ISO/IEC27001 Implementation

Hooran Mahmoudinasab
Department of Computing
Macquarie University,
Sydney, Australia
hooran.mahmoudinasab@students.mq.edu.au

Abstract

The International Organization for Standardization (ISO) is an international organization that sets standards which provide measurable quality to products and services which, if implemented correctly, should increase reliability and operational efficiency. ISO established several IT standards, one of which is ISO/IEC27001:2005 Information Security Management System (ISO27001), providing security requirements to establish and implement security management within the scope of business. ISO27001 is used by companies around the world. For example, in 2008 in the USA only 85 companies held current certification while in Japan 2994 companies held a certification. This research tries to identify the reasons for the difference in the number of companies among Germany, UK, Austria and Switzerland that use ISO27001. The paradox is that the UK and Germany, who were the initial proponents of the standard, have less certificate holders than Japan and Taiwan. What is the reason for this?

1 Introduction

ISO/IEC27001 Information Security Management System is one of the standards of ISO that provides required planning and implementing security management. In this regard, ISO27001 gives some guidelines to establish, maintain and improve ISMS. This standard is being used in approximately 60 countries and the total number of companies that are certified to this standard is slightly more than 5000. [1] However, in each country, the number of companies having ISO27001 is different from other countries. While the founders such as UK and the Germany established the standard, the later adopters outnumber the proponents. This difference in registration raised this question: if the importance of the standard and the advantages are clearly understood by the founders and if these companies are more aware of its implementation, why are there more ISO27001 holders in those countries that have less participation and a less active role in the creation of the standard. This difference has no specific pattern, it is not possible to assign this distribution to simply one factor. In 2008, there were 85 certified organizations in the USA, and 2 in Canada. This suggests that despite geographical, economical and social similarities between the USA and Canada, ISO27001 holders were distributed varyingly in a way that geographical, economical and social factors might not be the reasons for the discrepancy. This project sets out to identify the reasons that make countries not involved in the development of ISO27001 use it more than those that originally set it up. The benefits that could derive from this include substantial improvements in Information Security Management, reduced management costs and a clearer understanding of the reasons to implement the standard. These improvements cannot be carried out unless we know why about the distribution of ISO27001 in different countries.

2 Country Selection

In order to understand this difference within the time scope of the research and to form a model for the future studies, four countries were selected including UK, Germany, Austria and Switzerland. The first reason of selection was to

[1] http://www.iso27001certificates.com

choose countries with similar economical, social and geographical characteristics with different number of registration to remove any factors that is related to these characteristics. All of these countries are located in Europe and are the EU (European Union) members. Besides, the social and economical statuses of the countries are similar. Although Australia was in the same level with the selected countries according to the economical and social factors, the geographical distance and its trade status were not on par with the other selected countries. The other major reason was the fact that UK was the founder of ISO27001 while Germany has had most contribution of the standard and was good nominations in the research. Switzerland is bordered by Germany in north while having a specific standing in Europe with advanced infrastructure industries and level of life standard. Austria is in neighborhood of Germany and Switzerland but has more transaction with eastern Europe countries. In 2005, the number of standard holders was 368, 108, 21 and 4 in UK, Germany, Austria and Switzerland respectively. The overall status of the countries gave the appropriate framework for comparison

Hence, the current research was taken to clarify if there is a relation between the numbers of ISO27001 holders. Three factors were investigated including 'population', 'total number of companies' and 'trade volume' (volume of import and export). The research needed a background to reduce the time of study and effort to narrow down the possible reasons. However, since there was no study taken to explore this discrepancy, the scope of the research was narrowed down to the above mentioned countries. Consequently, the review of resources was limited to ISO as the main standardization institute and the relevant standardization bodies in the selected countries.

3 The View of ISO Bodies

ISO was the starting point for the study. It reflected some reasons as the benefits of ISO27001 implementation. The main reasons were categorized under ISO. Besides, the reasons communicated by the standardization bodies of the countries were also categorized under the same table. Meanwhile, two related articles were also studied in order to find the purpose of ISO27001 implementation and its various implementations.

4 The View of the Organizations

The views were categorized according to the reasons in the SoAs. The main category was designated to the IT infrastructure security (establishing and maintaining ISMS and security controls) and the other categories were designated to specific security purposes such as securing customers information and data centre protection. The result of categories was divided by each country to form the final table. The data of this table were used as the data collected from the organizations for analysis.

5 Data Analysis

The analysis included two phases: data analysis and statistical analysis. During data analysis the following stages were accomplished:

1. Preparing the list of companies accredited by ISO27001 in the four selected countries.
2. Finding the main field of activity of the companies and categorizing them.
3. Investigating the SoA of the companies to find the reasons of implementation.
4. Categorizing the reasons in each country based on the responses by the companies within that country.

