 certification have positive contributions to the firm performance.

We now turn to the results. As we can see, in most of the tests, the results showed generally low significance as the p-values are high and well above the significant threshold 0.1. The non-significance of our test has failed to reject our null hypothesis in our statistical test that the mean abnormal return is zero. This indicates that there are no evidence of extra contributions from ISO 27001 accreditation in every tests, every matching criteria, and every time period.

We will discuss the result in detail in the following section.

Table 4.1
Student's t-test result, one-to-one matching

Criteria	t-2	t-1	t	t+1	t+2
Total Assets	0.9914	0.9258	0.9093	0.6723	0.9029
ROA	0.9762	0.7936	0.6511	0.9216	0.1334
Total Assets / ROA	0.9144	0.1087	0.9260	0.1697	0.7791

Table 4.2
Student's t-test result, portfolio matching

Criteria	t-2	t-1	t	t+1	t+2
Total Assets	0.3925	0.5543	0.9215	0.4464	0.8078
ROA	0.4319	0.5372	0.6638	0.5723	0.3838
Total Assets / ROA	0.2151	0.5526	0.5942	0.4803	0.5789

Table 4.3
Wilcoxon signed-rank test result, one-to-one matching

Criteria	t-2	t-1	t	t+1	t+2
Total Assets	0.5459	0.8538	0.7285	0.6705	0.7337
ROA	0.7680	0.8032	0.5787	0.9866	0.1819
Total Assets / ROA	0.7246	0.2697	0.7246	0.3884	0.5412

Table 4.4
Wilcoxon signed-rank test result, portfolio matching

Criteria	t-2	t-1	t	t+1	t+2
Total Assets	0.6023	0.4964	0.8368	0.4980	0.6261
ROA	0.6947	0.4522	0.3277	0.7817	0.3516
Total Assets / ROA	0.3339	0.5155	0.6584	0.5819	0.8538

Table 4.5
Buy-and-Hold Abnormal Return, one-to-one matching

Student t-test	0.1997
Signed Rank Test	0.5000

Table 4.6
Buy-and-Hold Abnormal Return, portfolio matching

Student t-test	0.3522
Signed Rank Test	0.6257

4.2 Analysis

In the previous section, we have found out that there is no evidence of both financial and stock market impact after ISO 27001 certification. This indicates that there is no support for our hypotheses from the tests. Although the results are not consistent with our hypotheses, we found the results very interesting in multiple aspects. We would like to analyze the results in detail in the followings.

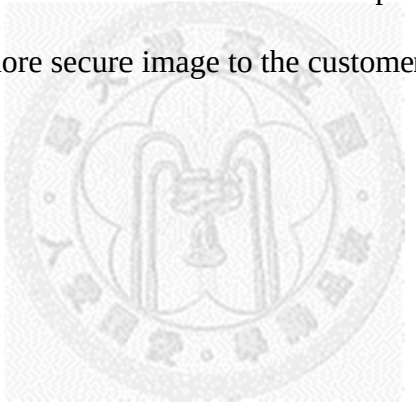
First and foremost, we would like to return to the nature of the ISO 27001 certification for explanations that it brings no advantage in terms of financial and stock market performance. In contrast, the ISO 9001 standard is another ISO standard that have a very different story. In the literature, most studies found ISO 9001 consistently making positive contributions to firm's financial performance and stock market value, as we reviewed in Chapter 2. Though ISO 9001 is focused on quality, while ISO 27001 is on information security, ISO 27001 standard is actually comparable to ISO 9001 in many ways. They both require formulating explicit policy and guidelines to ensure compliance. They both require extensive documentation on processes that the employees carry out. They are both based on the same Plan-Do-Check-Act (PDCA) cycle for continuous improvement. They both require involvement from top or senior management. In general, their approach on building a management system is very similar. The only difference left would be the context of the management.