In the statistical analysis the following stages were accomplished:

1. The following data were gathered for analysis:

A) The total number of companies in each country.

B) The population of the four countries according to the UN census.

C) The volume of export and import of each country.

D) The relation between the number of registrations in each country and four variables: total number registrations, population, volume of export and volume of import based on Chi-Square test.

5.1 Registered Companies

The companies registered to ISO/IEC 2001 were almost accredited by the standardization body within the country. In UK and Germany, the standardization bodies were BSI and DIN. However some of registrations were accredited by other standardization bodies such as TUV and Certificate Europe.

5.2 Companies Activities

The fields of activity were divided according to the importance and the total number of companies in each group. However, it was difficult to have a clear categorization since some of the companies were working in more than one field. Besides, some had distinct activities which did not fit in any category. The major problem was to find categorization which fit all the companies and conform to activities in companies in other countries.

It appeared that security in the field services is of most important activities of the organizations which were accredited by ISO27001. This included both IT and non-IT fields, which can indicate the importance of services in all the countries. The numbers of registration were almost the same in both UK and Germany. However, UK showed a larger number in non-IT services compared to Germany. In addition, three fields of activities were identified with larger numbers in UK compared to other countries including Telecommunication, Health and Medicine and Finance and Banking. Meanwhile, Germany contributed more in Network and Internet Services. It appeared that ISO27001 registrations in UK had more inclination towards non-IT services. Since the number of registrations were small in Austria and Switzerland, it was not possible to draw a conclusion on the types of activities in these two countries.

5.3 Implementation of the Standard

Having read all the SoAs of the companies, the reasons were extracted and categorized based on the key terms in SoA and importance of them. The reasons included:

1. Forming IT Security Infrastructure
2. Securing Organization Information and Assets
3. Security for Organization Services
4. Protection of Customers' Information
5. Data Centre Security
6. Internet & Network Security

This categorization was in accord with the needs in IT sector as it identified specific areas requires security such as Internet & Network, Data Centre and System Data Recovery. The key reason of implementation was categorized as IT Infrastructure that covered essential requirements for establishing ISMS. Based on the reasons given by the companies, the findings indicated that few common benefits for ISO27001 which has been stated both by the standardization bodies and the organizations such as risk management and product or service safety for the customers.

The comparison between both the reasons of standardizations bodies and the companies showed that the standardization bodies emphasized on the importance of ISMS establishment and compliance with rules and regulations while the companies expressed emphasis on IT infrastructure and service and customers' information security. The trend observed in four countries showed a similar pattern of reasoning as IT infrastructure security was the major reason of registering for ISO27001 with 152, 42, 7 and 2 registrations in UK, Germany, Austria and Switzerland respectively. The next identified reason was Organization Services, the process of securing services offered by the organization to the customers or a third party. The figure showed 105 companies located in UK that expressed Organization Service security as the reason of using ISO27001. However, this amount was significantly less in Germany reaching to only 15 companies. In Austria and Switzerland this amount was 2 and 1 respectively. The amounts of companies which recognized the reason for the implementation showed that a reason of discrepancy in the number of implementation may be rooted in the types of advantage ISO27001 may offer. This difference in the numbers of reasons for Organization Services security may indicate that since a significant number of companies have expressed this reason for using ISO27001, it can be the justification for the large number of the implementation of the standard in UK.

It is interesting to notice that both number of reasons given for securing Organization Information & Assets and Customers' Information hovered around the same amount. This may indicate the same level of importance for securing the information related to a company as well as customers while the amounts in other categories were not following a certain trend.

Reason of Implementation	UK	Germany	Austria	Switzerland
IT Infrastructure	152	42	7	2
Organization Information & Assets	51	3	2	0
Organization Services	104	15	2	1
Customers' Information	45	4	2	0
Data Centre	24	7	0	0
Internet & Network	39	6	2	2
Outsourcing	8	4	0	0
System Data Recovery	10	0	0	0

Table 1.The Number of Reasons of Implementation of ISO27001 in the Four Countries

6 Statistical Analysis

To investigate why the implementation was different in quantity, it was evaluated by some influential factors seemingly have impact on the implementation numbers. The criterion for this evaluation was through statistical calculations of Chi-Square. In this study three factors were selected. First factor was the total number of companies located in each country accredited by the ISO27001. It was expected that the number of companies would be consistent with the number of registration but the figure countered what observed in the number of registrations. Although UK had more number of registrations but its total number of companies was comparatively less than the other companies. To examine the relation between the total number of companies and the registrations the statistical test were performed that indicated no relation between the number of companies as a factor and the registrations.