The nature of ISO 9001 is about quality management. It 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 customer's satisfactory. ISO 27001, on the other hand, while still an management system featuring

continuous improvement, but instead of pursuing meeting customers' requirements and gain advantage, ISO 27001 is more about "prevent loss through management". ISO 27001 starts at a very different point. The design of the management system is based on a risk-based approach. The approach is to identify, control, and treat the risk that exists in the organization's IT. Minimization the impact that the risk might potentially bring, along with continuous improvement to ensure the survivability of the organization, is the goal of the standard. That is to say, ISO 9001 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 impacts which potential IT failures or breaches might bring. 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 a "meeting the requirement", instead of an advantage. This would explain why there is no reaction from the market toward the certification.

Another contributing reason might be the scope of the certification. In our previous certificate-by-certificate review, we found out that large amount of the firms did not apply for 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. As ISO 27001 implemented the risk management as its basic approach to implement the ISMS, it is best to plan the whole risk management at organization 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 ("Environment"), through risk identification, assessment and treatments, and finishing with monitoring the ongoing activities ("Monitoring") (COSO, 2004). This approach is nearly identical to what ISO 27001 requires, but with the height at the enterprise level. As ERM has become a very popular among the risk management context, people might take a non-organization-level ISO 27001 certification as a compromised or 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.



Chapter 5. Conclusion

5.1 Conclusion

We now draw this study to a conclusion. This study has provided an overview on the impact of ISO 27001 certification on financial aspects. As information security becomes a public concern, we would like to investigate that whether a certification on information security management system (ISMS) would benefit the certified firms through competitive advantage. We have seen consistent results in the literature that ISO 9001 brings competitive advantage to firms. Also, similar methodology has been used to investigate the impact that IT investment brings. However, we have found no study that investigate ISO 27001 certification in the same manner. We hypothesized that ISO 27001 would bring competitive advantage and draw market attention that result in enhancements in firm performance in both financial and stock market terms.

We used event study as our methodology for this investigation, which is widely used in studies, including those we previously reviewed. Results showed that there is no evidence of positive impact. We believe that the nature of ISO 27001 certification are the major explanation for this, since a sound information security management would not be seen as an advantage, but an obligation that an organization should carry out. In addition, the scope of the certification is also a concern, since most of our samples only have a partial coverage of certification, instead of having certified at organizational level.

5.2 Limitations

The most concerned limitation for this research is the number of available samples in out tests. Though there is more than thousands of ISO 27001 certificates around the world, the rather low availability of financial data for the certified firms are a major obstacle in our study. Our study approach completely relies on financial figures and stock market prices. However, as we pointed out in the previous chapters, most ISO 27001 certificates are either non-public or non-listed. We could never obtain stock prices from non-listed firms, or reliable financial information from either of the firms. Only listed firms have stock prices from a public stock market, and listed firms are usually required to publish an audited financial report at least at an annual basis. This would be the only reliable source of financial data for our study.

We have reported in the previous chapter that our available sample size has been dramatically decreased due to the lack of financial information. To retain our sample size at a reasonable level, our only feasible approach would be including as much firms as we can in our study, regardless of the origin country of the firm. We have mentioned that most event study analyzes samples from a single country. However, we believe that as the firms in our study are majorly international companies, and as the market is globally available, an event study based on multinational samples would still report reliable results. In addition, our source of financial and stock market data, COMPUSTAT, is very reliable and widely adopted by studies around the world. With appropriate handling of the monetary values and exchange rates, we consider this event study is consistently reliable as one with only samples of single origin of country.

5.3 Future Research

We have mentioned in the previous chapter that our study approach, event study, could explicitly indicate that whether an event would make impact on performance. We can know in statistical terms that whether such abnormal return exists. But the underlying mechanics that the impact works is not explained. That is, how abnormal return is generated, or not generated, is not within the scope of an event study. Event study only answers a yes-or-no question on existence of excess in performance for firms with experience in the event. We believe that no matter the abnormal return exists or not, which in our case is absent, the reason and the explanation of such results is very interesting and could make impressive contribution. This would require 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 that help firms achieve certification, which would greatly expand the magnitude of this study. Thus, we suggest that in the future, on the basis of this quantitative empirical research with event study, future researchers can take a qualitative methodology to investigate this issue.