	Number of Registrations	Total Number of Companies
UK	366	2,016,700.00
Germany	110	2,915,482.00
Austria	24	161,732.00
Switzerland	5	311,324.00
Total	505	5,405,238.00

Table 2. The Values of Registrations and Total Number of Companies

Chi-Sq = 289.387, DF = 3, P-Value = 0.000

The same test was conducted with variable of population to see if there was a relation between the registrations and the population.

	Number of Registrations	Population
UK	366	60,776,238.00
Germany	110	82,400,996.00
Austria	24	8,199,783.00
Switzerland	5	7,554,661.00
Total	505	158,931,678.00

Table 3. The Values of Registrations and Population

Despite having more registrations, UK showed the large margin of 20 millions in population. Meanwhile, the result of the statistical test also showed no relation between the numbers of population:

Chi-Sq = 258.023, DF = 3, P-Value = 0.000

As using ISO standards are supposed to be facilitators of trades between the countries, the quantity of business transactions was selected as a variable to measure if it had an impact on the number of registrations. In doing so, the volume of export and import of the countries were selected to the test and the following result was observed:

	Number of Registrations	Export(Million dollar)
UK	366	348,430.00
Germany	110	911,742.00
Austria	24	103,742.00
Switzerland	5	118,527.00
Total	505	1,482,441.00

Table 4. The Values of Registrations and Volume of Export

Chi-Sq = 678.899, DF = 3, P-Value = 0.000

	Number of Registrations	Total Number of Companies
UK	366	461,076.00
Germany	110	718,150.00
Austria	24	104,489.00
Switzerland	5	111,603.00
Total	505	1,395,318.00

Table 5. The Values of Registrations and Volume of Import

Chi-Sq = 359.933, DF = 3, P-Value = 0.000

7 Conclusion

The implementation of ISO27001 furnishes companies with a framework to establish ISMS and guidelines for security implementation. Companies which have been accredited by this standard vary in number from a country to another. The reason may be tied to different factors and may be different in any specific country. Yet, the impact of certain factors such as number of registered companies, rules and regulations of the country, population, geography, business transactions are inevitable. During this research, four countries were selected for the study with similar economical and geographical status.

To evaluate the efficient factors influence the implementation of ISO27001, the reasons of implementation expressed by both the standardization bodies and the companies were evaluated. Besides, the types of activities of the companies as a contributor to the quantity of the registrations were examined. In addition, three factors (total numbers of companies, population and business transactions including the volume of export and import) were statistically examined. The overall finding indicated that the reason of discrepancy between the selected countries could be rooted in the nature of companies' activities and possibly social and regulatory factors. While number of companies and population seemed to be the efficient factors, the outcome of the statistical analysis negated this notion.

Appendices

Appendix A. The Table of the Variables

Country	Population	Companies	Export (Million dollar)	Import (Million dollar)
United Kingdom	60776238	2,016,700	348430	461076
Switzerland	7554661	311,324	118527	111603
Germany	82400996	2,915,482	911742	718150
Austria	8199783	161,732	103742	104489

Appendix B. The Table of Activities

Type of Activity	Business & Products	Education	Finance & Banking	Hardware Products	Health & Medicine	ICT	Infrastructure Group	Internet & Network	IT Consultant	IT Security Services	IT Services and Solutions	Management	Marketing	Non-IT Services	Security Services	Software Products	Telecommunication
UK	47	7	24	1	24	8	3	1	2	9	92	5	6	88	9	11	29
Germany	28	0	4	4	4	3	0	7	0	4	30	0	1	15	1	5	4
Austria	4	0	3	0	1	0	2	1	0	1	8	0	0	4	0	3	2
Switzerland	1	0	1	0	1	1	0	0	0	0	0	0	0	1	0	0	0

References

[1]. Economic Impact of International Standardization. Pages 19-20, Architecture-based Approaches to International Standardization and Evolution of Business Models, Junjiro Shintaku, Koichi Ogawa, Tetsu Yoshimoto, IEC CENTENARY, The University of Tokyo, Manufacturing Management Research Centre, Japan.

[2]. Standards: Unnoticed Factor for Business Results, Pages 130-132, Standards for Business, How companies benefit from Participation in International Standard Setting**,** Henk Je de Vries, IEC CENTENARY, Erasmus University, Switzerland, 2006.

[3]. International Organization of Standardization, ISO/IEC27001 [Online] Available at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 [Accessed 20th May 2009].

[4]. International Organization of Standardization, What the Standard Do, [Online] Available at: http://www.iso.org/iso/about/discover-iso_what-standards-do.htm [Accessed 20th May 2009].

[5]. International Register for ISMS Certificates, [Online] Available at: http://www.iso27001certificates.com [Accessed 20th May 2009].

[6]. United Nations Conference On Trade and Development (UNCTAD), Handbook of International Trade and Development Statistics, United Nations Publications, Geneva, [Online] Available at: www.unctad.org [Accessed 20th May 2009].