Reference

AM Lima, M., Resende, M., & Hasenclever, L. (2000). Quality certification and performance of Brazilian firms: an empirical study. *International Journal of Production Economics*, *66*(2), 143–147.

Anderson, M., Banker, R. D., & Hu, N. (2003). Returns on investment in information technology. *Proceedings of Twenty-Fourth International Conference on Information Systems* (pp. 563–575).

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201.

Barber, B. M., & Lyon, J. D. (1996). Detecting abnormal operating performance: The empirical power and specification of test statistics. *Journal of Financial Economics*, *41*(3), 359–399.

Barber, B. M., & Lyon, J. D. (1997). Detecting long-run abnormal stock returns: The empirical power and specification of test statistics. *Journal of Financial Economics*, *43*(3), 341–372.

Boehmer, W. (2009). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. *Availability, Reliability and Security, 2009. ARES'09. International Conference on* (pp. 392–399).

Boehmer, Wolfgang. (2008). Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001 (pp. 224–231). IEEE.

Calder, A. (2006). *Information Security Based on ISO 27001/ISO 17799: A Management Guide*. Van Haren Publishing.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24–38.

Casadesus, M., & Gimenez, G. (2000). The benefits of the implementation of the ISO 9000 standard: empirical research in 288 Spanish companies. *The TQM Magazine*, *12*(6), 432–441.

Chai, S., Kim, M., & Rao, H. R. (2011). Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems*, *50*(4), 651–661.

Corbett, C. J., Montes-Sancho, M. J., & Kirsch, D. A. (2005). The financial impact of ISO 9000 certification in the United States: An empirical analysis. *Management Science*, 1046–1059.

COSO. (2004). Enterprise Risk Management — Integrated Framework: Executive Summary.

Docking, D. S., & Dowen, R. J. (1999). Market interpretation of ISO 9000 registration. *Journal of Financial Research*, *22*(2), 147–60.

Dos Santos, B. L., Peffers, K., & Mauer, D. C. (1993). The impact of information technology investment announcements on the market value of the firm. *Information Systems Research, 4*(1), 1–23.

Foster, G. (1973). Stock Market Reaction to Estimates of Earnings per Share by Company Officials. *Journal of Accounting Research, 11*(1), 25–37.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404–410.

Hendricks, K. B., & Singhal, V. R. (1997). Does implementing an effective TQM program actually improve operating performance? Empirical evidence from firms that have won quality awards. *Management Science*, 1258–1274.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems, 18*(2), 140–150.

Im, K. S., Dow, K. E., & Grover, V. (2001). Research Report: A Reexamination of IT Investment and the Market Value of the Firm–An Event Study Methodology. *Information Systems Research, 12*(1), 103–117.

Jeng, Y. C. (1998). Performance evaluation of ISO 9000 registered companies in Taiwan. *The TQM Magazine, 10*(2), 132–138.

Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in Taiwan. *Telecommunications Policy*, *33*(7), 371–384.

Schultz, E. E. (2004). Sarbanes-Oxley–a huge boon to information security in the US. *Computers & Security*, *23*(5), 353–354.

Simmons, B. L., & White, M. A. (1999). The relationship between ISO 9000 and business performance: does registration really matter? *Journal of Managerial Issues*, 330–343.

Terlaak, A., & King, A. A. (2006). The effect of certification with the ISO 9000 Quality Management Standard: A signaling approach. *Journal of Economic Behavior & Organization*, *60*(4), 579–602.

Terziovski, M., Power, D., & Sohal, A. S. (2003). The longitudinal effects of the ISO 9000 certification process on business performance. *European Journal of operational research*, *146*(3), 580–595.

Tong, C. K. ., Fung, K. ., Huang, H. Y. ., & Chan, K. . (2003). Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard. *International Congress Series*, *1256*(0), 311–318.

von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security*, *19*(7), 615–620.

Weill, P. (1992). The relationship between investment in information technology and firm performance: a study of the valve manufacturing sector. *Information Systems Research*, *3*(4), 307–333.

Woolridge, J. R., & Snow, C. C. (1990). Stock market reaction to strategic investment decisions. *Strategic Management Journal*, *11*(5), 353–363.